**OPEN ACCESS**

Volume: 5

Issue: Special 1

Month: May

Year: 2026

ISSN: 2583-7117

Published: 09.05.2026

Citation:

Lucky Makharia, Ms. Priya Gupta "Shifting Trends in Cybercrime: A Comparative Study of Pre-, During-, and Post-COVID-19 Eras h" International Journal of Innovations in Science Engineering and Management, vol. 5, no. S1, 2026, pp. 124-134.

DOI:

10.69968/ijisem.2026v5Si1124-134



# Shifting Trends in Cybercrime: A Comparative Study of Pre-, During-, and Post-COVID-19 Eras

**Lucky Makharia[1], Ms. Priya Gupta[2]**

*[1] Student, Department of Commerce, St. Xavier's College of Management & Technology, Patna [2] Research Scholar, Department of Commerce, Jai Prakash University, Chapra, Assistant Professor, Department of Commerce, St. Xavier's College of Management & Technology, Patna*

**Abstract**

*The COVID-19 pandemic reflected a major global transformation in the digital landscape, reshaping the individuals, organisations, and governments interact with technology. This rapid digitalisation also led to a parallel surge in cybercrime. The present study analyses the levels and evolution of cybercrime across three phases — pre-COVID, during COVID, and post-COVID — while assessing the effectiveness of digital awareness initiatives in mitigating cyber threats. Before COVID-19 (2018–2019), the average reported cyberattacks remained around 350,000 cases per day, primarily involving phishing and data breaches. During the pandemic, the most crucial phase (i.e., 2020–2021), was when cybercrimes increased by nearly 300%, with ransomware attacks rising by 62%, and phishing emails accounting for over 90% of security breaches, according to the recent data by INTERPOL and WHO. In the post-pandemic period, where some relief was seen, and it was observed that in (2022–2024), cyber incidents declined to some extent by 15–20%, yet new threats such as cryptocurrency scams and AI-enabled fraud have emerged rapidly, demonstrating the adaptive nature of cybercriminals and the lack of knowledge and awareness among the victims. In today's VUCA (Volatile, Uncertain, Complex, and Ambiguous) world, cyber threats reflect the uncertainty and complexity of the accelerated digital transformation. The pandemic amplified this volatility by revealing critical weaknesses in Cybersecurity systems and user preparedness. This study is based on the primary data supported with secondary data from Top Institutions like the WHO & INTERPOL. This paper will help benefit the various policymakers, Cybersecurity professionals, and other researchers to analyse the changing cybercrime patterns and the effectiveness of awareness. It will also help organisations and individuals in order to strengthen their digital security strategies in a VUCA-driven world.*

***Keywords; Cybercrime, COVID-19, VUCA World, Digital Awareness, Cybersecurity, Online Fraud, Post-Pandemic Trends, Comparative Study.***

## INTRODUCTION

The term cybercrime can be broadly defined as the criminal activities involving computers; digital systems, networks, or data serve as the primary tools or targets—has emerged as one of the most pressing global security challenges of the twenty-first century. Cybercrime includes a wide range of offences, such as phishing, social engineering, online financial fraud, identity theft, malware and ransomware attacks, cyber espionage, denial-of-service attacks, and crimes involving illegal or harmful online content (United Nations Office on Drugs and Crime. Global Cybercrime Trends Report, 2021). Earlier the forms of cybercrime can be traced back to the 1960s and 1970s when experimental networks like ARPANET existed. According to a thorough research one of the earliest documented cases is the "Creeper" Worm (1971), often cited as the first self-replicating program for malicious uses of computer code (Bernner, 2010). Cybercrimes can be broadly classified into three categories. First, computer-assisted crimes popularly known as traditional crimes—such as fraud or harassment—are facilitated by digital tools. Secondly it includes computer-focused crimes comprising hacking, malware distribution, and ransomware, which directly targets the systems or data of big companies or MNCs. Lastly it comprise the most sensitive part the content-related crimes, which involve illegal online material, including child sexual exploitation content or extremist

propaganda which is highly vulnerable in nature (United Nations Office on Drugs and Crime. Global Cybercrime Trends Report, 2021). Categorizing cybercrime helps researchers to compare patterns across different phases, especially when one examine the changes influenced by external events such as the COVID-19 pandemic. Pre-COVID cybercrime trends (before 2020) reflected a steady, predictable growth aligned with an increasing digital adoption globally. The COVID-19 pandemic (2020–2021) marked a major turning point in global cybercrime patterns. Lockdowns forced rapid digitization of work, education, healthcare, and commerce, creating massive dependence on digital technology. According to recent study of (INTERPOL, 2020), cybercriminals quickly adapt to the pandemic-related vulnerabilities, leading to a surge in COVID-themed phishing emails, fake health-care websites, fraud schemes involving relief funds, and malicious domain registrations. Majorly the Healthcare institutions, vaccine research centres, and governmental organizations became prime targets for ransomware and espionage due to their critical role easy availability during the crisis (Europol, 2020). The pandemic thus served as a catalyst, accelerating the sophistication of cybercrime operations. The post-COVID period (2022 onwards) demonstrates a consolidation of the trends amplified during the pandemic. Phishing remained abundant, and ransomware evolved into more structured, corporate-like enterprises using Ransomware-As-A-Service (RAAS) models, where experienced developers sell tools to less-skilled attackers for profit-sharing (Secuity, 2023 ). Post-pandemic reports proved that increasingly combining tactics—data theft, extortion, public data leaks, and Distributed Denial-Of-Service (DDOS) threats—to pressurise victims for paying ransoms (ENISA, 2022). This research paper is thoroughly based on the comparative and critical study of pre-, during-, and post-COVID cybercrime trends reveals three major dimensions of change. First the volume and diversity of cyberattacks: pre-COVID threats which were increasing but manageable; during COVID, drastic rise in the number of cases ; post-COVID, the frequency stabilized but the level of crime increased. Second is the critical evolution of cybercriminal strategies, shifting from simple phishing scams which were common earlier to complex ransomware ecosystems and hybrid attacks which are highly difficult to be managed. Third is the response landscape, with organizations and governments strengthening Cybersecurity capacity in the post-pandemic era. The COVID-19 pandemic thus functions as a natural experiment helping researchers to evaluate and illustrate how global crises helped in reshaping digital behaviours, vulnerabilities, and criminal opportunities. This research paper aims to examine these shifting patterns of cybercrime across the three phases—pre-COVID, during COVID, and post-COVID—offering insights that can guide future policymaking, Cybersecurity strategy, and academic research.

