Section A-Research paper
ISSN 2063-5346

UNREPORTED CYBER CRIMES IN INDIA

Kiranpal Singh

(Research Scholar, Geeta Global Law School, Geeta University, Panipat)

Dr. Amit Kumar Srivastava

(Supervisor, Professor, Geeta Global Law School, Geeta University, Panipat)

Abstract

Cybercrime, with its ever-evolving complexity, poses a significant threat to the security of individuals, businesses, and the nation of India. The aim of this research paper is to explore the prevalence of unreported cyber crimes in India, despite the emergence of various cybercrime reporting portals and centers. This study delves into the factors that contribute to the lack of reporting, such as the reluctance of individuals to report or lack of awareness of cyber attacks and their consequences.

Unreported cybercrimes in India can be attributed to various causes. These include a lack of awareness about the appropriate authorities to report such incidents, fear of retaliation from attackers, and a lack of faith in the legal system. As a result, many cases go unreported, leading to impunity for the perpetrators and increasing the risk to the public. It is crucial to recognize the severity of cybercrime and its potential impact on an individual's personal and financial security. Reporting cybercrime and taking appropriate measures to prevent similar incidents from occurring can promote a safer and more secure cyberspace.

The paper investigates the types of cybercrime prevalent in India and the potential impacts of unreported cybercrimes on individuals and society as a whole. The study highlights the need for a comprehensive reporting mechanism and the provision of educational programs and awareness campaigns to encourage reporting. Cybercrime is a critical issue in modern society, and India must take action to address the under-reporting of cyber crimes. This research paper also proposes recommendations for addressing the issue, such as promoting awareness about cybercrime and its reporting methodologies, enhancing the efficacy of investigation and prosecution processes, and providing additional resources to law enforcement agencies to combat cybercrime. In the end, India's success in countering the

growing threat of cybercrime will be based on its ability to encourage the reporting of unreported incidents, increase public awareness, and take effective measures to prevent and deter cyber attacks.

Here are some recent resepective Indian judiciary judgements & orders and Central Government issues orders related to unreported cybercrimes in India:

1. The Supreme Court of India directs establishment of national cybersecurity body (2019) - In a landmark judgement in 2019[1], the Supreme Court of India directed the establishment of a national cybersecurity body to tackle cybercrime in the country.

2. Delhi High Court directs police to take cybercrime complaints seriously (2017)[2] - In 2017, the Delhi High Court directed the police to take complaints of cybercrime seriously and to investigate them thoroughly, emphasizing the importance of tackling cybercrime in the country.

3. Central Government issues order mandating reporting of cyber incidents (2021)[3] - In April 2021, the Indian central government issued an order mandating the reporting of all cybersecurity incidents to the Indian Computer Emergency Response Team, with strict penalties for non-compliance.

Keywords

Cybercrime, Cyberspace, Unreported incidents, India, Security, Threats, Awareness, Investigation, Prosecution, National Cyber Crime Reporting Portal, Cyber Crime Volunteers Concept, Indian Cyber Crime, Coordination Centre (I4C), Ecosystem, Academia, Industry, Public, Government, Good Samaritans, Unlawful Content Flaggers, Law Enforcement Agencies, Reporting, Volunteers Program, State Nodal

Introduction

Cybercrime is a growing global threat that negatively affects individuals, businesses, and countries, India included. With the increase of internet usage in India, there is a rise in the number of cybercrimes that occur annually. Despite this alarming trend, not all cases are reported to law enforcement, and even the ones that are reported do not always result in

[1] (The Supreme Court, 2019)
[2] (Delhi Hight Court, 2017)
[3] (Central Government, 2021)

justice for the victims. The purpose of this research paper is to analyze the extent of unreported cybercrime in India and offer solutions to address this issue.

The growth and success of the digital era have also paved the way for the expansion of cybercrime. with such a large user base of more than 100 crore mobiles phones in India it is boosting the Digital India and doing extra ordinary change in peoples life which also result of the cyber crimes are being happening in daily life, India's cyberspace has become a playground for cybercriminals. The Indian government has been taking proactive measures to tackle cybercrime, but unreported cybercrime has been a significant challenge in bringing the cybercriminals to justice. This research paper aims to delve deeper into the issue of unreported cybercrime in India.

A. Defining unreported cybercrime:

Unreported cybercrime refers to online criminal activity that goes undetected or unreported to the relevant authorities. A significant portion of cybercrimes goes unreported in India due to several factors such as lack of awareness, fear of repercussions, and lack of faith in law enforcement agencies.Cybercrime is a rapidly growing problem not just in India but across the globe. Though there have been several measures undertaken in India to fight cybercrime, a significant portion of such crimes go unreported. In this essay, we will look into the issue of unreported cybercrimes in India while also exploring some of the reasons behind the same.

