Educational Administration: Theory and Practice
2024, 30(11), 1882-1897
ISSN: 2148-2403
https://kuey.net/

Research Article

"The Growing Menace Of Cybercrime In India: Analyzing The Effectiveness Of Current Law Enforcement Strategies"

Ms. Sakshi Rewaria[1]*, Dr. Ramveer Singh[2]

[1]*Research Scholar, MVN University, Palwal, Haryana; advocate.sakshirewaria@gmail.com
[2]Associate Professor, MVN University, Palwal, Haryana; ramveer.singh@mvn.edu.in

Citation: Ms. Sakshi Rewaria, et.al (2024). "The Growing Menace Of Cybercrime In India: Analyzing The Effectiveness Of Current Law Enforcement Strategies", *Educational Administration: Theory and Practice*, 30(11) 1882-1897
Doi: 10.53555/kuey.v30i11.10088

ARTICLE INFO

ABSTRACT

Cybercrime has emerged as one of the most pressing challenges in India, with the country witnessing a sharp increase in digital offenses due to rapid internet penetration and the widespread adoption of technology. This paper aims to analyse the effectiveness of India's current law enforcement strategies in combating cybercrime, focusing on existing legal frameworks, enforcement mechanisms, and the role of specialized agencies.

Key legislation such as the Information Technology Act, 2000, and the establishment of the Cyber Crime Coordination Centre (I4C) have laid the foundation for a structured response to cybercrime. However, despite these efforts, the country continues to face significant challenges in addressing the growing complexity of cybercrimes, including online fraud, identity theft, data breaches, cyberbullying, and financial scams. This paper examines the limitations of India's legal and institutional structures, such as gaps in law enforcement training, delayed investigations, and the lack of a unified cybersecurity policy. It also highlights the difficulties posed by the transnational nature of cybercrime, where jurisdictional issues complicate the prosecution of offenders. By addressing the identified gaps and fostering collaboration among stakeholders, law enforcement can significantly improve its effectiveness in tackling this pervasive issue. This study contributes to the ongoing discourse on cybersecurity in India and offers actionable recommendations for policymakers and law enforcement agencies to strengthen their strategies against cybercrime.

Keywords: *Cybercrime, Data Breaches, Cyber Fraud, Cybersecurity, Digital Technology*.

1. INTRODUCTION

"Unless and until our society recognizes cyber bullying for what it is, the suffering of thousands of silent victims will continue."
— Anna Maria Chávez[3]

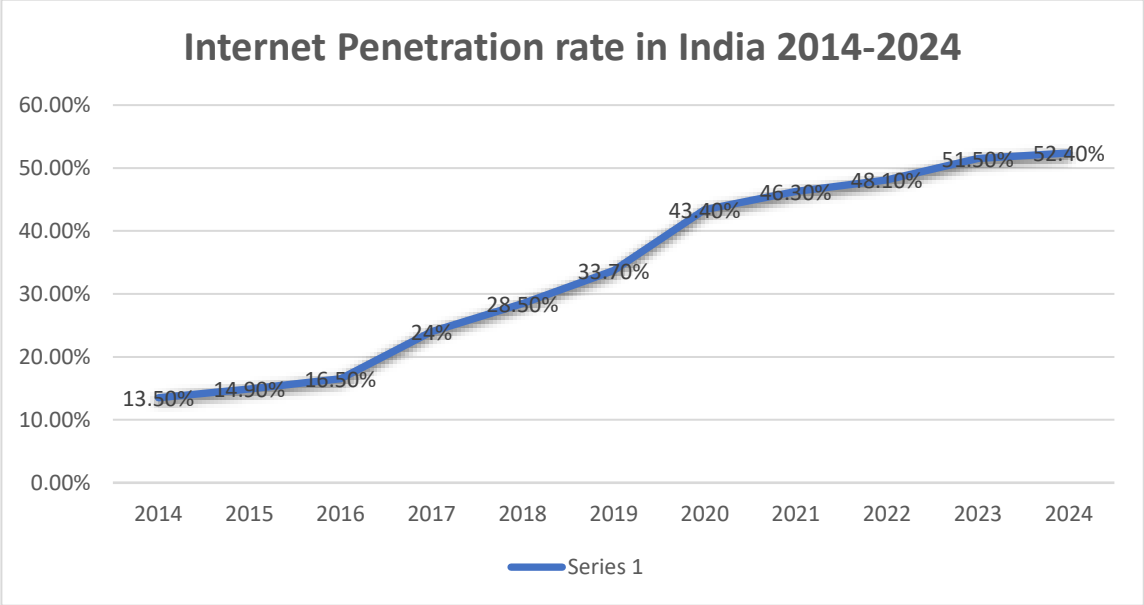
As society becomes increasingly digitized, the frequency and sophistication of cybercrimes have escalated exponentially, presenting novel challenges for law enforcement agencies worldwide. While many countries have developed robust regulatory frameworks and operational capabilities to counteract cybercrime, India lags, grappling with a myriad of obstacles that hinder effective investigation and prosecution of cyber offenses. Notably, the dearth of skilled personnel, inadequate legal frameworks, and complicated jurisdictional issues pose substantial hurdles for Indian law enforcement agencies endeavouring to combat cybercrime. Addressing these challenges requires a thorough examination of the underlying factors impairing the efficacy of the criminal justice response to cyber offenses in India. Therefore, this research aims to identify, scrutinize, and offer viable remedies for the principal challenges confronting Indian law enforcement agencies in investigating

[1] Research Scholar, MVN University, Palwal, Haryana; advocate.sakshirewaria@gmail.com
[2] Associate Professor, MVN University, Palwal, Haryana; ramveer.singh@mvn.edu.in
[3] Amc. (2013, June 25). Confronting cyber violence in the digital age. *HuffPost*. https://www.huffpost.com/entry/confronting-cyber-violenc_b_3157086

and prosecuting cybercrimes.[4] By doing so, this study intends to elucidate the intricacies of cybercrime investigation in India, offering cogent suggestions to augment the proficiency of the criminal justice apparatus and foster a secure digital landscape for all stakeholders .

In an increasingly digital world, the rise of cybercrime presents significant challenges for law enforcement agencies globally, and India is no exception. With a population exceeding 1.4 billion and a rapidly expanding digital landscape, the country has witnessed a surge in internet users, leading to an unprecedented increase in cyber-related offenses.[5] As the complexity and sophistication of these crimes evolve, so too must the capacity of law enforcement agencies to effectively combat them. [6] The term "cybercrime" refers to a broad range of unlawful actions made possible by the internet, such as financial fraud, identity theft, cyberbullying, data breaches, and cyberterrorism.[7]

In 2024, India's internet penetration rate surged to over 52%, a remarkable increase from just 14% in 2014. This shift meant that more than half of India's population of 1.4 billion people had access to the internet, reflecting a significant digital transformation. As a result, India ranked second globally with 629 million in terms of active internet users, only behind China.[8]This rapid expansion in internet access has facilitated greater connectivity, increased online services, and opened new avenues for digital education, e-commerce, and government services. However, it has also raised concerns about cybersecurity and the rise in online crimes, as more people engage in digital activities.



The graph illustrates the steady growth of internet penetration in India from 14% in 2014 to over 52% in 2024, highlighting a significant increase in digital connectivity over the past decade.[9]

Law enforcement agencies play a crucial role in maintaining public order, ensuring the rule of law, and safeguarding citizens' rights and freedoms. In India, a country characterized by its vast population, diverse culture, and complex social fabric, law enforcement faces a myriad of challenges that significantly impact its efficacy and public perception. The challenges faced by these agencies are multifaceted, encompassing systemic issues, resource constraints, socio-political dynamics, and evolving crime patterns.

One of the primary challenges confronting law enforcement agencies in India is the issue of inadequate resources. Many police departments operate with limited manpower, outdated technology, and insufficient

---

[4] Kumar, S., & Manhas, A. (2021). Cyber crimes in India: Trends and Prevention. *GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ) ISSN (E)*, *9*(5), 2347-6915.

[5] Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2022). A review on cyber crimes on the internet of things. *Deep learning for security and privacy preservation in IoT*, 83-98.