## OBJECTIVES

1. To analyse changes in cybercrime patterns across the three COVID-19 phases.

2. To assess the impact of digital awareness initiatives taken by the government on reducing cybercrimes.

## LIMITATIONS

The study was conducted within a limited time frame and focused on only on respondents' from Patna, Bihar which restricts the availability of the findings of various other geographical territories. Different forms of socio-economic and technological conditions in other areas may produce different results in forms of facts figure and opinion. The availability of the primary data was limited and its reliability depends largely on respondent's awareness and active participation. It was difficult to isolate Covid-19 as the sole factor influencing the cybercrime and its patterns because of several social, economic and technological factors were involved simultaneously. Rapid digital transformation, increased internet usage, evolving cyber threats and changes in cybersecurity policies also influenced cybercrime patterns. Therefore these limitations should be considered while Interpreting the findings and drawing conclusions.

## RESEARCH METHODOLOGY

This study employs a mixed-method research approach to examine the shifting trends in cybercrime across the pre-, during-, and post-COVID-19 periods. The research comprises both qualitative and quantitative data for a comprehensive analysis. Primary data were collected through Personal Interaction with the help of structured questionnaires and in-depth interviews conducted among academicians, bankers, self-employed individuals, working professionals, and students from various sectors in Patna, Bihar. These responses came out with valuable insight into evolving cybercrime patterns and public awareness levels. In addition to it, some secondary data from renowned sources, such as government reports, journals, and policy documents, to support the findings and key reasons associated with it. This combination of primary and secondary data facilitates a holistic understanding of how Shifting Trends in Cybercrime with the evolution of time, a critical comparison of pre-, during-, and post-COVID-19

Eras and a holistic understanding of how digital awareness initiatives have influenced the reduction of cybercrimes in the post-COVID era.

## LITERATURE REVIEW

According to recent study of Kumar and Sharma (2021), available on Research Gate titled Cyber Crime Trends Before and During COVID-19 Pandemic: A Global Perspective indicates that cybercrime experiences a significant surge during the COVID-19 pandemic due to increase in number of digital dependency where phishing attacks, ransomware incidents, and online fraud increased by more than 60% during lockdown periods. This study mainly highlights the impact of how remote working environments leading to vulnerabilities due to weak cybersecurity infrastructure and network bandwidth. Pre-COVID-19 cybercrime was more planned, structured and target based, whereas during the pandemic, attackers shifted to opportunistic strategies exploiting lack of knowledge, fear and uncertainty. Lastly, the authors argue that the lack of preparedness and readiness among organizations accelerated the growth of cyber threats, making cybersecurity a strategic priority post-pandemic.

A study by Singh et al. (2022) on Impact of COVID-19 on Cybersecurity: Emerging Threats and Challenges explores the changing trends and pattern of cyber threats during COVID-19, focusing on emerging attack vectors such as Zoom-bombing, fake healthcare websites, and vaccine-related scams. This literature reveals that cybercriminals usually adapt to socio-economic changes, targeting individuals and organizations through social engineering techniques. Compared to the pre-COVID era, where attacks were largely financially motivated, pandemic-period crimes were psychological in nature. This study also discusses how the post-COVID phase continues to witness threats combining traditional hacking with incorporation of AI-based tools. The research highlights the significance of adaptive cybersecurity frameworks and policy interventions to counter evolving risks.

Research by Verma and Patel (2023) on Comparative Analysis of Cyber Crime Patterns in Pre- and Post-Pandemic Era provides a comparative analysis of cybercrime trends before and after the outbreak of COVID-19. The findings suggest that during its initials cybercrime was concentrated on corporate data breaches, the post-pandemic era has seen a democratization of cybercrime affecting individuals, small businesses, and educational institutions. The study identifies a notable increase in identity theft and digital payment frauds post-COVID due to the widespread adoption of online transactions and adaptation to it on wider horizon. Additionally, the authors highlight the role of digital literacy in reducing the level of cyber risks. The literature concludes that cybercrime has become more decentralized and scalable in the post-pandemic digital ecosystem.

According to a systematic review conducted by Ali and Khan (2021), on Ransomware and Phishing Attacks during COVID-19: A Systematic Review ransomware and phishing attacks became the most dominant forms of cybercrime during the COVID-19 period. This research analyses multiple datasets and reports from cybersecurity agencies, revealing that healthcare institutions were primary targets which were highly focussed sector due to their critical role during the pandemic. The study also indicates that post-pandemic cybercrime continues to rely on similar strategies but with enhanced sophistication of AI driven tools, including automation and integration. The authors recommend strengthening institutional cybersecurity, laws, policies thereby promoting international cooperation.

