IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.

IJSRA

International Journal of Science and Research Archive

Research Journal Archive, INDIA

(Review Article)

Check for updates

The unseen enemy: Understanding dynamics, challenges, and strategic responses to cybercrime in India: A review

Sachin Singh [1, *] and Manini Srivastava [2]

[1] Research Scholar, Department of Psychology, University of Lucknow, Lucknow, Uttar Pradesh, India.
[2] Assistant Professor, Department of Psychology, University of Lucknow, Lucknow, Uttar Pradesh, India.

International Journal of Science and Research Archive, 2025, 15(03), 655-659

Publication history: Received on 28 April 2025; revised on 08 June 2025; accepted on 10 June 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.3.1783

Abstract

Cybercrime has become an important and growing global problem that puts people, businesses, and governments at serious risk all around the world. Cybercriminal activity has noticeably increased in India, a country that is rapidly transforming digitally under the banner of "Digital India." These increasingly complex attacks target important industries like banking systems, compromise private information, and threaten essential public infrastructure. In order to provide a thorough grasp of the intricate nature of cybercrime in India, this extensive review attempts to consolidate the body of existing academic literature, relevant statistical data, and empirical studies. It explores the different factors that contribute to its expansion, examines its far-reaching effects, and assesses the countermeasures that are now being used. Additionally, this research analyzes new patterns in cybercriminal conduct, shows the substantial enforcement issues authorities confront, and offers a comprehensive evaluation of India's current regulatory frameworks intended to combat cybercrime. In the end, the assessment emphasizes how crucial it is to promote strong stakeholder collaboration, raise public awareness, and enact proactive policy changes in order to successfully reduce the escalating cyberthreat.

Keywords: Awareness; Legal Framework; Cybersecurity; Digital India; Cybercrime

1. Introduction

Digital technology's explosive growth has drastically changed how we connect globally, communicate, and do business in today's world. While there are many advantages to this digital transformation, it has also brought up new vulnerabilities that bad actors, also referred to as cybercriminals, are increasingly taking advantage of (Kumar & Roy, 2024). The term "cybercrime" refers to a wide variety of unlawful actions conducted through digital networks and platforms. These practices include, but are not restricted to, identity theft, financial fraud, cyberbullying, and even highly skilled cyberterrorism. Unfortunately, India's rapidly growing digital presence has come at the same time as a startling rise in cybercrime cases. To protect India's digital landscape, this concerning trend calls for the swift adoption of strong strategic efforts and commensurate legislative measures.

2. Nature and Scope of Cybercrime in India

India has seen an exponential increase in cybercrime in recent years, underscoring the pressing need for stronger cybersecurity defenses. The number of recorded cybercrime complaints has sharply increased, according to data from the Indian Cybercrime Coordination Centre (I4C). The I4C received 26,049 complaints in 2019; by 2023, that number had skyrocketed to nearly 1.5 million. Furthermore, estimates suggest that by 2025, these figures would surpass 2.5 million (The Economic Times, 2025). Numerous prevalent and new cyberthreats are included in this growing trend,

[*] Corresponding author: Sachin Singh

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

including disruptive ransomware attacks, widespread phishing scams, extensive cyberstalking, and significant data breaches. These occurrences show how widespread cyber risks are in India, as they are not limited to urban areas but are progressively impacting both urban and rural populations nationwide (Tripathy, 2025).