Unreported cybercrimes in India are those that are typically not reported or registered with any law enforcement agency. These could range from identity theft, credit card fraud, phishing scams, ransomware attacks, to cyberstalking, cyberbullying, and revenge porn. In addition, other unreported forms of cybercrimes that are common in India include hacking, online radicalization, and social media abuse[4].

As of 2020, the number of unreported cybercrimes in India is believed to outnumber reported incidents by ten times or more, highlighting the gap in the ability of the government and law enforcement agencies to track and punish cybercriminals. According to a report by the Ministry of Home Affairs, cybercrime cases registered under the Information Technology Act increased by 63.5% in 2019 as compared to 2018. But the actual number of cybercrime

[4] (Bigger Than Ever: Cybercrime Report 2020, 2020)

incidents is believed to be much higher, with many victims not coming forward due to lack of trust in the system, embarrassment, or fear of retaliation.[5]

Another significant issue is the delay and inefficiency in the judicial process, with cybercrime cases taking years to reach a verdict. This slow pace of justice dissuades many victims from filing complaints and exacerbates the problem. Moreover, the cybercriminals who manage to evade arrest continue to operate with impunity, leading to a further increase in cybercrime incidents[6]

B. Definition and types of cybercrime:
Cybercrime refers to criminal activity that occurs through the use of technology, typically involving a computer, network, or the internet. It encompasses unlawful activities such as hacking, phishing, identity theft, cyberbullying, computer viruses, denial-of-service attacks, ransomware, and many others.

Hacking refers to accessing a computer system without authorization to gain confidential information, while phishing involves obtaining sensitive information like login credentials or credit card details by posing as a legitimate entity. Identity theft involves stealing personal information like social security numbers to fraudulently obtain credit or benefits. Cyberbullying is the use of technology to harass, intimidate, or embarrass an individual or group, while computer viruses are malicious programs created to damage computer systems or steal data. Denial-of-service attacks aim to disrupt online services by flooding them with traffic, while ransomware is a type of malware that locks users out of their systems until a ransom is paid. Other types of cybercrime include online harassment, cyberstalking, and cyberterrorism. Cybercrime can cause harm to individuals, corporations, and countries.

C. Importance of reporting cybercrime:
Reporting cybercrime is crucial in preventing the perpetrator from causing further harm and in bringing justice to victims. here are some key points on the importance of reporting cybercrime:

1. Reporting cybercrime helps law enforcement agencies to track and catch the criminals involved in the act.
2. By sharing information, authorities can analyze the crime patterns, identify its severity, and take preventive measures for future cyber threats.

[5] (National Crime Records Bureau, 2020)
[6] (The Hindu, 2020)

3. Reporting cybercrime can help victims recover their financial loss and prevent further damage.
4. It helps to identify new types of cyber threats and helps to educate people to safeguard themselves from future attacks.
5. Reporting cybercrime can help create awareness among people about the necessary precautions they need to take.
6. Information collected from the reports helps law enforcement agencies to investigate and prosecute cybercriminals.
7. It helps to maintain records of such crimes and can be referred to for future similar incidents.
8. Reporting cybercrime can help organizations, businesses, and the government to improve cybersecurity frameworks and make necessary changes to their systems to prevent such incidents.
9. It assists in victim relief and compensation for damages.
10. Lastly, reporting cybercrime can promote a safer and secure digital world for everyone.

D. Scope of the problem in India:

The Internet and Mobile Association of India (IAMAI) and market research firm IMRB International reported that the number of internet users in India has increased from 422 million in 2016 to 566 million in 2018, and 692 million active internet users in India, including 351 million from rural India and 341 from urban Indian. The report estimates that there will be 900 million internet users in India by 2025[7]. This exponential growth of internet use has increased the vulnerability of Indian citizens to cybercrime. According to the National Crime Records Bureau (NCRB), 27,248 cybercrime cases were registered in 2020[8], which showed a 63.5% increase in such cases since 2017.

E. Types of unreported cybercrime in India:

1. Cyberstalking- Cyberstalking is the act of harassing, threatening, or intimidating someone through digital mediums. Cyberstalking is a common form of unreported cybercrime in India, and it's often perpetrated against women.