The study by Gupta and Mehta (2022) on the title of the research Digital Transformation and Cyber Crime Evolution in the COVID-19 Era examines how rapidly digital transformation contributes to the development and growth of cybercrime. The literature suggests that the sudden shift to online platforms in education, banking, and business operations created new opportunities for cybercriminals. Pre-pandemic systems were not designed to handle such large-scale digital engagement, leading to increased vulnerabilities. The research also highlights that post-COVID-19 cybercrime is more technology-driven; involving advanced persistent threats and data exploitation techniques. The authors conclude that continuous monitoring, investment in cybersecurity infrastructure, and user awareness are essential to address future cyber threats effectively.

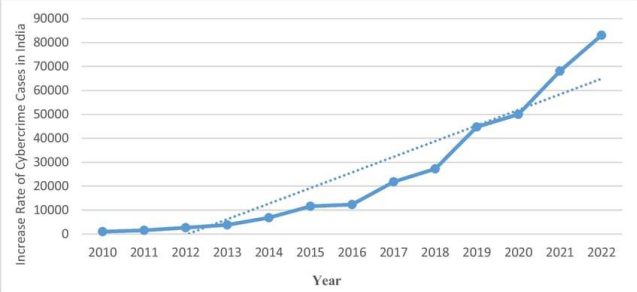
## ANALYSIS AND DISCUSSION

### Evolution of Cybercrime in India

With the passage of time Cybercrime in India has evolved slowly over the last two decades, shaping the country's digital transformation. This evolution led to social, legal, and technological dynamics involving majorly early internet adoption, emergence of IT laws, evolving various cyber-offences, and shifting of motives (from hacking to fraud and exploitation). Cybercrime in India has gone through a profound transformation over the last few decades. This paper traces the evolution of cybercrime in India from

its Initial stage to its present-day scale and complexity, examining legal frameworks, institutional responses, and persistent challenges.

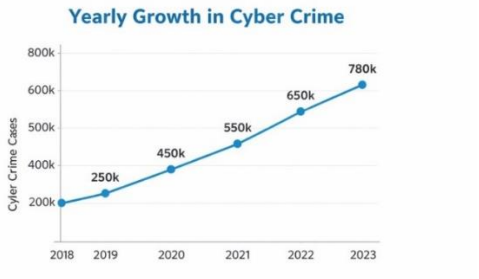
The beginning of cybercrime in India can be easily traced with the help of footprints of cybercrime in the late 1990s, a period characterised by low internet connectivity but increasing the usage of computers in business operations. One of the first cases, named Akash Arora (Delhi High Court, 1999), involved early recognition of cyber-related disputes. Around the same period, India faced its first reported incidents of hacking and email fraud. As businesses and individuals began adopting digital communication tools, the government recognized the need for a legal framework to address computer-related offences. This is because of the Information Technology Act, 2000, India's first comprehensive cyber law, which came into effect on 17th October, 2000 (IT ACT , 2000). The Act was introduced with the prime objective of criminalised hacking, unauthorised access, data theft, and digital impersonation, forming the foundation of India's cyber-legal ecosystem.




In the mid-2000s as internet usage expanded sharply, with the advancement and upgradation of cyber cafés, online banking, e-commerce, and social networking platforms, cyber offences diversified from basic hacking to phishing, identity theft, credit card fraud, cyber stalking, and online harassment. The 2008 amendment to the IT Act strengthened the capacity of internet users to make response to these threats by introducing the provisions for cyber terrorism, availing data protection obligations against intermediaries, and expanded definitions of digital offences as per the law in the record of cybercrime (Singh, 2025).

However, after 2010, a materialistic rise was observed in cyber offences. The launch of Digital India platform in 2015 further increased the level of internet penetration, leading to increase in exposure of citizens to online risks and crimes. National Crime Records Bureau (NCRB) data reflect these shifts clearly. In 2018, India faced 27,248 cybercrime cases, a number which is more than tripled to 86,420 cases in the year 2023, marking one of the largest increases in cyber offences in the country's history (Indian Express, 2025).

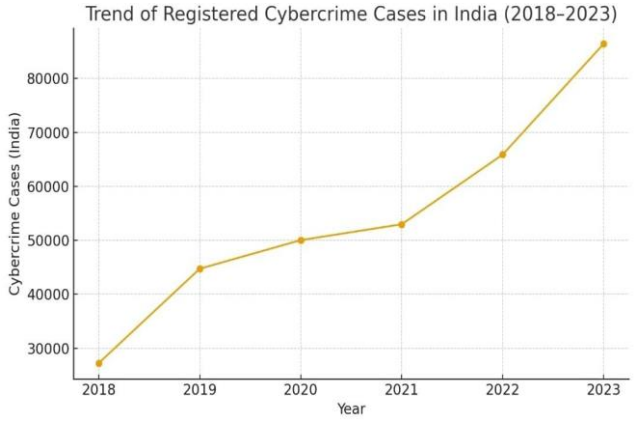
A major turning point was observed in this evolution with the positivity of establishing Indian Cyber Crime Coordination Centre (I4C), approved in 2018 and formally inaugurated in month of January 2020 (Press Information Bureau, 2020). I4C was designed as a base on the seven-pronged national framework to address cybercrime comprehensively. However, even with improvements in reporting technology, challenges continue to exist, including under-reporting in rural regions, a mismatch between complaints and registered FIRs, and shortages of trained cyber forensic experts across states (Press Information Bureau, 2020).