3. Key Determinants of Cybercrime

The surge in cybercrime in India is caused by a number of interrelated factors:

- **Technological Advancement**: New vulnerabilities are inevitably created by the quick speed of digitalization and the creation of ever-more complex digital systems. Cybercriminals' strategies to take advantage of flaws in these complex systems are evolving together with technology (Kumar & Roy, 2024).
- **Anonymity**: Offenders can conceal their genuine identities thanks to the internet's and other digital platforms' built-in anonymity. Because of this, it is much more difficult for law authorities to find, follow, and prosecute cybercriminals (Tomer et al., 2023).
- **Economic Incentives**: For many hackers, money is the main motivator. This drive supports a number of criminal behaviors where digital currencies can be used for illegal transactions, such as complex fraud schemes, demanding ransomware attacks, and profitable cryptocurrency scams (Tripathy, 2025).
- **Lack of Awareness**: A major contributing issue is that a sizable portion of digital users do not fully comprehend the fundamentals of cyber hygiene and online safety procedures. Due to this ignorance, people and organizations are more vulnerable to frequent social engineering scams, in which criminals trick victims into disclosing private information or doing acts that jeopardize their security (SBI General Insurance, 2023).
- **Weak Cyber Technology**: A lot of systems, especially older ones, could have antiquated technology and use inadequate encryption techniques. The likelihood of successful assaults is greatly increased by these flaws, which give hackers access points they can exploit (Sarkar et al., 2023).

3.1. Types and Trends of Cybercrime

India's cybercrime scene is dynamic, with a wide range of attack methods and changing patterns:

- **Financial Crimes**: This category accounts for a sizable amount of cybercrime in India and includes actions such as sophisticated phishing attempts intended to steal financial credentials, widespread credit card fraud, and numerous online scams intended to defraud both individuals and businesses (Kumar & Roy, 2024).
- **Distributed Denial of Service and Ransomware**: These sophisticated attack techniques seek to extort money and interfere with services. Distributed Denial of Service (DDoS) assaults overload systems with traffic to render them inoperable, frequently as a form of extortion, whereas ransomware encrypts a victim's data and demands a payment to unlock it (Tomer et al., 2023).
- **Cyberbullying and Online Harassment**: As social media usage has grown, cyberbullying and online harassment have become more common. They target young people in particular on a variety of digital platforms, causing them to experience severe psychological suffering (European Economic Letters, 2023).
- **Cyber Espionage**: This describes illegal actions used to obtain private data from people, businesses, or governments. It encompasses both industrial espionage aimed at obtaining intellectual property and trade secrets as well as state-sponsored attacks directed at national security (Sarkar et al., 2023).
- **Internet of Things -based Attacks**: As smart devices proliferate, attacks on Internet of Things (IoT) devices and smart homes are becoming more frequent. These assaults may allow for surveillance, jeopardize individual privacy, or even serve as gateways to more extensive networks (SBI General Insurance, 2023).

3.2. Impacts of Cybercrime

Cybercrime has a variety of negative effects in India, going beyond monetary losses to affect national security and mental health:

- **Economic Losses**: According to Economic Times (2025), cyber-related damages are expected to cause India to suffer severe financial consequences, with an anticipated loss of ₹20,000 crore in 2025. These losses include productivity losses, recovery expenses, and outright financial theft.
- **Psychological Effects**: Cybercrime victims often endure extreme psychological discomfort, such as anxiety, depression, and trauma, highlighting the offenses' significant human toll (European Economic Letters, 2023).
- **National Security Threats**: Cyberattacks that target vital industries like defense networks, power grids, healthcare systems, and other critical infrastructure present serious risks to national security because they have the potential to compromise sensitive national data and disrupt vital services (Tomer et al., 2023).

- **Loss of Privacy and Trust**: Unauthorized access to personal data and data breaches undermine public and consumer confidence in online services and digital platforms, which may impede the uptake of digital technologies (SBI General Insurance, 2023).

In extreme situations, cybercrimes like identity theft or online harassment have resulted in chronic mental health issues including depression. Some victims have experienced suicide thoughts as a result of the mix of social isolation, financial loss, and emotional pain. (D. Halder, 2021). These studies emphasize the severe and enduring psychological impacts that cybercrimes have on their victims, emphasizing the necessity of public awareness campaigns, support networks, and preventative steps to lessen these effects.

