Cybercrime *en Masse* in the Digital India: A Case Study

Siddhant Chandra

***Abstract:** Cyberspace is essentially a digital universe where people establish their online identities, and it has been expanding rapidly in recent years, mainly due to the widespread adoption of the internet and the rise of smartphones. What began as basic online activities, such as emailing and web surfing, has now grown to influence nearly every aspect of our daily lives, including how we communicate, bank, travel, and shop. The increase in smartphone usage has made the internet more accessible, leading to greater independence, new economic opportunities, and societal shifts. Government programs, such as the Jan Dhan Yojana, and the emergence of digital payment systems following demonetization have further advanced India's journey toward a digital economy. However, this digital shift also brings with it a heightened risk of cybercrimes, especially since many users aren't well-versed in technology. States such as Karnataka and Jharkhand have reported an increase in cyber offences, underscoring the pressing need for enhanced cybersecurity measures and improved digital literacy. This paper examines the growth of cyberspace, its societal implications, and the challenges we face in ensuring secure digital participation.*

***Keywords:** Cyberspace, Digital Transformation, Smartphone Usage, Cybercrime*

Abbreviations:
KYC: Know Your Customer
CDR: Call Detail Report
MoU: Memorandum of Understanding
CCITR: Cyber Crime Investigation Training and Research
DSP: Deputy Superintendent of Police

I. INTRODUCTION

The term "Cyberspace" denotes a virtual space in the digital world, where the existence of individuals is felt, and this Cyberspace is expanding at an exponential rate. Cyberspace emerged with the growth of cyber usage and the Internet boom that occurred over the past few years. The traditional understanding of cyberspace was limited to computers and laptops, and this cyberspace was approached with the help of an internet service provider. Still, in the last few years, internet service providers have increased, and as a result, the internet is now a household feature. Now, almost every person is connected to the internet [1].

People primarily accessed the internet through websites, and their presence in cyberspace was limited to email accounts and some social media accounts, which were restricted by data-sharing policies. However, with the advancement of technology, internet usage has increased. considerably over time, and smartphones have replaced many tasks that were previously performed in one way or another. These uses have brought significant changes in the digital era.

Manuscript received on 26 June 2025 | First Revised Manuscript received on 08 July 2025 | Second Revised Manuscript received on 19 August 2025 | Manuscript Accepted on 15 September 2025 | Manuscript published on 30 September 2025.
* Correspondence Author (s)

Dr. Siddhant Chandra*, Assistant Professor, St. Xavier's University, Kolkata (West Bengal), India. Email ID: subhajit.swati555@gmail.com, ORCID ID: 0009-0009-8648-6761

Cyberspace can now be accessed through smartphones, which is a more accessible option compared to previously used devices like laptops and computers. The number of Smartphone users in 2017 was 468 million, and it is expected to reach around 859 million by 2022 (Report by a joint study of ASSOCHAM and PwC) [2]. In recent years, Smartphones have changed the way people use the internet. The shift from websites to mobile applications has provided access in the digital era as never before, and people are using cyberspace not only for social media but also for banking, messaging, video calls, online shopping, travel booking, and several other purposes across almost all spheres [3].

The technology has increased the total number of smartphone users, resulting in a noticeable impact on society. Smartphones have made people more independent, and this technological advancement has provided job opportunities to individuals. The application of Ola and Uber seems to be a blessing for people who use private transport. The Ola and Uber applications give you the freedom to travel at any point in time. With the proper security check and identification of the driver, this mode of transportation can replace traditional commuting methods, offering both safety to the commuter and cost efficiency. The *Jan Dhan Yojna*, a brainchild of PM Modi's initiative, has allowed all to open bank accounts across India. This move is further strengthened by technological advancements in cyber technology, where one can connect bank accounts with a payment gateway [4]. This revolutionary step is paving the way towards digitalising India, where vendors can accept e-money with ease. This practice will help mobilise the flow of currency and curb the excessive use of hard currency, thereby regulating bank money.