[6] *Cyber Crime | CID, Crime Branch*. (n.d.). https://odishapolicecidcb.gov.in/?q=node/251

[7] Staff, U. W. (2024, May 25). Cybercrime and Social Media: The Unseen Connection. *Subhash Ahlawat*. https://subhashahlawat.com/blog/cybercrime-and-social-media-the-unseen-connection

[8] TIMESOFINDIA.COM. (2024, June 16). 10 countries with the highest number of internet users. *The Times of India*. https://timesofindia.indiatimes.com/technology/tech-news/10-countries-with-the-highest-number-of-internet-users/photostory/111014666.cms#:~:text=India%20currently%20ranks%20second%20with,accounts%20for%20692%20million%20people

[9] Statista. (2024, May 15). *Internet penetration rate in India 2014-2024*. https://www.statista.com/statistics/792074/india-internet-penetration-rate/

funding, which hampers their ability to effectively prevent and respond to crime. According to the Bureau of Police Research and Development (BPRD), India has one of the lowest police-to-population ratios globally, with approximately 150 police personnel for every 100,000 citizens.[10] Furthermore, the lack of modern equipment and technology, such as forensic tools and communication systems, restricts the investigative capabilities of law enforcement, making it challenging to solve crimes efficiently.

Another significant challenge is the pervasive issue of corruption within law enforcement agencies. Corruption erodes public trust and undermines the legitimacy of the police force. In many cases, officers may be influenced by political pressures, leading to biased law enforcement practices and a lack of accountability. This culture of corruption not only hampers the effectiveness of crime prevention but also deters citizens from reporting crimes or seeking assistance from law enforcement. The perception of corruption can create a sense of helplessness among the public, further complicating the relationship between law enforcement and the communities they serve.

The socio-political landscape in India also presents unique challenges for law enforcement. The country is marked by regional disparities, communal tensions, and socio-economic inequalities that can lead to unrest and violence. Law enforcement agencies often find themselves at the forefront of managing protests, riots, and communal clashes, which can escalate quickly and require a delicate balance between maintaining order and respecting citizens' rights to assemble and express dissent.[11] Additionally, political interference in law enforcement can compromise the autonomy of police agencies, leading to decisions driven by political motives rather than the rule of law.

The rise of cybercrime and technological advancements has introduced new complexities for law enforcement in India. As the digital landscape expands, criminals exploit technology to perpetrate fraud, identity theft, and cyberbullying, among other offenses. Law enforcement agencies must continuously adapt to these evolving threats, often lacking the necessary training and resources to combat cybercrime effectively. This necessitates a collaborative approach, where law enforcement agencies work alongside tech companies and cybersecurity experts to develop effective strategies for preventing and investigating cybercrimes.[12]

Moreover, the increasing incidence of organized crime and terrorism poses significant challenges to law enforcement in India. Criminal organizations often operate across state and national borders, complicating law enforcement efforts. The nexus between organized crime and political corruption can create a formidable barrier to effective policing. Additionally, the threat of terrorism, particularly in regions like Jammu and Kashmir and the northeastern states, requires law enforcement agencies to adopt specialized training and strategies to counteract these threats while ensuring the protection of civil liberties.[13]

Public perception and community relations are crucial elements in the effectiveness of law enforcement. In India, the relationship between police and communities is often strained due to historical grievances, instances of police brutality, and perceived lack of accountability. Building trust between law enforcement agencies and the communities they serve is essential for effective policing. [14] Community policing initiatives, which emphasize collaboration between police and community members, can help bridge this gap. However, implementing such initiatives requires a cultural shift within law enforcement agencies, emphasizing transparency, accountability, and engagement with the public.

Mental health issues among law enforcement personnel also warrant attention.[15] The nature of police work can be inherently stressful, exposing officers to traumatic incidents and high-pressure situations. The stigma surrounding mental health in India often prevents officers from seeking help, leading to untreated psychological issues that can affect their performance and decision-making. Addressing mental health within law enforcement agencies is vital for ensuring the well-being of officers and enhancing their ability to serve the community effectively.[16]

One of the most pressing challenges is the lack of adequate resources and infrastructure within law enforcement agencies. Despite the growing prevalence of cybercrime, many police departments in India are

---

[10] Mudaliar, S. (2023, March 30). Police-public ratio stands at 152.80 per lakh person: Govt informs Parliament. *Hindustan Times*. https://www.shindustantimes.com/india-news/policepublic-ratio-stands-at-152-80-per-lakh-person-govt-informs-parliament-101680162971094.html

[11] Chudasama, D., & Solanki, L. (2021). Cyber crimes and challenges faced by criminal justice system. *International Journal of Information Security and Software Engineering*, *7*(1), 6-12.

[12] Vinay, K. A. (2024). *Challenges faced by law enforcement agencies in investigating and prosecuting cyber crimes in India*. ResearchGate. https://www.researchgate.net/publication/383785171

[13] Ministry of Home Affairs, Government of India. (2024). *Counter Terrorism and Counter Radicalization Division*. https://www.mha.gov.in/en/divisionofmha/counter-terrorism-and-counter-radicalization-division

[14] Common Cause & Lokniti-CSDS. (2023). *Status of Policing in India Report 2023: Surveillance and the Question of Privacy*. Common Cause. https://www.commoncause.in/wotadmin/upload/SPIR_2023_Key_Findings_%28English%29.pdf

[15] International Association of Chiefs of Police. (2022). *Addressing law enforcement mental health*. https://www.theiacp.org/sites/default/files/2022-09/258181~4.PDF

[16] Kumar, N. A., & Pandey, P. (2011). Cyber Crime-Law & Enforcement in India. *International Transactions in Applied Sciences*, *3*(1).

ill-equipped to handle the technical demands of investigating such offenses. Traditional policing methods often fall short in the digital realm, where criminals exploit technology to conceal their identities and activities. Law enforcement agencies frequently lack access to advanced forensic tools, cybersecurity expertise, and specialized training programs that are essential for effectively investigating cybercrimes. This resource gap not only hampers the ability to respond to incidents but also affects the overall deterrent effect of law enforcement efforts.[17]

Cybercriminals are often at the forefront of adopting new technologies, utilizing sophisticated tactics to evade detection and prosecution. The dynamic nature of cyber threats requires law enforcement to remain vigilant and adaptable, continuously updating their skills and knowledge to keep pace with emerging trends.[18] However, many agencies struggle to maintain this level of preparedness due to bureaucratic inertia, limited funding, and insufficient training opportunities. As a result, the gap between the capabilities of cybercriminals and those of law enforcement agencies continues to widen, undermining efforts to combat cybercrime effectively.[19]

"Ethics is a branch of philosophy which deals with what is considered to be right or wrong."[20] There are now numerous ethics programs and centers focused on bioethics, medical ethics, engineering ethics, computer ethics, corporate ethics, and legal ethics. Cybercrime is becoming a significant danger. Cybercrime encompasses a wide range of illegal activities, from denial of service attacks to electronic cracking, where computers or computer networks are utilized as a tool, a target, or a location for criminal conduct. It is also used to refer to more conventional crimes where the illegal action is made possible by computers or networks.[21]

2. MEANING OF CYBERCRIME

Cybercrime typically involves unauthorized access to data, online fraud, identity theft, hacking, cyberbullying, and other illegal activities conducted in cyberspace. Cybercrime can target individuals, organizations, or even governments, and often takes the form of financial theft, data breaches, or online harassment.[22]

One widely cited definition is from Lillian Edwards and Andrew Murray in their book *"Cybercrime: Law and Practice"* (2011). According to them, cybercrime is:

"Any criminal activity that involves a computer, a networked device, or the internet. This includes a range of offenses from identity theft to hacking, cyberbullying, and the spread of malware."[23]

Cybercrime refers to criminal activities that are carried out using computers, digital devices, or networks, often exploiting the internet as a medium for illegal conduct. It is a broad term that encompasses any unlawful act in which a computer or network plays a central role in facilitating, executing, or concealing the crime.[24] The essence of cybercrime lies in its reliance on digital technology, where perpetrators use the internet and related technologies to conduct illicit activities, bypass security measures, steal information, or disrupt systems. This category of crime is distinguished from traditional forms of crime by its focus on virtual environments, making it more challenging to detect, investigate, and prosecute.[25]

The key characteristic of cybercrime is that it involves some form of malicious intent or illegal action facilitated by digital tools. While the specific methods and targets may vary, the underlying concept remains the same: exploiting the vulnerabilities inherent in digital systems for personal, financial, or other malicious purposes. As digital platforms and networks continue to grow in scope and complexity, cybercrime has become

---

[17] Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: trends and challenges. *International Journal of Innovations & Advancement in Computer Science*, *6*(12), 187-196.

[18] Dashora, K., & Patel, P. P. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the social sciences*, *3*(1), 240-259.