3.3. Legal and Regulatory Framework

The Information Technology (IT) Act, 2000, is India's main piece of legislation that combats cybercrime. It was later revised in 2008 to take into account new and emerging online dangers. But even with these changes, there are still significant holes in the Act's capacity to effectively combat new and complex cybercrimes. These comprise, among other things, crimes such as revenge porn, cyberbullying, and emerging dangers made possible by artificial intelligence (AI) (Subramanian, 2001; Nappinai, 2011; Chawki, 2015). Significant obstacles to the efficient execution of current laws are further highlighted by difficulties with cross-border jurisdictional concerns and a persistently low conviction rate for cybercrime cases (Malik & Mittal, 2023).

3.4. Challenges in Enforcement

Several major obstacles stand in the way of India's cybercrime laws being effectively enforced:

- **Low Technical Capacity**: Insufficient training and experience in digital forensics may cause problems for law enforcement organizations. Their capacity to gather, examine, and properly present digital evidence in court is hampered by this shortcoming (Sood, 2019).
- **Cross-Border Crimes**: Because cybercrime is international in nature, offenders frequently operate from several nations, creating difficult jurisdictional obstacles. The prosecution of criminals is greatly hampered or complicated by these difficulties because international cooperation procedures can be onerous.
- **Reactive Legislation**: One enduring problem with Indian legislation is that it frequently tends to be reactive, changing only in response to particular occurrences or the emergence of new types of cybercrime. The legal system finds it challenging to proactively address and avoid new dangers as a result of this latency (Rathore & Sharma, 2020).

3.5. Awareness and Education

In the battle against cyberthreats, public education and awareness campaigns are unquestionably essential. Research continuously shows that the general public's pervasive lack of digital literacy and training is a major element in the rising prevalence of cybercrime (Sreehari et al., 2018). By putting in place thorough awareness programs in a variety of contexts, such as educational institutions, workplaces, and corporations, users can be greatly empowered with the information and abilities needed to recognize and steer clear of assaults, hence decreasing their overall vulnerabilities.

3.6. Strategic Recommendations

India's complicated cybercrime problem calls for a multifaceted, proactive strategic approach:

- **Strengthening Legal Frameworks**: More proactive legislation that can anticipate and respond to future cyberthreats is desperately needed. Furthermore, data security and privacy would be greatly improved by putting strong data protection rules into place, such to the strict guidelines found in the GDPR (General Data Protection Regulation) (Chaudhury & Paul, 2023).
- **Improving Cybersecurity Infrastructure**: It is imperative to make a sizable investment in state-of-the-art security solutions. To create more robust digital defenses, this involves utilizing developments in blockchain-based security systems, machine learning (ML) for threat identification, and artificial intelligence (AI).
- Encouraging robust cooperation between the public and private sectors is essential. This entails the active involvement of government agencies, academic institutions, and technology corporations to create collaborative strategies, exchange intelligence, and carry out coordinated efforts to counteract cyberthreats (Kulshrestha et al., 2022).
- **Forensics Training and Cybercrime Cells**: It is essential to set up specialist cybercrime cells with cutting-edge equipment and trained workers. According to Tomer et al. (2023), law enforcement and judicial personnel

will be better equipped to investigate and prosecute cyber offenses if they receive thorough training in digital forensics.

- **Youth-Centric efforts**: Targeted youth-centric efforts are required due to the susceptibility of younger populations to specific cybercrimes. The main goal of these programs should be to inform young people about the dangers of identity theft, cyberbullying, and the psychological damage that comes with misbehavior online (European Economic Letters, 2023).

4. Conclusion

To sum up, cybercrime in India is a complex socio-economic and psychological issue that impacts all societal levels and is much more than a technological or legal problem. To effectively combat this escalating threat, a comprehensive and integrated strategy is required. Continuous technological development to strengthen digital defenses, proactive legislation reform to stay up with changing cyberthreats, and thorough behavioral education to equip people with cyber literacy must all be seamlessly integrated into this strategy. India can only hope to create a really robust and safe digital society by implementing such proactive, inclusive, and cooperative strategies.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Alajrami, M., & Al-Olayan, M. (2021). A comprehensive study on cyberbullying among university students in Kuwait. International Journal of Educational Technology in Higher Education, 18(1), 1-18.