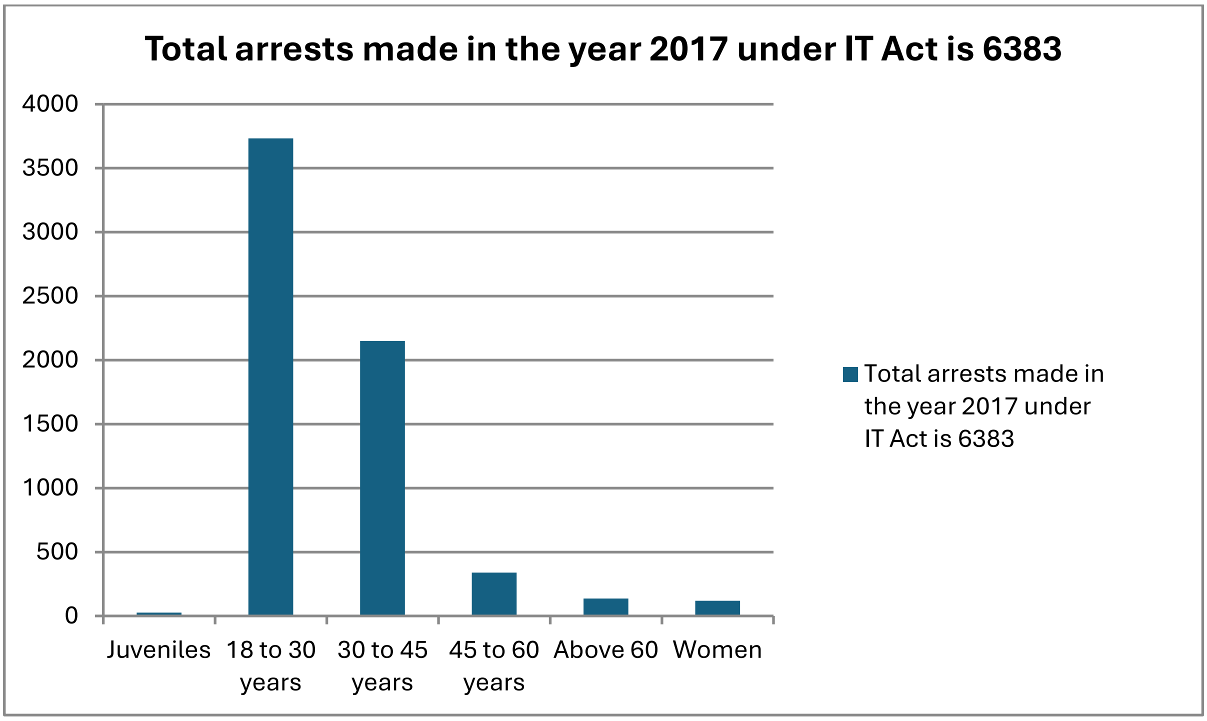
Digitalisation is a phenomenon that has changed the nation's outlook. After demonetisation on 8th November 2016, digital payments have gained prominence in our country; however, adequate security measures have not been specified. The rise of cybercrimes, digital frauds, and economic offences has been unprecedented in recent times. Cybercrime is one of the leading crimes in the crime index, having penetrated deeply into the country, from metropolitan cities to smaller towns. According to the latest NCRB data report, Karnataka is the state most affected by cybercrime, and Bengaluru is the city worst affected. Surprisingly, the State of Jharkhand also finds a place in the infamous lists of these cyber offences. One of the reasons for the commission of these frauds is the lack of basic knowledge among users of these applications [5]. Some users are unaware of the technical aspects of these apps and thus become an easy target for these fraudsters. People use various apps on their mobiles, but are technically negligent.

II. RESEARCH METHODOLOGY

This study employs a doctrinal research methodology, which entails a comprehensive analysis of current laws, policies, judicial decisions, and academic literature related to cyberspace and cybercrime. It focuses on the legal framework that governs digital transactions, data protection, and cyber offences in India. By scrutinising statutes such as the Information Technology Act of 2000, along with its amendments and relevant case law, the research aims to investigate how these legal provisions address the escalating challenges in the digital world. Additionally, it incorporates secondary sources, such as government reports, Law Commission papers, and expert commentaries, to enrich the analysis and pinpoint areas where the law must adapt to technological advancements and bolster cybersecurity.