[19] Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

[20] ACCA - https://www.accaglobal.com. (n.d.). *What is ethics? | ACCA Global*. https://www.accaglobal.com/in/en/about-us/regulation/ethics/what-is-ethics.html#:~:text=Ethics%20is%20a%20branch%20of,fines%20or%20even%20jail%20sentences

[21] Goni, O., Ali, N. M. H., Showrov, N., Alam, N. M. M., & Shameem, N. M. A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, *1*(2), 16–24. https://doi.org/10.56556/jtie.v1i2.113

[22] K, N., V K, C., & City College, Jayanagar. (2024). A Study On Cybercrime Its Impact And Awareness Towards Society [Journal-article]. *International Journal of Creative Research Thoughts (IJCRT)*, *12*(4), a23–a25. https://ijcrt.org/papers/IJCRT2404004.pdf

[23] McIntyre, T. (2015b). Cybercrime: towards a research agenda. In *Routledge Handbook of Irish Criminology*. Routledge.

[24] Brush, K., & Cobb, M. (2024, September 3). *What is cybercrime and how can you prevent it?* Search Security. https://www.techtarget.com/searchsecurity/definition/cybercrime

[25] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.

increasingly sophisticated and far-reaching.[26] Unlike traditional crimes, which are often localized to specific geographic areas, cybercrime has a global reach, allowing perpetrators to operate across borders, often without being detected or held accountable.

What sets cybercrime apart from other forms of crime is the way it can occur in a virtual environment that transcends physical boundaries. With the internet providing anonymity, cybercriminals can conceal their identity and location, making it difficult for law enforcement agencies to track and apprehend them. Additionally, the rapid evolution of technology means that cybercriminals are constantly adapting to new security measures, creating new techniques and methods to exploit emerging vulnerabilities.[27] This ongoing game of cat-and-mouse between cybercriminals and security experts makes it particularly challenging to prevent and combat cybercrime.

Another distinctive aspect of cybercrime is its ability to cause widespread harm, often affecting not just individual victims, but entire organizations, industries, and even nations. The consequences of cybercrime can be profound, ranging from financial losses to breaches of privacy, disruption of essential services, and threats to national security. The ability to steal, alter, or destroy critical data in real-time makes the digital realm a high-stakes arena for criminals.[28] As a result, cybersecurity has become a critical field of concern for both private and public sectors, prompting governments, businesses, and individuals to adopt measures to safeguard against the growing risks of cybercrime.

3. TYPES OF CYBER CRIME

In India, as the digital landscape has rapidly expanded, the government has recognized the growing threat of cybercrime and has taken steps to address various forms of online criminal activities. With the increasing reliance on technology for communication, business, and governance, cybercrimes have become more complex and diverse. The Government of India has identified several types of cybercrime, which not only threaten the privacy and security of individuals but also pose risks to national security and economic stability.[29] These include offenses such as hacking, identity theft, online fraud, cyberbullying, and the spreading of malicious software (malware).

To combat these crimes effectively, India has enacted several laws, including the Information Technology Act, 2000, and established specialized cybercrime units to investigate and prosecute offenders. In this context, understanding the different types of cybercrime identified by the Indian government is essential for both prevention and legal redress.

Lets discuss the types of cybercrime as identified by Government of India by Indian Cybercrime Coordination Centre (14C)

3.1. Cryptocurrency Crime-

Cryptocurrency has become an increasingly popular form of digital asset in recent years, attracting millions of users and investors globally. However, the rise of cryptocurrencies has also led to a surge in cybercrimes related to digital currencies, as criminals exploit the anonymity, decentralized nature, and technological vulnerabilities associated with blockchain and crypto platforms. Some of the most common types of cryptocurrency-related crimes include cryptojacking, crypto mining scams, cloud mining scams, and cryptocurrency investment frauds.[30] These illicit activities pose significant risks to individuals, businesses, and the broader financial ecosystem.

With 840 incidents filed, India came in fifth place worldwide in terms of complaints pertaining to cryptocurrencies, according to the FBI's study.But with $44,054,244 in losses, India was among the top 10 nations in terms of overall financial impact.[31]

---

[26] Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of communication engineering & Systems*, *11*(1), 1-6.

[27] Sharma, V., Manocha, T., Garg, S., Sharma, S., Garg, A., & Sharma, R. (2023, February). Growth of Cyber-crimes in Society 4.0. In *2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 1-6). IEEE.

[28] Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world'policing and law enforcement. *The Police Journal*, *96*(4), 573-592.

[29] Ministry of Home Affairs. (n.d.). *Indian Cyber Crime Coordination Centre (I4C)*. Government of India. https://www.mha.gov.in/division_of_mha/indian-cyber-crime-coordination-centre-i4c

[30] Halder, D., & Saiyed, A. A. (2022). Legal challenges to cryptocurrency and its guardian-less victims in India: a critical victimological analysis. *International Annals of Criminology*, *60*(1), 79-98.

[31] Singh, S. G. (2024, September 10). *US extends work permit renewals to 540 days for immigrants: What this means*. Business Standard. https://www.business-standard.com/finance/personal-finance/us-extends-work-permit-renewals-to-540-days-for-immigrants-what-this-means-124091000206_1.html:contentReference[oaicite:3]{index=3}

The largest losses were from stock trading frauds, with 2,28,094 complaints totaling Rs 4,636 crore. Following this, scams involving investments cost victims Rs 3,216 crore out of 1,00,360 instances, while scams using "digital arrest" caused losses of Rs 1,616 crore out of 63,481 complaints.[32]
According to information obtained by The Indian Express from the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), there were about 12 lakh cyber fraud complaints in 2024. Southeast Asian nations, such as Cambodia, Myanmar, and Laos, accounted for 45% of these.[33]

3.2. Cryptojacking

In a typical cryptojacking attack, cybercriminals use malware or compromise vulnerable systems to install hidden mining scripts. Cryptojacking is particularly harmful because it can slow down the performance of the victim's device, cause overheating, and significantly increase electricity costs. Attackers can spread these mining scripts through malicious websites, phishing emails, or software vulnerabilities. While the victim is not directly harmed financially in terms of stolen assets, the crime can result in increased operational costs and potential damage to hardware or infrastructure, especially for businesses.[34]

3.3. Crypto Mining Scams

Crypto mining scams involve fraudulent schemes designed to deceive individuals into investing in non-existent or fake cryptocurrency mining operations. These scams typically promise high returns on investments for mining cryptocurrencies, often with the claim of operating large mining farms or cloud-based mining operations.[35] Victims are usually asked to invest large sums of money to purchase mining hardware or to rent mining power from a company that claims to have cutting-edge mining technology.

3.4. Cloud Mining Scams

Cloud mining scams are a specific type of crypto mining scam where individuals are encouraged to invest in mining contracts through cloud services, with the promise of mining cryptocurrencies remotely using shared computing power. Cloud mining services typically allow users to rent mining hardware and earn cryptocurrency without needing to buy and maintain physical mining rigs themselves. However, many cloud mining platforms are fraudulent or operate using fraudulent business models.[36] Scammers promote cloud mining services that appear legitimate, offering enticing return-on-investment (ROI) claims.

3.5. Cyber Terrorism:

India, the increasing dependence on digital technologies for government operations, commerce, defense, and personal communication has made the country a target for various forms of cyber threats, including cyber terrorism.[37] Cyber terrorism refers to the deliberate use of technology, particularly the internet and computer systems, to cause harm to a nation's sovereignty, security, or integrity, or to instil fear among its citizens. It has emerged as a significant threat to India, considering its large and expanding digital infrastructure, reliance on technology for key sectors, and vulnerability to geopolitical tensions.[38]
Moreover, in India, the rise of cross-border cyber-attacks, particularly from neighboring countries, highlights the growing risk of cyber terrorism. Hacktivists or terrorist organizations from regions with strained relations with India may use cyberspace to further their political or ideological motives.[39] Cyber-attacks may serve as a tool to destabilize the country, spread misinformation, or disrupt critical infrastructure that the public heavily depends on, such as electricity supply, transportation, or communication networks.[40]

---

[32] Manral, M. S. (2024, November 27). *Rs 11,333 crore lost in just 9 months: A look at the cyber scams that have hit India the worst*. The Indian Express. https://indianexpress.com/article/india/cyber-scams-india-pm-modi-9692771/:contentReference[oaicite:3]{index=3}
[33] The Wire Staff. (2024, November 28). *India lost Rs 11,333 crore to cyber fraud in 2024: Report*. The Wire. https://thewire.in/tech/india-lost-rs-11333-crore-to-cyber-fraud-in-2024
[34] INTERPOL. (n.d.). *Cryptojacking*. https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking
[35] Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, *34*(2), e2255.
[36] Chandran, R., Kumar, S. R., & Gayathri, N. (2021). Designing a locating scams for mobile transaction with the aid of operational activity analysis in cloud. *Wireless Personal Communications*, *117*, 3015-3028.
[37] Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. *Computers & Security*, *102*, 102145.
[38] NAVDHA MAHESHWARI "A Critical Study on Cyber Terrorism and Its Interrelationship with Cyber Security" 2(1) 618-635
[39] Vats, P. (2016). A comprehensive review of cyber terrorism in the current scenario. *2016 Second International Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH)*, 277-281.
[40] Henschke, A. (2021). Terrorism and the internet of things: cyber-terrorism as an emergent threat. In *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism* (pp. 71-87). Cham: Springer International Publishing.