[2] Borwell, J., Jansen, J., & Stol, W. (2025). The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors. European Journal of Criminology, 0(0). https://doi.org/10.1177/14773708241312506

[3] Chaudhury, A., & Paul, A. (2023). GDPR and India: Understanding the Impact on Data Protection and Privacy. The International Technology Law Review, 2(2), 105-117.

[4] Chawki, M. (2015). Cybercrime in India: An Overview. Computer Law Review International, 6, 178-184.

[5] The Economic Times. (2025, March 1). India to lose Rs. 20,000 crore to cybercrime in 2025. The Economic Times. https://economictimes.indiatimes.com/industry/banking/finance/indian-entities-may-lose-rs-20000-cr-to-cyber-crimes-in-2025-cloudsek-report/articleshow/118651127.cms

[6] Tiwari, S., Rai, S. K., & Sisodia, V. (2023). Analysis of Cybercrime against Indian Youth on Social Media. European Economic Letters, 13(4), 73-79.

[7] Gangwar, S., & Narang, V. (2022). A survey on emerging cybercrimes and their impact worldwide. In Research Anthology on Combating Cyber-Aggression and Online Negativity (pp. 1583-1595). IGI Global.

[8] Kumar, A., & Roy, O. P. (2024). Review On Dynamics Of Cyber Crimes And Awareness: A Study In Bihar. https://doi.org/10.1177/14773708241312506

[9] Kulshrestha, P., Gautam, R., & Singh, A. (Eds.). (2022). Cyber Crime, Regulation and Security: Contemporary Issues and Challenges. Libertatem Media.

[10] Singh, V., Malik, V., & Mittal, R. (2023). Challenges to Cybercrime Reporting, Investigation, and Adjudication in India. In Advancements in Cybercrime Investigation and Digital Forensics (pp. 1-24). Apple Academic Press.

[11] Nappinai, N. S. (2011). Technology laws decoded. LexisNexis India.

[12] Rathore, A. S., & Sharma, P. K. (2020). An Analysis of the IT Amendment Act 2008. International Journal of Law, 6(2), 96-100.

[13] Sarkar, G., Singh, H., Kumar, S., & Shukla, S. K. (2023, August). Tactics, techniques and procedures of cybercrime. In Proceedings of the 18th International Conference on Availability, Reliability and Security. IEEE.

[14] SBI General Insurance. (2023, January 24). The effect of cybercrime on society. SBI General Insurance. https://www.sbigeneral.in/blog/cyber-insurance/cyber-articles/effect-of-cyber-crime.

[15] Singh, R. K. (2015). Cybercrime: Prevention, detection, and response strategies. International Journal of Computer Applications, 114(12), 39-44.

[16] Singh, M., & Singh, H. (2022). Cyber Crime and IT Act 2000: A Critical Review. International Journal of Computer Science and Mobile Computing, 2(4), 400-408.

[17] Sreehari, K., & Abinanth, A. V. (2018). A study of awareness of cyber crime among college students with special reference to Kochi. International Journal of Pure and Applied Mathematics, 119(16), 1353-1360.

[18] Subramanian, S. (2001). Cyberlaws in India: Emerging Trends. Journal of Cyber Law & Information Security, 1(2), 25-37.

[19] Tomer, A., Gautam, J. K., Gupta, J. K., Singh, H., & Deshwal, A. (2023). Psychological, economical, privacy and personnel impacts of cybercrime. Journal for ReAttach Therapy and Developmental Diversities, 6(8s), 114–133.

[20] Tripathy, S. S. (2025). A comprehensive survey of cybercrimes in India over the last decade. arXiv preprint arXiv:2505.23770. https://doi.org/10.30574/ijsra.2024.13.1.1919