[7] (Economic Times, 2022)
[8] (NCRB, 2020)

2. Cyberbullying- Cyberbullying is the use of digital mediums to harass, intimidate, and embarrass someone. Cyberbullying is prevalent amongst school-going children and teenagers in India, and it often goes unreported as children are too afraid to speak up.

3. Identity theft- Identity theft is a type of cybercrime where a cybercriminal steals another person's personal information to commit fraud. Identity theft is a common form of unreported cybercrime in India, and it can have devastating consequences for the victim.

4. Financial fraud- Cybercriminals use various means to gain access to a victim's financial information, stealing money through fraudulent means. Financial fraud is a common form of unreported cybercrime in India.

The State of Unreported Cybercrime in India:

A. Statistics and trends:

According to a survey conducted by Norton by Symantec, the true scale of cybercrime in India remains uncertain as many incidents go unreported. The survey found that only 31% of Indian respondents reported cybercrime incidents to the authorities[9]. This unreported cybercrime could lead to a "black hole" of data, skewing perceptions of the scale of the problem in India[10]. Unreported cybercrime could lead to a black hole of data, skewing the perceptions of the scale of the problem in India.

B. Reasons for unreported cybercrime in India:

There are numerous factors that prevent victims from reporting cybercrime to authorities.

1. Fear of Legal Consequences:

The fear of legal consequences is yet another crucial reason behind the high number of unreported cybercrimes in India. Many victims of cybercrime may not report the incidents due to fear of facing legal consequences or getting involved in prolonged legal battles. Even those who do report may face protracted and frustrating legal procedures, leading to a lack of confidence in the system and the unlikelihood of receiving justice.

2. Lack of Awareness and Understanding:

Another reason why many cybercrimes remain unreported in India is due to a lack of awareness and understanding among the general public regarding cyber threats and

[9] (Symantec, 2013)
[10] (Iyer, V., & Dey, J., 2019)

security. Many people may not be aware of the risks associated with using the internet and may not know how to report incidents to the appropriate authorities. This lack of knowledge and understanding can lead to incidents going unreported, posing a significant threat to individuals and businesses alike.

3. Fear of repercussions:

Fear of repercussions is a significant reason why many cybercrimes go unreported in India. Many victims of cybercrime may choose not to report the incident out of fear of the repercussions that may follow, such as retaliation from the perpetrator or damage to their reputation. This fear of potential negative consequences can prevent individuals from seeking help or reporting cybercrimes, contributing to the high number of unreported incidents in the country.

4. Lack of faith in system:

Another significant reason behind the increasing incidents of unreported cybercrimes in India is the lack of trust in the system. Victims of cybercrime often lack faith in the system's ability to protect them and bring the perpetrators to justice. Fear of bureaucratic red tape, lengthy legal procedures, and a lack of accountability often discourage victims from reporting incidents of cybercrime, leading to a low reporting rate. Without decisive action and effective measures, unreported cybercrimes in India will likely remain a serious concern.

5. Unresponsive law enforcement agencies:

Unresponsive law enforcement agencies are also a significant reason why many cybercrimes go unreported in India. When victims of cybercrime make reports to law enforcement, they often receive a slow or no response, which discourages them from reporting similar crimes in the future. This lack of confidence in the justice system not only fuels the number of unreported cybercrimes but also poses a threat to the fight against cybercriminals. With law enforcement agencies failing to meet their expectations, individuals feel helpless and vulnerable, leading to a decline in reporting cases.

6. Perception of Police Inefficiency:

Another possible reason for the high number of unreported cybercrimes in India is the perception of police inefficiency. Victims of cybercrime may not report incidents if

they believe that law enforcement agencies are not efficient enough to handle the problem. This lack of trust in the police can cause victims to feel like their complaints will not be taken seriously. As a result, the problem of underreporting becomes increasingly challenging to resolve.

7. Social Reputation:

Cybercrimes go unreported in India is due to people's unwillingness to report them out of fear of damaging their social reputation. Many people tend to keep quiet as they think that reporting a cybercrime would harm their reputation, and they do not want to become known as a victim. This reluctance to report cybercrimes perpetuates a culture of silence and could enable cybercriminals to continue their illegal activities, thereby making it difficult for law enforcement authorities to track them down and hold them accountable. The need of the hour is therefore to create awareness among people and help them understand that there is no shame in reporting cybercrimes and that it is essential to do so to ensure that justice is served.