3.6. Email Hacking

Email hacking is one of the most prevalent forms of cybercrime and can have serious personal, financial, and reputational consequences. It involves gaining unauthorized access to a person's or organization's email account to steal information, send malicious emails, or exploit the account for fraudulent purposes.[41]

In 2023, there were over 79 million phishing assaults in India, indicating a sharp increase in online fraud. To counter these risks, the Indian government and companies have implemented cybersecurity safeguards including the Digital Personal Data Protection Act and Zero Trust tactics. [42]

3.7. Tampering with Computer Source Documents

Tampering with computer source documents involves unauthorized access and alteration of the software or data stored on a computer system. This can include modifying, deleting, or altering source code, program files, or databases, usually to gain unauthorized control or to manipulate the system's functionality.[43] Consequences of tampering with computer source documents can be dire, particularly in sectors like finance, healthcare, and government, where data integrity is crucial. Inaccurate data can lead to financial losses, legal issues, or a loss of trust among customers or stakeholders.

3.8. Unauthorized Access / Data Breach

This includes gaining access without permission to sensitive or private information. This is a severe form of hacking, as it often results in the theft or exposure of confidential data such as personal identification information, business secrets, government records, and more.[44]

According to the Ministry of Electronics and Information Technology (MeitY), India experienced 13.91 million cybersecurity incidents in 2022 alone. Over the past five years, there have been 47 major data breaches and 142 data breaches. However, discrepancies between data from different sources suggest that these numbers may only represent the tip of the iceberg, as many incidents go undetected or not officially reported. This highlights the urgent need for more effective reporting mechanisms, better detection systems and increased awareness of cybersecurity risks in the country.[45]

3.9. Online and Social media crimes

Online and social media crimes encompass a wide range of illegal activities conducted through the internet and digital platforms. These crimes exploit technology to harm individuals, organizations, and society.[46] Cyberbullying, for example, involves using the internet or social media to harass or intimidate others, while identity theft occurs when criminals steal personal information to commit fraud. Phishing scams trick individuals into revealing sensitive data through fake communications, and hacking involves unauthorized access to computer systems for malicious purposes. Online fraud can include fraudulent online marketplaces or investment scams, while sexting and revenge porn involve the distribution of explicit content without consent, often used for blackmail or public humiliation.[47]

Fraud accounts for over thirty percent of all cyber crimes in total, and that includes email frauds, internet frauds and fake job offers etc. Financial frauds continue to increase their prevalence, especially those against e-wallets and banking applications. In 2023, the Indian Cyber Crime Coordination Centre (I4C) reported more than 1.5 million occurrences of fraudulent activities in cyberspace, highlighting a sharp increase in the case of internet frauds.[48]

3.10. Online Financial Cybercrimes

Online financial cybercrimes refer to illegal activities that target financial transactions, accounts, or assets through digital platforms. These crimes typically involve cybercriminals using sophisticated techniques to steal money, personal information, or manipulate financial systems. Common forms include phishing, where criminals trick individuals into providing sensitive financial details like credit card numbers or bank account information, and online fraud, such as fake investment schemes, lottery scams, or fraudulent e-commerce

---

[41] Naha, A. (2022). Emerging cyber security threats: India's concerns and options. *International Journal of Politics and Security*, *4*(1), 170-200.

[42] Sharma, D. (2024, April 30). *India recorded over 79 million phishing attacks in 2023, new study suggests*. India Today. https://www.indiatoday.in/technology/news/story/india-recorded-over-79-million-phishing-attacks-in-2023-new-study-suggests-2533497-2024-04-30

[43] Wagner, J., Rasin, A., Heart, K., Malik, T., Furst, J., & Grier, J. (2018, March). Detecting database file tampering through page carving. In *21st international conference on extending database technology*.

[44] Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality (JDIQ)*, *13*(1), 1-33.

[45] Lok Sabha Secretariat. (2024, April 30). *Unstarred Question No. 2418: Cybercrime statistics in India*. Ministry of Home Affairs. https://eparlib.nic.in/bitstream/123456789/1931390/1/AU2418.pdf

[46] Thukral, P., & Kainya, V. (2022). How social media influence crimes. *Issue 2 Indian JL & Legal Rsch.*, *4*, 1.

[47] Almadhoor, L., Alserhani, F., & Humayun, M. (2021). Social media and cybercrimes. *Turkish Journal of Computer and Mathematics Education*, *12*(10), 2972-2981.

[48] Press Information Bureau. (2024, December 3). *Cyber fraud and digital harassment*. Ministry of Home Affairs. https://pib.gov.in/PressReleseDetailm.aspx?PRID=2080186&reg=3&lang=1

websites designed to deceive users and steal funds.[49] Credit card fraud and identity theft are also prevalent, where hackers steal financial data and use it to make unauthorized purchases or withdrawals.

Cyber fraud has been particularly prevalent in FY2024, surpassing the preceding three years in terms of both incidence volume and loss amount. In FY 2024, there were 2,92,800 instances of cyber fraud, up from 75,800 cases in FY 2023. From ₹421.4 crore in FY2023 to ₹2,054.6 crore in FY2024, the amount of money lost increased.[50]

In India, cyber fraud and digital harassment have become critical issues as the country witnesses an exponential rise in online crimes. According to the National Crime Records Bureau (NCRB) and the Indian Cyber Crime Coordination Centre (I4C), cases related to fraud and digital harassment have significantly increased in recent years. Data from the Government of India on fraud cases registered under cyber crimes reveals alarming figures for 2023. The total number of fraud cases registered amounted to 17,470, with the following breakdown: 1,665 cases involving credit/debit cards, 1,690 cases related to ATMs, 6,491 cases concerning online banking frauds, 2,910 cases involving OTP frauds, and 4,714 cases categorized as other types of cyber fraud. [51]

These numbers underscore the growing threat of financial fraud and identity theft in the digital space, with frauds related to credit/debit cards and online banking being the most prevalent. The data highlights the vulnerability of users to cybercrime, driven by factors such as inadequate cybersecurity practices, the widespread use of digital payment systems, and increasing dependence on online services. The government has responded by enhancing cybercrime reporting mechanisms and strengthening laws, but these statistics emphasize the urgent need for increased public awareness, digital literacy, and stricter enforcement of cyber laws.[52]

3.11. Ransomware

This kind of malicious software renders a victim's files unavailable by encrypting them or locking them out of their systems. Once the attack is successful, cybercriminals demand a ransom, typically in cryptocurrency, in exchange for the decryption key or to restore access. Ransomware can infect computers, networks, and even mobile devices through phishing emails, malicious downloads, or vulnerabilities in software. The impact can be devastating, particularly for businesses and organizations, as it disrupts operations, causes financial losses, and damages reputations. [53]

According to a study conducted by the Data Security Council of India (DSCI) and cybersecurity firm Seqrite, there were around 370 million malware attacks identified in India in 2024, with an average of 702 detections per minute. This underscores the scope and severity of the nation's cyberthreats. Additionally, over the course of the year, one million ransomware detections were reported. With over 22% of the attacks, the healthcare sector was the most attacked, followed by the hospitality sector (20%), banking and financial services organizations (17%), education (16%), and micro, small, and medium-sized businesses (8%).[54]

3.12. Child sexually abusive material (CSAM)

Child Sexual Abuse Material (CSAM) refers to any visual depiction, including photographs, videos, or digital content, that involves the sexual exploitation or abuse of minors. This illegal material is often distributed, shared, or accessed online, posing significant risks to children and society. CSAM is considered a form of child abuse, as it involves the exploitation and victimization of minors for sexual purposes.[55] The creation, possession, and distribution of CSAM are serious criminal offenses worldwide, with strict laws aimed at preventing such abuse and protecting children from harm. Efforts to combat CSAM include using advanced technology to track and remove illicit content, alongside international cooperation between law enforcement

---

[49] Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access*, *9*, 163965-163986.