With the beginning of lockdowns all over the world in March 2020, millions of households and businesses were abruptly affected and forcefully shifted to digital platforms, which deliberately pushed individuals to remote work condition, telemedicine, digital learning platforms, and online payment systems expansion. According to the research of NCRB data reveals, cybercrimes related to fraud and extortion saw a consistent year-on-year growth during the pandemic. The pandemic also witnessed the emergence of various types of cyber offences, including Zoom-bombing, credential harvesting through fake COVID-related apps, and data breaches involving health information systems (Marnal, 2025). This period marked the vulnerability of both individuals and institutions in crisis-driven digital environments.

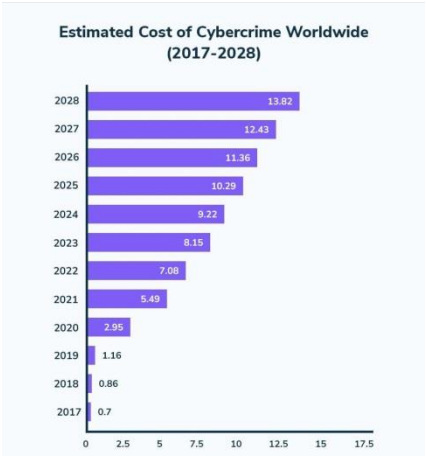
The extent cybercrime in India is clearly visible when we evaluated the trend reflected in the above given continuous time-series graph, as seen in the chart generated for the period 2018 to 2023. Cybercrimes increased from 27,248 cases in 2018 to 86,420 cases in 2023, reflecting increase in digital usage and greater opportunities for offenders to affect

the users. One of the most significant changes is observed between 2018 and 2019, when the number of cases surged from 27,248 to 44,735 due to improved reporting mechanisms and initiatives like the National Cyber Crime Reporting Portal increasing the level of awareness and literacy among the victims. During the COVID-19 years, the number of cases continued to rise from 50,035 in 2020 and 52,974 in 2021—as a result of shift from remote work, online learning, and digital payments created more vulnerability in the VUCA World. The rise accelerated further, with cases jumping to 65,893 in 2022 and peaking at 86,420 in 2023, marking a 31% increase in a single year.




The upward trend not only symbolizes the growth in numerical terms but also reflects a shift in the nature and context of cyber-offences. The trend also highlighted India's growing number of digital risks cases, marked by low conviction rates of the victims, limited forensic capabilities, and inadequate level of Cybersecurity awareness among new internet users. This trend assures the digital users that cybercrime is no longer a risk but a persistent, systemic challenge and drawback of the advance digital literacy that requires stronger legal frameworks, enhanced cyber-forensic capability, and widespread public education.

The chart illustrates a dramatic and continuous rise in global cybercrime costs from 2017 to 2028. Beginning at $0.7 trillion in 2017, the financial impact grows sharply each year, reaching $2.95 trillion in 2020, $7.08 trillion in 2022, and a projected $13.82 trillion by 2028. The growing dependence on digital systems, remote work, and emerging technologies has expanded vulnerabilities, enabling cybercriminals to inflict greater financial damage. Overall, the trend emphasizes the critical need for advanced cybersecurity strategies, global cooperation, and stronger preventive mechanisms to mitigate escalating risks.




**Impact of Increased Digital Dependency**

**Digital Dependency across the Three Phases of COVID-19 on Cybercrime**

The COVID-19 pandemic played a vital role in the process of reshaping global digital behaviour, resulting in sudden increases in online communication, digital payments, remote work, telemedicine, e-commerce, and other facilities like online education. This unplanned digital expansion altered the remarkable ecosystem of cybercrime across globe, transforming both the scale and the nature of cyber threats. Evaluating the pre-COVID, during-COVID, and post-COVID phase's critically reveals how cybercriminal activity evolved along with the rise of digital dependency and how these major changes led to increase in the number of cybercrime incidents, financial losses, and victim vulnerability.

| Year | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|---|---|
| Reported Cases | 27,248 | 44,735 | 50,035 | 52,974 | 65,893 | 86,420 |

(Sources: NCRB reporting summarizes and national press coverage summarizing the cybercrime in India reports).

**Pre-COVID 19 (Before 2020): Gradual level of Growth and Establishment of the Cybercrime Patterns**

Before the arrival and onset of the pandemic, cybercrime was increasing globally, driven by expansion in the level of internet penetration, adoption of various online financial services by the users, and the development of professional criminal networks. Europol's Internet Organised Crime Threat Assessment (IOCTA) marked that before 2020, cybercriminal activity was usually dominated by business-

email compromise scams (BEC), malware-based crime for the credential theft, and traditional phishing attacks, often targeting enterprises rather than individuals (Internet Organised Crime Threat Assesment, 2023). In India, reported cybercrime cases rose from 27,248 in 2018 to 44,735 in 2019, demonstrating how increase in digital usage is correlated with rising victimization even before the pandemic (NCRB, 2025). Although the number of cybercrime was constantly increasing, the pace was observed to be little slower and more predictable than what emerged during the global health crisis.