8. Lack of communication:

One of the critical reasons for the increasing number of unreported cybercrimes in India is the lack of communication between parents and their children due to the changing dynamics of social media. Most parents are unaware of the technology that their children are using, the privacy settings, and the potential risks that come with it. The proliferation of social media platforms has enabled offenders to exploit young people through grooming techniques which can lead to harassment, cyberstalking, and sextortion. Furthermore, the rise of instant messaging and private communication channels has made it even more challenging for parents to monitor their children's online activities. This lack of communication and awareness has resulted in underreporting of cybercrimes, further compounding issues for law enforcement when it comes to investigating and prosecuting these crimes. It is essential for parents and caregivers to be vigilant and take proactive measures to educate themselves and their children on the safe use of technology and social media.

Consequences of Unreported Cybercrime in India:

A. Impacts on Individuals and Corporations:
Unreported cybercrime is harmful to individuals who fall victim to cyber-attacks, as it can lead to psychological trauma. It can result in loss of information, fraud, identity theft, and financial damage. Similarly, businesses also face financial losses, tarnished reputations, and damage to their intellectual property.

B. Impacts on the Indian Economy:
Cybercrime losses also have a significant impact on the Indian economy. According to a report by Accenture, India's GDP could suffer $1 trillion in accumulative economic growth losses due to cyber threats by 2035.

C. Influence on Global Cyber Threat Landscape:
As the world becomes more digitally connected, the handling of cybercrime becomes a global concern. India's handling of cybercrime affects global cybersecurity efforts in various ways such as legislation and policy-making.

Enabling Reporting and Addressing the Issue:

A. National Cyber Crime Reporting Portal (NCCRP):
The National Cyber Crime Reporting Portal (NCCRP) is a platform launched by the Indian government to facilitate the reporting of cybercrimes in India. The portal enables citizens to report various cybercrimes, including online fraud, hacking, identity theft, and cyberbullying, among others.

The NCCRP aims to bridge the gap between the victims of cybercrime and the law enforcement agencies. By providing a centralized platform for reporting cybercrimes, the portal ensures that incidents are reported and documented, enhancing the accuracy of data regarding cybercrime in India.The portal enables the victims of cybercrime to report incidents anonymously, which encourages individuals to come forward and report any cybercrime they may have experienced. This is especially important, given that many cybercrimes in India go unreported, a fact that skews the perception of the scale of the problem in the nation.The NCCRP system also ensures that the reports submitted to it are promptly forwarded to the law enforcement agencies concerned, making it easier for them to act upon it. By working

closely with victim support groups and law enforcement authorities, the NCCRP aids in developing efficient and effective ways of addressing the issue of cybercrime in India.Overall, the NCCRP plays a vital role in addressing the issue of cybercrime in India by enabling the reporting of cybercrime incidents, enabling prompt law enforcement engagements, and encouraging more significant numbers of victims to come forward.[11]

B. Public-Private Partnerships (PPP):

Public-Private Partnerships (PPPs) can be a useful strategy to enable reporting and address the issue of cybercrime. PPPs are when government organizations and private entities work together to achieve a common goal. In the context of cybercrime, PPPs can help improve reporting and response to cybercrime incidents. PPPs can facilitate the sharing of information between government and private organizations, which can help law enforcement agencies detect and respond to cybercrime incidents. They can also assist in raising public awareness about cybercrime, which can encourage more people to report cybercrime incidents.One successful example of a PPP is the Cyber Swachhta Kendra initiative in India, which is a collaborative effort between the Indian Computer Emergency Response Team[12], public sector organizations, and private companies. The initiative aims to provide free anti-virus and malware tools to Indian citizens, and has been successful in identifying and addressing thousands of cyber threats.PPPs can also address the issue of under-reporting of cybercrime incidents, which is a major challenge in India. By building trust between public and private entities, PPPs can encourage people to report cybercrime incidents. PPPs can also help bridge gaps in understanding and capacity between the public and private sectors in dealing with cybercrime.

In conclusion, PPPs can be a valuable strategy for enabling reporting and addressing the issue of cybercrime in India. By combining the resources and expertise of both public and private entities, PPPs can help improve the overall cyber security landscape in India.