[50] The Hindu. (2025, May 17). *Cyber fraud in banking transactions surges in FY24: Data*. https://www.thehindu.com/data/cyber-fraud-in-banking-transactions-surges-in-fy24-data/article68813626.ece

[51] National Crime Records Bureau & Indian Cyber Crime Coordination Centre. (2024). *Cyber crime statistics: Fraud and digital harassment cases in India* [Data set]. Ministry of Home Affairs, Government of India. https://ncrb.gov.in https://cybercrime.gov.in

[52] Press Information Bureau. (2024, December 3). *Cyber fraud and digital harassment*. Ministry of Home Affairs, Government of India. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2080186

[53] hea, S., & Irei, A. (2025, May 19). *What is ransomware? Definition and complete guide*. TechTarget. https://www.techtarget.com/searchsecurity/definition/ransomware

[54] The Economic Times. (2024, December 4). *India faces 370 million malware attacks in 2024, healthcare and hospitality among top targets: Report*. https://economictimes.indiatimes.com/tech/technology/india-faces-370-million-malware-attacks-in-2024-healthcare-and-hospitality-among-top-targets-report/articleshow/115975435.cms

[55] Salter, M., & Whitten, T. (2022). A comparative content analysis of pre-internet and contemporary child sexual abuse material. *Deviant behavior*, *43*(9), 1120-1134.

agencies. However, the rise of the internet and social media has made it more difficult to detect and prevent these crimes, making ongoing vigilance and prevention efforts essential.[56]

As per the media report published on May 15, 2023, "there have been around 450207 occurrences of child sexual abuse material spreading in 2023."[57] Delhi Police has responded to 3039 of these cases. Currently, "447168 of these cases are being investigation"[58]. In certain instances, an American non-governmental organization has labeled even affectionate photos of young children shot by their fathers, siblings, and siblings in India as child sexual assault. Child sexual abuse content on social media was reported in India in 204056 incidents in 2022, 163633 cases in 2021, and 17390 cases in 2020.[59]

4. CHALLENGES FACED BY LAW ENFORCEMENT AGENCIES IN INVESTIGATION IN INDIA

Law enforcement agencies in India face a myriad of challenges when it comes to conducting investigations, deeply influencing the effectiveness of the criminal justice system. These challenges are multifaceted and stem from a combination of structural, operational, and socio-political factors that complicate the investigative process.[60] With over 1.4 billion people, India is a vast and diverse country, and its law enforcement agencies are often stretched thin in trying to address the needs of a wide-ranging and rapidly growing population. This vastness and diversity create logistical and administrative hurdles, particularly when it comes to coordination between different states and regions, as well as maintaining a consistent standard of law enforcement across the country.[61] The effectiveness of law enforcement agencies is fundamental to the functioning of a democratic society.

4.1. Inadequate Resources

4.1.1. Manpower Shortages

One of the most pressing challenges faced by law enforcement agencies in India is the lack of adequate manpower. According to the Bureau of Police Research and Development (BPR&D), India[62] has approximately 150 police personnel per 100,000 citizens, significantly lower than the United Nations recommended standard of 222. This shortage leads to increased workloads for officers, resulting in burnout, decreased morale, and ultimately, ineffective investigations (BPR&D, 2019).

4.1.2. Insufficient Training

The lack of specialized training in investigative techniques, forensic science, and modern policing methods further hampers the effectiveness of law enforcement agencies. Many officers are not adequately trained to handle complex cases, particularly those involving cybercrime or organized crime. A report by the National Police Commission[63] highlighted that police training in India is often outdated and does not equip officers with the necessary skills to deal with contemporary challenges (National Police Commission, 1980).

4.1.3. Outdated Technology

Many law enforcement agencies in India rely on outdated equipment and technology, which significantly impairs their ability to conduct thorough investigations. The absence of modern forensic tools and databases limits the effectiveness of crime scene investigations and data analysis. A 2020 report by the Ministry of Home Affairs noted that only a fraction of police departments in India had access to advanced forensic laboratories (Ministry of Home Affairs, 2020).[64]

---

[56] Insoll, T., Ovaska, A. K., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. *The Journal of Online Trust and Safety*, *1*(2).

[57] National Human Rights Commission. (2023, April 19). *NHRC notices to the Centre, States, and Union Territories over the reported increase of 250–300% in Child Sexual Abuse Material (CSAM) on social media platforms*. https://nhrc.nic.in/media/press-release/nhrc-notices-centre-states-and-union-territories-over-reported-increase-250-300N

[58] Ibd.

[59] National Human Rights Commission. (2023, April 19). *NHRC notices to the Centre, States, and Union Territories over the reported increase of 250–300% in Child Sexual Abuse Material (CSAM) on social media platforms*. https://nhrc.nic.in/media/press-release/nhrc-notices-centre-states-and-union-territories-over-reported-increase-250-300

[60] Verma, A. ROLE OF LAW ENFORCEMENT AGENCIES IN SOCIETY. *Law & Order Administration*, 1.

[61] Saleem, M. (2024). Role of Investigation Agencies under Criminal Justice System in India. *Issue 1 Int'l JL Mgmt. & Human.*, *7*, 770.

[62] Bureau of Police Research and Development. (2019). *Police personnel statistics in India*. Ministry of Home Affairs, Government of India. https://bprd.nic.in

[63] National Police Commission. (1980). *Report of the National Police Commission*. Ministry of Home Affairs, Government of India. https://mha.gov.in

[64] Common Cause, & Lokniti Programme at the Centre for the Study of Developing Societies. (2023). *Status of Policing in India Report 2023: Surveillance and the Question of Privacy*. https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf

4.2. Corruption

Corruption within law enforcement agencies is a significant barrier to effective investigations. It undermines public trust, distorts the rule of law, and hampers the pursuit of justice.

4.2.1. Bribery and Extortion

Instances of bribery and extortion by police officers are prevalent, leading to a culture of impunity. Victims may be reluctant to report crimes or cooperate with investigations if they believe that officers are corrupt. According to a survey conducted by Transparency International, 69% of respondents in India believed that corruption was widespread in the police force (Transparency International, 2017).[65]

4.2.2. Political Interference

Political interference in law enforcement can compromise the integrity of investigations. Officers may be pressured to manipulate evidence, suppress cases, or protect influential individuals, further eroding public trust in the justice system. A study by the Commonwealth Human Rights Initiative (CHRI) found that political interference is a major impediment to police accountability in India (CHRI, 2016).[66]

4.3. Legal and Procedural Obstacles

The legal framework governing law enforcement in India presents several challenges that complicate investigations.

4.3.1.Complex Legal Procedures

The Indian legal system is characterized by complex procedures and lengthy processes. Investigations can be delayed due to bureaucratic red tape, leading to a backlog of cases and prolonged trials. According to the National Judicial Data Grid, over 3.5 crore cases were pending in Indian courts as of 2020, many of which involve delays in police investigations (National Judicial Data Grid, 2020).[67]

4.3.2.Inadequate Legal Provisions

Existing laws may not adequately address emerging crime trends, such as cybercrime and organized crime. The Information Technology Act of 2000, for example, has been criticized for being outdated and insufficient in tackling modern cyber offenses. A report by the Cyber Crime Investigation Cell of the Delhi Police noted that the existing legal framework does not provide adequate provisions for the investigation and prosecution of cybercrimes (Delhi Police, 2019).[68]

4.3.3. Jurisdictional Issues

India's federal structure leads to jurisdictional complexities that can hinder investigations. Different states may have varying laws and procedures, complicating inter-state investigations and coordination. This lack of uniformity can result in delays and inefficiencies, as law enforcement agencies struggle to navigate the legal landscape across state lines.

4.4. Technological Limitations

The rapid advancement of technology has transformed the nature of crime, posing new challenges for law enforcement agencies.