**During COVID 19 (2020–2021): Explosive Growth Accelerated by Pandemic-Driven Digital Reliance**

The onset of COVID-19 marked the beginning of the inflection point. Lockdowns and government restrictions forced billions of people worldwide to rely on digital technologies for essential services, communication, and regular employment. This sudden shift created ideal conditions leading to opportunities for cybercriminals and massive threat to users. According to the recent study from INTERPOL's COVID-19 Cybercrime Report found that the first several months of 2020 reflected a widespread abuse of pandemic-related themes, with an increase in malicious domains impersonating health authorities, fake COVID relief portals for assistance, and phishing of emails exploiting the fear and deriving benefit out of it, urgency, and misinformation by websites to its users (INTERPOL, 2020). With the data of recent study from (Internet Organised Crime Threat Assesment, 2023) reported that COVID-19 lockdowns led to a significant increase in attacks which majorly targeted remote-access infrastructure, including virtual private networks (VPNs) along with other cloud services, and collaboration of various tools such as Zoom and Meet and others. This positive shift led to a dramatic rise in account takeover attempts, credential harvesting, and ransomware intrusions. This sudden influx of inexperienced digital users created a large pool of vulnerable targets. In India, cybercrime cases increased from 50,035 in 2020 to 52,974 in 2021, reflecting both rising attacks and improved reporting mechanisms introduced during the pandemic (NCRB, 2025).

**Post-COVID 19 (2022–Present): Persistence, Evolution, and Intensification of Financial Losses**

With the ease in restrictions for mobility after 2021, digital dependency did not decline. The FBI's Internet Crime Complaint Centre noted huge amount financial losses in its 2023 and 2024 annual reports, with total victim's amount of loss reaching an estimated amount of $12.5 billion in 2023 and rising further to $16.6 billion in 2024 (Federal Bureau of Investigation Annual Report, 2024). Importantly, the most drastic increases occurred in investment related fraud, which rose by more than 100% in some categories. Crypto-investment scam most common in nature nowadays also known as "pig-butchering" emerged as one of the most dominant post-pandemic schemes, which enabled the widespread of digital financial activity and weak global regulation of cryptocurrency markets. FinCEN's 2023 alert highlighted how criminals used social media, messaging apps, and digital payment platforms to manipulate victims into fraudulent investments, often resulting in extremely high individual losses (Financial Crimes Enforcement Network [FinCEN], 2023),

National data further illustrate the post-COVID escalation didn't stopped it continues where reported cybercrime cases in India jumped sharply to its peak of 65,893 cases in 2022 and to 86,420 in 2023, representing a more than 3X increase since 2018 (NCRB, 2025). This steep rise not only reflects the real victimization but also developed its reporting infrastructures, including digital complaint portals and cybercrime helplines which were created during and after the pandemic. However, the simultaneous increase in global and national financial losses confirms that the surge is not merely a reporting artifact.

**Interpreting the Trends across All Three Phases of the covid-19:-**

Across all three stages, a clear pattern is noticed which states greater digital dependency, the prime reason is for increases in the number of victimization, particularly for inexperienced users and unsecure organizations. During COVID-19, digital adoption led to ignorance of cybersecurity education and infrastructure, creating a temporary but massive mismatch between exposure and preparedness. Post-COVID, cybercrime high-yield financial deception that leverages the trust and convenience associated with online communication and digital finance.

Awareness campaigns during and after the pandemic helped in one another way to some extent in order to reduce some forms of opportunistic cybercrime, but research emphasizes that user individual education alone cannot reduce or decline the scale of emerging threats. FBI, Europol, and INTERPOL advisories consistently call for multi-layered safeguards such as multi-factor authentication to its users, endpoint that hardens the continuous monitoring, and stronger financial-sector reporting to mitigate fraud,

especially those involving crypto currencies (Europol, 2023; FBI, 2024).

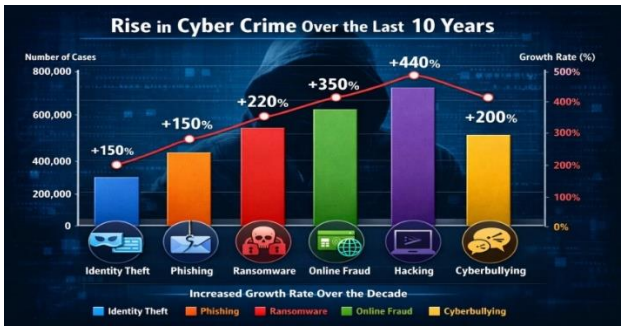
Evaluating the discussion it can be conclude that the increased level of digital dependency associated with the pandemic altered global cybercrime patterns, which accelerated the volume, expansion of targeted demographics, and diversifying financial impacts. The data strongly support the conclusion that cybercrime in the pandemic era was not just a temporary act of evidence but a structural shift with long-term implications for cybersecurity policy and digital governance.

**Types of Cybercrime in India and their Impact**

Cybercrime in India has grown rapidly with expansion in digital connectivity, mobile usage, and internet penetration which continue to expand nationwide. Being the world's second-largest online population, India continuously faces increasing vulnerabilities and complaints related to data theft, fraud, privacy violations, and cyber-attacks targeting individuals, corporations, and majorly public infrastructure.

One of the most relevant forms of cybercrime in India is Financial Cyber Fraud, which majorly involves phishing, vishing, ATM skimming, UPI frauds, and credit-card scams. According to the recent study of National Crime Records Bureau (NCRB), more than half of the cybercrime cases registered annually are financially motivated offences (Crime in India 2023: Statistics. National Crime Records Bureau, Government of India, 2023). The economic impact of financial cyber fraud is highly significant, leading to direct monetary losses thereby reducing trust of consumer in digital payment mechanism, and increasing the burden of additional costs for banks and other fintech companies to upgrade security infrastructure (Rani & Singh, 2022).