The Indian Government's Ministry of Home Affairs has launched the National Cyber Crime Reporting Portal and introduced the "Cyber Crime Volunteers Concept." The Indian Cyber Crime Coordination Centre (I4C) was established under the Ministry of Home Affairs to serve as the national focal point in the fight against cybercrime. Its mission is to provide a platform for addressing cybercrimes in a coordinated and comprehensive manner. One of

[11] (National Crime Records Bureau., 2021)
[12] ((CERT-In))

I4C's principal objectives is to establish an ecosystem that brings together academia, industry, public, and government in preventing, detecting, investigating, and prosecuting cybercrimes. I4C has created the Cyber Crime Volunteers Program to bring together citizens who are enthusiastic about serving their country on a single platform to contribute to the battle against cybercrime in India. Good Samaritans are encouraged to register as Cyber Crime Volunteers, particularly as Unlawful Content Flaggers, to assist law enforcement agencies in identifying, reporting, and removing illegal/unlawful online content. Individuals who are willing to volunteer in any area that can assist in combating cybercrime are also welcome. The State Nodal will receive applications directly, and they will contact applicants on an as-needed basis.[13]

C. Awareness and Education Programs:
The Indian Government can create awareness campaigns about the different types of cybercrime, targeted towards vulnerable populations, to increase their awareness and knowledge about the reporting mechanisms.The Indian Government plays a crucial role in raising awareness about cybercrime in India. By creating awareness campaigns that focus on different types of cybercrime and how to identify them, the government can educate and inform vulnerable populations about the risks of cybercrime. These campaigns can present the reporting mechanisms and procedures that individuals can follow in case they become victims of cybercrime. By increasing people's awareness and understanding of cybercrime and how to report it, the government can reduce the impact of cybercrime in India and help prevent it from happening in the future.

D. Policing Response Strategies:
The police department can improve their response strategies by creating specialized cybercrime investigation units and by providing adequate resources, technical know-how, and personnel training to tackle cybercrime.

E.Incentives:
To encourage reporting of cyber crimes, incentives can be provided to individuals who come forward with information that leads to the arrest and conviction of cyber criminals.

F. Simplified reporting mechanisms:
The reporting process for cyber crimes can be made simple and user-friendly, to encourage people to report any such incidents without any fear or hesitation.

[13] (Ministry of Home Affairs)

Conclusion:

A. Summary of Research:
Cybercrime is a growing threat in India, with an increase in the number of internet users. However, unreported cybercrime hinders the overall perception of the extent of the issue. A lack of awareness, inefficient policing, and fear of legal consequences are factors that prevent individuals and corporations from reporting cybercrime to authorities. This research emphasizes the importance of the public and private sectors collaborating to create awareness campaigns, investment in cybersecurity research, specialized cybercrime investigation units, and effective cyber- police response strategies.

B. Policy and Practice Implications:
Policymakers need to integrate cybercrime awareness and training into the education system, become more proactive in securing government and business data, enhance technological infrastructure, and tighten existing laws and regulations.

C. Future Research Directions:
Future research should seek to address the effectiveness of programs and initiatives already established to reduce unreported cybercrime cases, examine the causes of fear of legal consequences and perception of police inefficiency, and explore the role of industry and civil society in building stronger, more comprehensive responses to cybercrime.

Bibliography

(CERT-In), I. C. (n.d.). *Ministry of Electronics and Information*. Retrieved from https://www.csk.gov.in/

Bigger Than Ever: Cybercrime Report 2020. (2020, January 23). Retrieved from Cybersecurity Ventures: www.cybersecurityventures.com/cybercrime-report-2020/.

Iyer, V., & Dey, J. (2019). Unreported cybercrimes in India: Its impact and solutions. *International Journal of Scientific and Technology Research , 8(9)*, 2948-2951.

Ministry of Home Affairs, G. o. (n.d.). Retrieved from National Cyber Crime Reporting Portal: https://cybercrime.gov.in/Webform/cyber_volunteers_concept.aspx

Mint, L. (2022, July 29). *India-to-have-around-900-million-internet-users-by-2025.* Retrieved from https://www.livemint.com/news/india-to-have-around-900-million-internet-users-by-2025-report-11659063114684.html

National Crime Records Bureau. (2021). *Cybercrime in India: A comprehensive analysis.* Retrieved from https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%201.pdf

National Crime Records Bureau, M. o. (2020, September 10). *Crime in India - 2019.* Retrieved from www.ncrb.gov.in: www.ncrb.gov.in/sites/default/files/CII%202019%20Volume%201.pdf.

NCRB. (2020).

Symantec, N. b. (2013). *Norton cybercrime report 2013: The human impact.* Retrieved from https://www.nortonlifelock.com/content/dam/nortonlifelock/documents/reports/2013/2013-norton-cybercrime-report.pdf

The Hindu. (2020, February 13). *India Ranks Second for Highest Number of Cyberattacks Globally.* Retrieved from The Hindu: www.thehindu.com/sci-tech/technology/internet/india-ranks-second-for-highest-number-of-cyber-attacks-globally/article30861908.ece.