4.4.1 Cybercrime

The rise of cybercrime presents unique challenges for investigators. Many law enforcement agencies lack the technical expertise and resources to effectively investigate cyber offenses, such as hacking, identity theft, and online fraud. A report by the National Crime Records Bureau (NCRB) indicated a significant increase in cybercrime cases, yet many police departments remain ill-equipped to handle these complex investigations (NCRB, 2020).[69]

4.4.2 Digital Evidence

The collection and preservation of digital evidence require specialized skills and tools. Many investigators are not trained to handle digital evidence, leading to potential mishandling and loss of crucial information. The lack of standardized procedures for digital forensics further complicates the investigation process, as highlighted in a study by the Indian Cyber Crime Coordination Centre (I4C) (I4C, 2021).[70]

4.4.3 Evolving Criminal Tactics

Criminals are increasingly using sophisticated technologies to commit offenses, making it difficult for law enforcement to keep pace. The use of encryption, dark web marketplaces, and advanced evasion tactics

---

[65] Abbink, K., Ryvkin, D., & Serra, D. (2020). Corrupt police. *Games and Economic Behavior, 123*, 101–119. https://doi.org/10.1016/j.geb.2020.07.001

[66] Commonwealth Human Rights Initiative. (n.d.). *Citizens for police reform*. https://www.humanrightsinitiative.org/programs/aj/police/india/police-reforms/citizens_for_police_reform.htm

[67] National Judicial Data Grid. (2020). *Case pendency data in Indian courts*. https://njdg.ecourts.gov.in

[68] Delhi Police, Cyber Crime Investigation Cell. (2019). *Report on challenges in cybercrime investigation and prosecution*. Delhi Police. https://delhipolice.nic.in/cybercrime

[69] National Crime Records Bureau. (2020). *Crime in India 2020: Cybercrime statistics*. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/en/crime-india-2020

[70] Indian Cyber Crime Coordination Centre. (2021). *Standardizing digital forensic procedures: Challenges and recommendations*. Ministry of Home Affairs, Government of India. https://cybercrime.gov.in

complicates investigations. A report by the United Nations Office on Drugs and Crime (UNODC) emphasized the need for law enforcement agencies to adapt to these evolving tactics to effectively combat crime (UNODC, 2021).[71]

4.5. Socio-Political Dynamics

The socio-political landscape in India significantly influences the functioning of law enforcement agencies.

4.5.1 Community Relations

However, strained relations between law enforcement and certain communities can hinder cooperation during investigations. Incidents of police brutality and discrimination have led to a breakdown of trust, making it challenging for officers to gather information and evidence.

4.5.2 Political Pressure

Law enforcement agencies often face political pressure that can influence their operations. Officers may be compelled to prioritize certain cases or protect political interests, undermining the impartiality of investigations. This dynamic can lead to a lack of accountability and transparency, further eroding public trust.

5. SUGGESTIONS FOR HANDLING CHALLENGES IN INVESTIGATING CYBERCRIME IN INDIA

The growing prevalence of cybercrime in India presents significant challenges to law enforcement agencies, judiciary, and policymakers. The rapid expansion of digital infrastructure, combined with increasing rates of cyberattacks, online frauds, and data breaches, has outpaced the capabilities of existing systems and laws designed to combat such crimes. In this section, we discuss various suggestions to improve the effectiveness of investigations into cybercrime in India, focusing on legal reforms, institutional capacity building, technological advancements, and international cooperation.

5.1. Strengthening Cybercrime Legislation

While India's Information Technology Act, 2000 (IT Act) was a pioneering step towards regulating cybercrimes, it needs updates to address emerging challenges. The Act currently faces criticism for not being comprehensive enough and for failing to keep pace with new types of cybercrime. Definitions of cybercrimes need to be more precise. For instance, the term "hacking" should be expanded to cover various techniques used by cybercriminals today.

5.2. Establishment of Specialized Cybercrime Units

One of the key challenges in investigating cybercrimes is the lack of specialized law enforcement agencies that understand the intricacies of cybercrimes. Cybercrimes are often technically complex, requiring specific expertise and knowledge of digital forensics. Every police station should have a dedicated Cybercrime Cell with trained personnel. The Cyber Crime Coordination Centre, established by the government, should be equipped with the resources, tools, and personnel to handle complex investigations.

Officers should undergo continuous training programs on cyber forensics, ethical hacking, and digital investigation techniques. Partnerships with tech experts, universities, and international agencies can be crucial in upskilling investigators.

5.3. Technological Upgradation and Infrastructure Development

The lack of modern forensic tools and technological resources is one of the biggest barriers to successful cybercrime investigations in India. Many law enforcement agencies still rely on outdated systems, making it difficult to trace digital crimes in real time. Indian law enforcement agencies need to acquire cutting-edge digital forensics tools and software for investigating various types of cybercrimes, from ransomware attacks to data breaches. Collaboration with global cybersecurity firms can assist in building this capacity.

The government should invest in real-time monitoring systems that can detect cyberattacks as they happen. Systems that allow authorities to track IP addresses, online transactions, and suspicious patterns can help in the rapid identification of cybercriminals.

5.4. Strengthening Digital Literacy and Awareness

Cybercrimes often succeed due to a lack of digital literacy among the general public, leading to vulnerabilities such as phishing, online scams, and data theft. A lack of awareness of cyber laws also prevents people from reporting cybercrimes. Governments and NGOs should launch widespread awareness campaigns to educate the public about common cybercrimes like phishing, fraudulent online transactions, and data protection. This should include education about cybersecurity best practices such as strong password usage, recognizing phishing emails, and securing personal data.

Integrating cybersecurity and digital literacy into the curriculum from an early age will help build a generation of citizens who are more informed about cyber threats and protective measures.

5.5. Enhancing International Cooperation

Cybercrime is inherently transnational, often crossing borders and jurisdictions. This complicates investigations because criminals can operate from any part of the world, making it difficult for national authorities to track them down. India must strengthen its partnerships with international organizations like

[71] United Nations Office on Drugs and Crime. (2021). *Global report on cybercrime and law enforcement adaptation*. https://www.unodc.org

INTERPOL, Europol, and regional cybersecurity forums to enable better information-sharing and collaboration in investigating cross-border cybercrimes. Bilateral agreements between countries should be developed to facilitate extradition and cooperation in cybercrime investigations.
India should adopt international frameworks like the Budapest Convention on Cybercrime to harmonize laws and regulations with global best practices, enabling better cross-border enforcement.

5.6. Improving Data Privacy and Protection Laws

In many cybercrime investigations, the issue of accessing and utilizing digital evidence is complicated by concerns about data privacy. The absence of strong data protection laws often creates legal hurdles for investigators trying to collect and analyze evidence. India's Personal Data Protection Bill should be passed as soon as possible, ensuring a strong framework for data privacy that does not hinder cybercrime investigations. Clear regulations on how personal data can be used in investigations must be established.
Create clear and efficient protocols for data-sharing between agencies, while ensuring compliance with privacy laws. Investigators should be able to access data relevant to investigations, but in a manner that is transparent and respects individual privacy.

5.7. Collaboration with Private Sector and Cybersecurity Experts

A large part of cybercrime involves attacks on private sector organizations, including businesses, banks, and online service providers. Often, these organizations have more technical expertise than the government but may lack the knowledge or legal frameworks to respond to cyber threats effectively. Establish stronger collaboration between the public sector and private companies (such as banks, e-commerce platforms, and IT firms).
Private cybersecurity firms and ethical hackers should be actively engaged in building the capabilities of law enforcement agencies. The government could incentivize collaborations with firms that specialize in cyber threat intelligence and investigations.

5.8. Proactive Cybercrime Prevention and Early Detection Systems

Preventing cybercrimes before they happen is far more effective than merely investigating them after the fact. However, proactive cybercrime prevention is often under-emphasized in India. Corporations and educational institutions should be required to implement cybersecurity protocols and incident response plans. This will help detect cybercrime at an early stage and mitigate its impact.
India should develop and implement AI-driven early detection systems that can identify suspicious online activity and cyber threats before they escalate. These systems should be capable of analysing data patterns and flagging anomalies for further investigation.