Another major category of cybercrime is Identity theft and Data Breaches which represent a situation where attackers often obtain personal data with the linked database, phishing attacks, or malware infections. With the development and technological advancement of e-governance systems, Aadhaar-based authentication, and widespread digital storage of citizen information, India has become a prime location & hotspot for large-scale of data leaks and increasing number of cybercrimes. In this identified amount of data can be misused for SIM card frauds, illegal loan applications, creation of fake social media accounts, and black-marketing of the personal records. Data breaches undermine public confidence in digital governance and exposing vulnerable populations to long-term risks such as credit related fraud and privacy violations (Chaudhary, 2021).




Another important prospect of cybercrime is Cyber Harassment and Online Abuse, including cyberstalking, cyberbullying, Revenge Pornography, and Online Threats, which abruptly affects the women and young internet users. With the recent study from different scholars it is determined that women in India are facing online gender-based violence, particularly on social media platforms (Garg & Sharma, 2020). Such a massive level of harassment had psychological, social, and economic implications, deliberately forcing victims to withdraw from digital spaces, limiting the level of freedom, and affecting mental well-being of an individual.

The sudden rise of Malware, Ransomware, and Hacking Attacks poses increasing threats to India's Corporate and Government Sectors. Ransomware attacks, in general have increased the level of frequency globally where attackers targets sensitive databases, hospitals, educational institutions, and small businesses. Hacking incidents also include website defacements and targeted intrusions by cyber espionage groups, often motivated by geopolitics.

Online Radicalization, Misinformation, and Fake News are one of the additional forms of cybercrime which had huge amount of societal implications in it. During the COVID-19 pandemic, misinformation regarding vaccines, treatments, and government guidelines created confusion and hindered public health efforts (Kadam & Atre, 2021). Addressing misinformation requires strong platform security, digital literacy, and effective level of content moderation mechanisms.

Another serious challenge is cybercrime targeting children, including online grooming, Child Sexual Exploitation Material (CSEM), and trafficking networks operating via encrypted platforms. Exposing children's to such harmful content and various online predators which create long-term psychological and developmental

consequences among them. Although India has strengthened its legal provisions through the Protection of Children from Sexual Offences (POCSO) Act, the complexity and threat of dark-web activities and encrypted networks which makes detection and prosecution extremely difficult.

The combined impact of these cybercrimes on India is multi-dimensional in nature where it begins economically where cybercrime results in substantial financial losses for individuals, businesses, and government organizations. Thereby proceeding socially, cybercrime erodes the trust of users in digital systems, especially among vulnerable populations such as women majorly the elder age group, and rural internet users. Lastly nationally, these threats led to critical infrastructure, defence systems, and governmental databases prone to national security. As India continues to digitalize, strengthening cyber literacy, improving capabilities for law enforcement, and fostering collaboration of public-private cybersecurity for mitigating these risks.

**Awareness Programs and Preventive Measures as Government Initiatives**

The rapid digital transformation, increased internet usage, and dependence on online platforms have made individuals, businesses, and governments more vulnerable to cyber threats. Recognizing these challenges, governments have undertaken several awareness programs and preventive measures to curb the rising trends in cyber-crime across different phases of the pandemic.

**Types of Government Awareness Programs on Cyber Crime (with Facts and Data)**

Governments, particularly in India, have implemented multiple awareness programs to educate citizens and reduce the growing incidence of cyber-crime. These programs have evolved with changing digital behaviour, especially during and after the COVID-19 pandemic.

1. **National Cyber Crime Awareness Campaigns**

The Government of India launched nationwide cyber awareness campaigns under the Ministry of Home Affairs (MHA) to educate citizens about online fraud, phishing, and identity theft. Mass awareness messages are disseminated through television, radio, newspapers, and social media. According to government data, cyber-crime awareness messages reached over 25 crore citizens through digital and print media between 2020 and 2023. These campaigns emphasize safe online behaviour, password protection, and reporting mechanisms.

2. **National Cyber Crime Reporting Portal (NCRP) Awareness Drives**

To promote timely reporting of cyber offences, the government conducted awareness programs highlighting the use of the National Cyber Crime Reporting Portal (www.cybercrime.gov.in). As per official records, the portal received over 31 lakh cyber-crime complaints between 2020 and 2024, reflecting increased public awareness and trust. Campaigns included SMS alerts, social media promotions, and public notices explaining how to report cyber frauds.

3. **Cyber Safety Awareness through Digital India Initiative**

Under the Digital India Programme, cyber safety awareness has been integrated with digital literacy initiatives. Programs such as PMGDISHA (Pradhan Mantri Gramin Digital Saksharta Abhiyan) trained rural citizens on safe internet usage. By 2022, more than 6 crore individuals were digitally trained, with cyber safety forming a key module. The initiative helped reduce vulnerability among first-time internet users in rural and semi-urban areas.

4. **School and College-Level Cyber Awareness Programs**

The government introduced cyber safety modules in schools and higher education institutions through workshops, webinars, and curriculum integration. The Cyber Jaagrookta (Awareness) Diwas, observed on the first Wednesday of every month, focuses on students and young users. Reports indicate that over 10,000 educational institutions participated annually in cyber awareness programs post-COVID.

5. **Social Media and Telecom-Based Awareness Initiatives**

Government agencies collaborate with social media platforms and telecom service providers to spread cyber safety alerts. Telecom operators send regular SMS warnings about OTP frauds, fake calls, and phishing links. Data from the Department of Telecommunications shows that more than 300 crore cyber awareness SMS alerts were sent annually after 2021 to mobile users across India.

6. **Targeted Awareness Programs for Vulnerable Groups**

Special cyber awareness programs have been designed for women, senior citizens, and small businesses. Initiatives such as women-centric cyber safety workshops and senior

citizen digital safety campaigns aim to address specific fraud patterns. Government reports indicate that targeted programs contributed to a 15–20% increase in reporting awareness among vulnerable groups between 2021 and 2023.

**Emerging Challenges in the VUCA World**

The rapid digital transformation of India has significantly increased exposure to cybercrime, creating a highly Volatile, Uncertain, Complex, and Ambiguous (VUCA) environment. With the expansion of digital payment systems, e-governance, online education, and social media usage, cyber threats have emerged as a major challenge to economic stability, national security, and public trust. This section analyses the emerging cybercrime challenges in India through the VUCA framework and discusses their implications.

1. **Volatility: Rapidly Evolving Cyber Threat Landscape**

The cyber threat environment in India is highly volatile, marked by frequent and unpredictable changes in the nature, scale, and sophistication of cyberattacks. India recorded over 265 million cyberattacks in 2025, reflecting a sharp increase in cyber incidents across financial institutions, government platforms, and individual users. Additionally, reported financial losses due to cyber fraud reached approximately ₹22,845 crore in 2024, showing a steep year-on-year rise.

2. **Uncertainty: Difficulty in Identifying Cyber Risks and Attack Source**s

Uncertainty is a major challenge in India's cyber ecosystem, particularly in identifying the source, intent, and scale of cyber threats. Many cybercrimes originate from cross-border networks, making attribution and legal prosecution extremely difficult. Cybercriminals frequently change techniques, using phishing, fake investment schemes, deepfake videos, and malware, which create an uncertainty for both law enforcement agencies and users. Moreover, India reported nearly 1.9 million cybercrime complaints in 2024, yet a significant number remain unresolved due to Anonymous attackers influence in cybercrime activities restricted by limited technical expertise at local enforcement levels due to several Jurisdictional constraints. This uncertainty weakens defence mechanisms and increases public vulnerability.

3. **Complexity: Increasing Interdependence of Digital Systems**

India's digital ecosystem is highly complex due to the interdependence of multiple platforms such as banking, telecom, and e-commerce, healthcare, and government services. A cyberattacks on one system can easily cascade into others. For example, compromise of a mobile device can lead to banking fraud, identity theft, and misuse of government-linked services. The complexity is further intensified by Integration of third-party applications in the fraud with the rapid expansion of cloud-based services leading to growth in number of internet users from rural and semi-urban areas.

4. **Ambiguity: Regulatory Gaps and Unclear Responsibilities:-**

Ambiguity arises from unclear legal frameworks, out-dated regulations, and limited public awareness. India's primary cyber law, the Information Technology Act, 2000, has struggled to keep pace with emerging threats such as AI-driven fraud, ransomware, and deepfake crimes. Victims often face confusion regarding proper redressal mechanism and the roles of banks, telecom companies, and law enforcement in the redressal mechanism.

Cybercrime poses a serious challenge to India's digital future in a VUCA environment. Without proactive and integrated strategies, the volatility, uncertainty, complexity, and ambiguity associated with cyber threats will continue to undermine economic growth and public confidence.

**KEY FINDINGS**

i. **Steady Growth before the Pandemic**: - With the evaluation of National data show a significant upward trajectory in cybercrime cases even before COVID-19: reported cases increased from around 27,248 in 2018 to over 44,546 by 2019, driven primarily by growing internet adoption and early digital financial services.

ii. **Sharp Surge During COVID-19**:- During the pandemic period (2020), several regions saw cybercrime spikes: for example, Gujarat experienced a 64 % increase in registered cybercrime cases in 2020 compared with 2019. With the help of broad analysis it was observed cyber breaches rose sharply (up to 2000 %, according to some expert events) as lockdowns pushed people and businesses online, expanding the attack surface for hackers. Specific categories such as attacks involving minors and exploitation on social platforms also surged, with

some estimates indicating over 400 % increases in cybercrime against children.

iii. **Post-COVID-19 Persistence and Expansion**:- The escalation in digital threats did not reverse after pandemic restrictions eased. In India, reported cybercrime complaints reached approximately 1.91 million in 2024 which is a nearly ten-fold increase since 2019, with financial fraud losses tripling in a short span. National projections estimated global cybercrime damages could exceed by $10.5 trillion annually by 2025, illustrating the economic scale of the problem. Whereas the financial losses associated with cyber fraud in India rose sharply: public reports indicate losses of ₹22,845 crore (about 206 % increase from the previous year) by 2024.

iv. **Regional and Local Impacts**:- In our domestic state, Bihar, cybercrime cases increased rapidly in recent years — jumping from 1,621 cases in 2022 to over 4,450 in 2023, reflecting localized spikes in internet misuse and fraud and expected to increase by 189% by the end of 2027. On the other hand urban centres such as Bangalore reported major cumulative losses (over ₹4,100 crore across 2023-2025), with relatively low recovery rates.

## CONCLUSION

This comparative study of detailed cybercrime trends across 3 eras of covid-19 i.e. before, during, and after the COVID-19 pandemic reveals an accelerated growth or surge rise of digital criminal activity aligned with global socio-technological shifts. However, the outbreak of COVID-19 marked a turning point which accelerated these trends at an increasing rate. The immediate shift to remote work, online education, telemedicine, and demand of digital financial services significantly widened the digital attack surface, creating new opportunities that cybercriminals quickly exploited.