6. CONCLUSION

In conclusion, investigating cybercrime in India presents a complex and multifaceted challenge that requires a coordinated, adaptive, and forward-thinking approach. With the rapid digital transformation of the country, India faces an unprecedented rise in the number and sophistication of cybercrimes. From data breaches, identity theft, and financial frauds to cyber terrorism and online harassment, the scope and variety of cybercrimes are ever-expanding. The existing infrastructure, legal framework, and law enforcement mechanisms, though evolving, are currently ill-equipped to tackle the full scale and complexity of these crimes. To address these challenges effectively, a holistic strategy involving legal reforms, capacity building, technological upgrades, and international cooperation is crucial.
One of the primary hurdles in investigating cybercrimes in India is the inadequacy of existing cybercrime legislation. The Information Technology Act, 2000 (IT Act), despite being a pioneering step towards regulating cyber offenses, has been criticized for its outdated provisions that fail to keep up with the technological advancements and emerging cyber threats. While the Act criminalizes a broad range of cyber offenses, it lacks specific provisions to address newer challenges, such as those related to cryptocurrency crimes, AI-driven frauds, and deepfake technology. Furthermore, cybercrimes often involve multiple jurisdictions, making the enforcement of laws difficult, as legal systems vary from one country to another. Thus, there is an urgent need for comprehensive amendments to the IT Act, not just to update existing sections, but also to introduce new provisions that reflect the current realities of digital crime.
Equally important is the need for stronger cybercrime investigation frameworks within law enforcement agencies. The lack of specialized training in digital forensics among police officers is a significant bottleneck. Cybercrime investigations require specific expertise in data analysis, forensic recovery, and the ability to interpret technical evidence. Yet, many officers are not adequately equipped to handle such cases. Law enforcement agencies, therefore, need dedicated Cybercrime Units at every level of policing, backed by professionals skilled in digital investigations. These units should be equipped with state-of-the-art tools for digital forensics, enabling them to trace, analyze, and preserve electronic evidence. Continuous training and upskilling of officers, combined with strategic hiring from the field of cybersecurity, can ensure that law enforcement agencies stay ahead of cybercriminals' ever-evolving methods.
Another significant challenge lies in cybercrime data collection and storage. The growing volume of data generated by digital devices and platforms often overwhelms investigators, making it difficult to extract relevant information and analyze evidence in real-time. This data deluge requires law enforcement agencies to adopt advanced tools and technologies for big data analysis, AI-driven threat detection, and data storage

solutions that comply with privacy regulations. As cybercriminals often exploit gaps in data protection, it is crucial for law enforcement agencies to be proactive in setting up secure digital infrastructures that can handle sensitive data without compromising on privacy or data protection rights.

In addition to these internal challenges, international cooperation plays a pivotal role in tackling cybercrime. Given the borderless nature of the internet, cybercrimes often span multiple countries, requiring cross-border collaboration for effective investigation and prosecution. Unfortunately, the lack of global harmonization of cyber laws often complicates investigations. For example, an offender operating from one country may exploit legal loopholes in another, making it challenging to track, apprehend, and prosecute them. Strengthening international partnerships through frameworks like the Budapest Convention on Cybercrime and fostering bilateral agreements between nations will be key in addressing these gaps. India should actively participate in international dialogues, share threat intelligence, and build strong partnerships with countries facing similar cybercrime challenges.

Additionally, the issue of digital literacy and awareness among the general public remains a major obstacle. Many people are still unaware of the risks of cyber frauds, phishing attacks, malware, and social engineering tactics used by cybercriminals. Public awareness campaigns are essential to educating citizens about safe online practices, such as using strong passwords, avoiding suspicious links, and safeguarding personal information. Cybersecurity education should not only be limited to the general public but also be integrated into school and university curricula, enabling the next generation to be more cybersecurity-conscious.

In terms of privacy and data protection, the current regulatory framework in India is still developing. The Personal Data Protection Bill, 2019, which seeks to regulate the processing of personal data, is an essential step in addressing the country's data privacy concerns. The bill aims to protect individuals' privacy rights while also enabling data sharing for legitimate purposes, such as law enforcement investigations. The passage of this bill, along with the effective implementation of data protection regulations, will ensure that cybercriminals cannot easily exploit personal data for fraudulent or malicious activities. However, careful consideration must be given to ensuring that data protection laws do not inadvertently impede law enforcement's ability to access critical evidence when investigating cybercrimes.

Moreover, public-private partnerships are increasingly recognized as crucial in combating cybercrime. Many private-sector entities, especially those in the IT, banking, and e-commerce sectors, are frequently targeted by cybercriminals. These organizations possess significant technological expertise and data analytics capabilities that can complement governmental efforts. Establishing partnerships between the government and private cybersecurity firms can help build cyber threat intelligence-sharing platforms, improve incident response systems, and create faster channels for reporting and addressing cybercrimes. Companies should be encouraged to share threat intelligence and collaborate with law enforcement in the fight against cybercrime, particularly when it comes to cross-border incidents.

With these reforms and innovations in place, India can develop a more effective and resilient system for combating cybercrime and securing its digital future. However, the road ahead is long and requires continuous effort, collaboration, and adaptation to stay ahead of the ever-evolving landscape of cyber threats.

References

1. Nischal, A. (2024, May 28). *Combating cybercrime: Strengthening India's legal framework and law enforcement capabilities*. Innovapolis. https://innovapolis.ca/combating-cybercrime-strengthening-indias-legal-framework-and-law-enforcement-capabilities/https://law.asia/india-cybersecurity-legislation-reform/
2. Ministry of Home Affairs. (n.d.). *Details about Indian Cybercrime Coordination Centre (I4C) Scheme*. Government of India. https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme
3. Kumar, S., & Manhas, A. (2021). Cyber crimes in India: Trends and Prevention. *GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ) ISSN (E)*, *9*(5), 2347-6915.
4. Amc. (2013, June 25). Confronting cyber violence in the digital age. *HuffPost*. https://www.huffpost.com/entry/confronting-cyber-violenc_b_3157086
5. Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2022). A review on cyber crimes on the internet of things. *Deep learning for security and privacy preservation in IoT*, 83-98.
6. *Cyber Crime | CID, Crime Branch*. (n.d.). https://odishapolicecidcb.gov.in/?q=node/251
7. Staff, U. W. (2024, May 25). Cybercrime and Social Media: The Unseen Connection. *Subhash Ahlawat*. https://subhashahlawat.com/blog/cybercrime-and-social-media-the-unseen-connection
8. TIMESOFINDIA.COM. (2024, June 16). 10 countries with the highest number of internet users. *The Times of India*. https://timesofindia.indiatimes.com/technology/tech-news/10-countries-with-the-highest-number-of-internet-users/photostory/111014666.cms#:~:text=India%20currently%20ranks%20second%20with,accounts%20for%20692%20million%20people
9. Statista. (2024, May 15). *Internet penetration rate in India 2014-2024*. https://www.statista.com/statistics/792074/india-internet-penetration-rate/