During the pandemic the second stage, cybercrime evolved both in the terms of quantitative and qualitative in nature. Increasing number of cases and filing reports of phishing campaigns, ransomware attacks, online fraud, identity theft, and misinformation operations surged as malicious actors capitalized on public fear, uncertainty, and heightened increase in digital dependency over the users. The rise in reported cases reaching increase over 60 per cent in several regions illustrates how the crisis created an enabling environment for opportunistic and organized cybercriminal networks. Importantly, cyberattacks during this period were not only limited to individuals rather critical infrastructure, healthcare institutions, financial systems, and government agencies also became prime targets by the attackers. This indicates the level that cybercrime transitioned from being primarily an economic issue to a significant threat to national security and public welfare raising a question to all the digital users.

Post-pandemic trends reveal that cybercrime has not reverted to pre-COVID levels. Instead of reduction in number of cases digital criminal activity has stabilized at a higher baseline, with huge amount of financial losses and attack sophistication continuing to grow. The facility or change in work mode from conventional to hybrid work facility by corporates or institutions, with implementation of digital transformation initiatives, and increased reliance on cloud technologies have entrenched new vulnerabilities. Furthermore, cybercriminals have adopted more advanced techniques, including artificial intelligence-driven phishing, deepfake fraud, and highly coordinated ransomware-as-a-service operations.

In conclusion, to this research paper the comparative findings evaluates and suggests the immediate need for strengthening cybersecurity frameworks, action-oriented risk management strategies, and most importantly cross-sector collaboration between government and organizations, where government must work to enhance regulatory mechanisms to reduce the threats and invest in cyber resilience infrastructure, while organizations should prioritize employee training, real-time threat monitoring, and robust data protection systems. If we want to address the increasing impact of COVID-19 on cybercrime, it requires adaptive, forward-looking strategies capable of responding to an increasingly complex and dynamic threat landscape.

## REFERENCES

[1] Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

[2] Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

[3] Europol. (2020). Cybercrime and COVID-19: Impact on criminal activity. European Union Agency for Law Enforcement Cooperation.

[4] Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

[5] Interpol. (2020). COVID-19 Cybercrime Analysis Report. International Criminal Police Organization.

[6] Europol. (2020). Cybercrime and COVID-19: Impact on criminal activity. European Union Agency for Law Enforcement Cooperation.

[7] United Nations Office on Drugs and Crime. (2021). Global Cybercrime Trends Report. UNODC.

[8] ENISA. (2022). ENISA Threat Landscape 2022. European Union Agency for Cybersecurity.

[9] Indian Express. (2025, September 30). NCRB report for 2023: Cybercrimes rise by 31.2%, maximum cases linked to fraud. https://indianexpress.com/article/india/ncrb-report-for-2023-cybercrimes-rise-by-31-2-maximum-cases-linked-to-fraud-10279119/

[10] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

[11] Manral, M. (2025). Cybercrime trends and reporting gaps in India. Indian Express Investigations.

[12] Press Information Bureau. (2020, January 10). Shri Amit Shah inaugurates Indian Cyber Crime Coordination Centre (I4C) dedicates National Cyber Crime Reporting Portal to the nation. Ministry of Home Affairs, Government of India. https://i4c.mha.gov.in/press-release.aspx

[13] Singh, A. (2025). The evolution of India's cyber law: A legislative analysis of The Information Technology Act, 2000 and its amendments. DME Journal of Law, 6(1), 17–26.

[14] https://doi.org/10.53361/dmejl.v6i01.03Press Information Bureau, Government of India, 2020

[15] Mishra, N. K., & Choudhury, A. (2020). Cybersecurity and cybercrimes in India: Challenges and solutions. Springer

[16] Kohli, D., & Saxena, A. (2019). Handbook of cybercrime and digital forensics in India. CRC Press.

[17] Yagati, A. K., Sridevi, M., & Naidu, S. T. (2023). Emerging trends in cybercrime: Challenges and countermeasures in India. South India Journal of Social Sciences, 21(17), 149–155.

[18] Mohanta, R. S. (2017). Evolution and shift in trend of cybercrime: An overview. Cyber Times International Journal of Technology & Management, 10(2), 1–4.

[19] Tripathy, S. S. (2024). A comprehensive survey of cybercrimes in India over the last decade. International Journal of Science and Research Archive, 13(1), 2360–2374. https://doi.org/10.30574/ijsra.2024.13.1.1919

[20] Europol. (2023). Internet organised crime threat assessment (IOCTA) 2023. Europol.

[21] Federal Bureau of Investigation. (2024). Internet Crime Complaint Centre (IC3) annual report 2024. FBI.

[22] Financial Crimes Enforcement Network. (2023). FIN-2023-Alert005: Pig butchering and cryptocurrency investment fraud. FinCEN.

[23] INTERPOL. (2020). INTERPOL COVID-19 cybercrime analysis report. INTERPOL.

[24] National Crime Records Bureau. (2025). Crime in India 2023: Cybercrime statistics (as reported through national summaries). Ministry of Home Affairs, Government of India.

[25] CERT-In. (2023). Annual report on cybersecurity incidents in India. Indian Computer Emergency Response Team.

[26] Chaudhary, P. (2021). Data breach implications in India's digital governance ecosystem. Journal of Information Security Studies, 9(2), 45–58.

[27] Garg, S., & Sharma, R. (2020). Online harassment and gender-based violence in India: A digital perspective. International Journal of Cyber Psychology, 4(1), 23–34.

[28] Kadam, A., & Atre, S. (2021). COVID-19 misinformation and its social impact in India. Journal of Public Health Research, 10(3), 1–8.

[29] NCRB. (2023). Crime in India 2023: Statistics. National Crime Records Bureau, Government of India.

[30] Rani, D., & Singh, A. (2022). The rise of digital payment fraud in India: Trends, causes, and preventive strategies. Asian Journal of Finance & Digital Security, 7(1), 66–79.