10. Mudaliar, S. (2023, March 30). Police-public ratio stands at 152.80 per lakh person: Govt informs Parliament. *Hindustan Times*. https://www.shindustantimes.com/india-news/policepublic-ratio-stands-at-152-80-per-lakh-person-govt-informs-parliament-101680162971094.html
11. Chudasama, D., & Solanki, L. (2021). Cyber crimes and challenges faced by criminal justice system. *International Journal of Information Security and Software Engineering*, *7*(1), 6-12.
12. Vinay, K. A**.** (2024). *Challenges faced by law enforcement agencies in investigating and prosecuting cyber crimes in India*. ResearchGate. https://www.researchgate.net/publication/383785171
13. Ministry of Home Affairs, Government of India. (2024). *Counter Terrorism and Counter Radicalization Division*. https://www.mha.gov.in/en/divisionofmha/counter-terrorism-and-counter-radicalization-division
14. Common Cause & Lokniti-CSDS**.** (2023). *Status of Policing in India Report 2023: Surveillance and the Question of Privacy*. Common Cause. https://www.commoncause.in/ wotadmin/upload/ SPIR_ 2023_Key_Findings_%28English%29.pdf
15. International Association of Chiefs of Police**.** (2022). *Addressing law enforcement mental health*. https://www.theiacp.org/sites/default/files/2022-09/258181~4.PDF
16. Kumar, N. A., & Pandey, P. (2011). Cyber Crime-Law & Enforcement in India. *International Transactions in Applied Sciences*, *3*(1).
17. Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: trends and challenges. *International Journal of Innovations & Advancement in Computer Science*, *6*(12), 187-196.
18. Dashora, K., & Patel, P. P. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the social sciences*, *3*(1), 240-259.
19. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.
20. ACCA - https://www.accaglobal.com. (n.d.). *What is ethics? | ACCA Global*. https://www.accaglobal.com/in/en/about-us/regulation/ethics/what-is-ethics.html#:~:text=Ethics%20is%20a%20branch%20of,fines%20or%20even%20jail%20sentences
21. Goni, O., Ali, N. M. H., Showrov, N., Alam, N. M. M., & Shameem, N. M. A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, *1*(2), 16–24. https://doi.org/10.56556/jtie.v1i2.113
22. K, N., V K, C., & City College, Jayanagar. (2024). A Study On Cybercrime Its Impact And Awareness Towards Society [Journal-article]. *International Journal of Creative Research Thoughts (IJCRT)*, *12*(4), a23–a25. https://ijcrt.org/papers/IJCRT2404004.pdf
23. McIntyre, T. (2015b). Cybercrime: towards a research agenda. In *Routledge Handbook of Irish Criminology*. Routledge.
24. Brush, K., & Cobb, M. (2024, September 3). *What is cybercrime and how can you prevent it?* Search Security. https://www.techtarget.com/searchsecurity/definition/cybercrime
25. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.
26. Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of communication engineering & Systems*, *11*(1), 1-6.
27. Sharma, V., Manocha, T., Garg, S., Sharma, S., Garg, A., & Sharma, R. (2023, February). Growth of Cyber-crimes in Society 4.0. In *2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 1-6). IEEE.
28. Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world'policing and law enforcement. *The Police Journal*, *96*(4), 573-592.
29. Ministry of Home Affairs. (n.d.). *Indian Cyber Crime Coordination Centre (I4C)*. Government of India. https://www.mha.gov.in/division_of_mha/indian-cyber-crime-coordination-centre-i4c
30. Halder, D., & Saiyed, A. A. (2022). Legal challenges to cryptocurrency and its guardian-less victims in India: a critical victimological analysis. *International Annals of Criminology*, *60*(1), 79-98.
31. Singh, S. G. (2024, September 10). *US extends work permit renewals to 540 days for immigrants: What this means*. Business Standard. https://www.business-standard.com/finance/personal-finance/us-extends-work-permit-renewals-to-540-days-for-immigrants-what-this-means-124091000206_1.html:contentReference[oaicite:3]{index=3}
32. Manral, M. S. (2024, November 27). *Rs 11,333 crore lost in just 9 months: A look at the cyber scams that have hit India the worst*. The Indian Express. https://indianexpress.com/article/india/cyber-scams-india-pm-modi-9692771/:contentReference[oaicite:3]{index=3}
33. The Wire Staff. (2024, November 28). *India lost Rs 11,333 crore to cyber fraud in 2024: Report*. The Wire. https://thewire.in/tech/india-lost-rs-11333-crore-to-cyber-fraud-in-2024
34. INTERPOL. (n.d.). *Cryptojacking*. https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking
35. Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, *34*(2), e2255.
36. Chandran, R., Kumar, S. R., & Gayathri, N. (2021). Designing a locating scams for mobile transaction with the aid of operational activity analysis in cloud. *Wireless Personal Communications*, *117*, 3015-3028.

37. Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. *Computers & Security*, *102*, 102145.
38. NAVDHA MAHESHWARI "A Critical Study on Cyber Terrorism and Its Interrelationship with Cyber Security" 2(1) 618-635
39. Vats, P. (2016). A comprehensive review of cyber terrorism in the current scenario. *2016 Second International Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH)*, 277-281.
40. Henschke, A. (2021). Terrorism and the internet of things: cyber-terrorism as an emergent threat. In *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism* (pp. 71-87). Cham: Springer International Publishing.
41. Naha, A. (2022). Emerging cyber security threats: India's concerns and options. *International Journal of Politics and Security*, *4*(1), 170-200.
42. Sharma, D. (2024, April 30). *India recorded over 79 million phishing attacks in 2023, new study suggests*. India Today. https://www.indiatoday.in/technology/news/story/india-recorded-over-79-million-phishing-attacks-in-2023-new-study-suggests-2533497-2024-04-30
43. Wagner, J., Rasin, A., Heart, K., Malik, T., Furst, J., & Grier, J. (2018, March). Detecting database file tampering through page carving. In *21st international conference on extending database technology*.
44. Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality (JDIQ)*, *13*(1), 1-33.
45. Lok Sabha Secretariat. (2024, April 30). *Unstarred Question No. 2418: Cybercrime statistics in India*. Ministry of Home Affairs. https://eparlib.nic.in/bitstream/123456789/1931390/1/AU2418.pdf
46. Thukral, P., & Kainya, V. (2022). How social media influence crimes. *Issue 2 Indian JL & Legal Rsch.*, *4*, 1.
47. Almadhoor, L., Alserhani, F., & Humayun, M. (2021). Social media and cybercrimes. *Turkish Journal of Computer and Mathematics Education*, *12*(10), 2972-2981.
48. Press Information Bureau. (2024, December 3). *Cyber fraud and digital harassment*. Ministry of Home Affairs. https://pib.gov.in/PressReleseDetailm.aspx?PRID=2080186&reg=3&lang=1
49. Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access*, *9*, 163965-163986.
50. The Hindu. (2025, May 17). *Cyber fraud in banking transactions surges in FY24: Data*. https://www.thehindu.com/data/cyber-fraud-in-banking-transactions-surges-in-fy24-data/article68813626.ece
51. National Crime Records Bureau & Indian Cyber Crime Coordination Centre. (2024). *Cyber crime statistics: Fraud and digital harassment cases in India* [Data set].
52. Ministry of Home Affairs, Government of India. https://ncrb.gov.in https://cybercrime.gov.in
53. Press Information Bureau. (2024, December 3). *Cyber fraud and digital harassment*. Ministry of Home Affairs, Government of India. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2080186
54. hea, S., & Irei, A. (2025, May 19). *What is ransomware? Definition and complete guide*. TechTarget. https://www.techtarget.com/searchsecurity/definition/ransomware
55. The Economic Times. (2024, December 4). *India faces 370 million malware attacks in 2024, healthcare and hospitality among top targets: Report*. https://economictimes.indiatimes.com/tech/ technology/ india-faces-370-million-malware-attacks-in-2024-healthcare-and-hospitality-among-top-targets-report/articleshow/115975435.cms
56. Salter, M., & Whitten, T. (2022). A comparative content analysis of pre-internet and contemporary child sexual abuse material. *Deviant behavior*, *43*(9), 1120-1134.
57. Insoll, T., Ovaska, A. K., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. *The Journal of Online Trust and Safety*, *1*(2).
58. National Human Rights Commission. (2023, April 19). *NHRC notices to the Centre, States, and Union Territories over the reported increase of 250–300% in Child Sexual Abuse Material (CSAM) on social media platforms*. https://nhrc.nic.in/media/press-release/nhrc-notices-centre-states-and-union-territories-over-reported-increase-250-300N
59. National Human Rights Commission. (2023, April 19). *NHRC notices to the Centre, States, and Union Territories over the reported increase of 250–300% in Child Sexual Abuse Material (CSAM) on social media platforms*. https://nhrc.nic.in/media/press-release/nhrc-notices-centre-states-and-union-territories-over-reported-increase-250-300
60. Verma, A. ROLE OF LAW ENFORCEMENT AGENCIES IN SOCIETY. *Law & Order Administration*, 1.
61. Saleem, M. (2024). Role of Investigation Agencies under Criminal Justice System in India. *Issue 1 Int'l JL Mgmt. & Human.*, *7*, 770.
62. Bureau of Police Research and Development. (2019). *Police personnel statistics in India*. Ministry of Home Affairs, Government of India. https://bprd.nic.in
63. National Police Commission. (1980). *Report of the National Police Commission*. Ministry of Home Affairs, Government of India. https://mha.gov.in

64. Common Cause, & Lokniti Programme at the Centre for the Study of Developing Societies. (2023). *Status of Policing in India Report 2023: Surveillance and the Question of Privacy*. https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf
65. Abbink, K., Ryvkin, D., & Serra, D. (2020). Corrupt police. *Games and Economic Behavior, 123*, 101–119. https://doi.org/10.1016/j.geb.2020.07.001
66. Commonwealth Human Rights Initiative. (n.d.). *Citizens for police reform*. https://www.humanrightsinitiative.org/programs/aj/police/india/police-reforms/citizens_for_police_reform.htm
67. National Judicial Data Grid. (2020). *Case pendency data in Indian courts*. https://njdg.ecourts.gov.in
68. Delhi Police, Cyber Crime Investigation Cell. (2019). *Report on challenges in cybercrime investigation and prosecution*. Delhi Police. https://delhipolice.nic.in/cybercrime
69. National Crime Records Bureau. (2020). *Crime in India 2020: Cybercrime statistics*. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/en/crime-india-2020
70. Indian Cyber Crime Coordination Centre. (2021). *Standardizing digital forensic procedures: Challenges and recommendations*. Ministry of Home Affairs, Government of India. https://cybercrime.gov.in
71. United Nations Office on Drugs and Crime. (2021). *Global report on cybercrime and law enforcement adaptation*. https://www.unodc.org