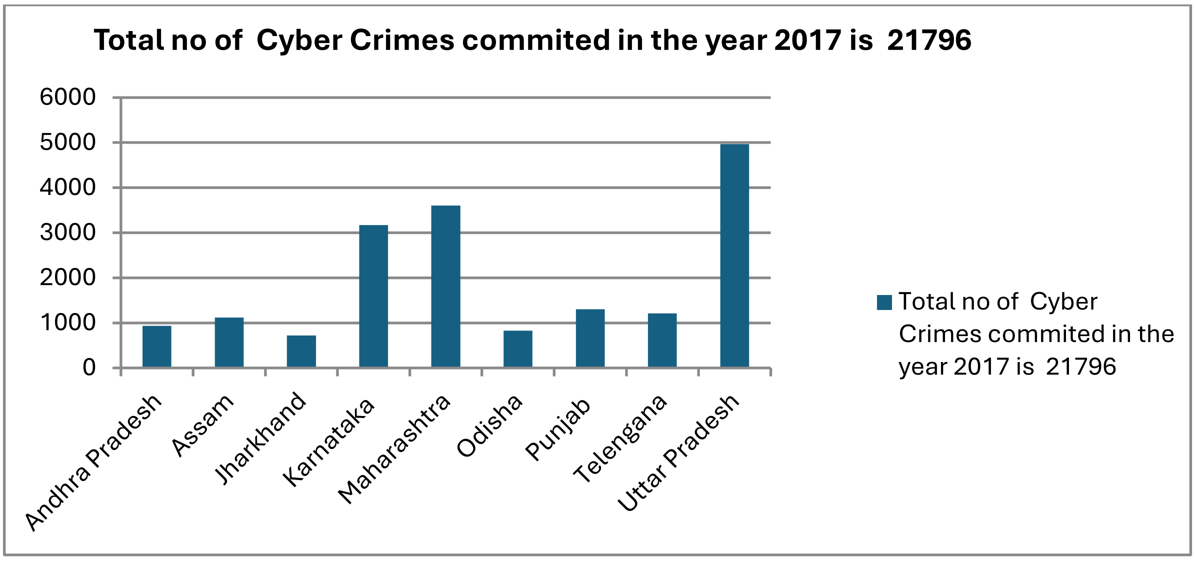
A. Threats in Cyberspace

With the development and overdependence on technology in recent years, cyberspace has become a hotspot for the commission of crime. Many youngsters are prone to indulge in these crimes. These crimes differ from traditional forms of crime, as the latter are often committed by various demographic groups within the population. In contrast, cybercrimes are often committed by young individuals, and in most cases, they are well-qualified individuals who have turned to cybercrime due to economic hardship or unemployment. In the report submitted by the National Crime Record Bureau concerning cybercrimes, it can be inferred that most of the persons in the age group of 18 to 30 years have been arrested in crimes relating to cyber offences, who are willing to make quick money, and cybercrimes have emerged as the easiest method of making fast bucks [6]. Out of the 6,383 persons arrested in 2017, 3,733 persons arrested belong to the age group of 18 to 30 years, i.e., nearly 60 per cent of the people arrested for committing cybercrimes belong to this age group.



[Fig.1: Arrests Made Under the Information Technology Act 2000]

Cybercrimes can be classified as those crimes that involve the computer as an object or as a subject, encompassing crimes that may also overlap with conventional crimes. In other words, any crime that includes the use of a computer for the commission of the crime falls under the purview of cybercrimes. In India, the legislation governing cybercrimes is known as the Information Technology Act 2000, which was amended in 2008. The crimes committed in traditional forms, but using a computer as a medium or remotely, will also fall under the purview of cybercrimes.



[Fig.2: Total Number of Cybercrimes Committed in the Year 2017, Read with all the Relevant Acts]

In the figure depicted above, the total number of cybercrimes committed in 2017 across states and Union territories in India stands at 21796. Uttar Pradesh has emerged as the most notorious state, reporting 4971 cases, which contribute around 29.5% of the total cybercrimes in the country. The population of Uttar Pradesh is also the highest, and owing to its large population, cybercrimes are also the highest in the country. Maharashtra and Karnataka, follow Uttar Pradesh both these states are the financial capital of the country and the Silicon Valley of the country, Mumbai and Bangalore have high rate of cybercrimes or we can say that the people in these states and particularly in Mumbai and Bangalore are aware of their rights and have hence reported the events to the cyber police and cases have been registered. Additionally, crimes committed in these metropolitan areas are also being replicated in smaller cities [7]. Jharkhand ranks ninth, ahead of developed states like Gujarat and Kerala, in terms of the number of cybercrimes committed in the country. The cases reported in different states also have many connections with the state of Jharkhand. However, as the law allows filing an FIR at the place of the incident, cybercrimes do have a link with the state of Jharkhand.

B. Steps Taken by the Investigating Officer After Registration of the First Information Report

When the police station receives information about the cybercrime, the officer handling the case shall ensure, first and foremost, that further damage is not done. In the event of an economic offence, the officer should contact the bank branch by telecommunication means or approach the bank in their capacity and block the account of the victim. They should also ensure that the rightful owner, i.e., the victim, is not unnecessarily harassed for using their account. Similarly, in cases of offences on social media, after the registration of the complaint, the officer shall write to the appropriate authorities to remove the offensive posts as soon as possible, as this would be an ongoing offence.

In the case of economic offences, the officer shall obtain the transaction records and track the route of the money that has been transferred, as well as get details of transactions that have taken place using the said money. After the digitalisation of specific sectors, many digital wallets have entered the market. Although some of these wallets may not be approved by the government, even those that have been approved might not be adhering to the guidelines issued by the Reserve Bank of India and flouting the rules made thereunder. After the inquiry a notice shall be served under section 91 and 102 of the Code of Criminal Procedure 1973 to the concerned nodal officer of the digital wallets, private and all scheduled commercial banks for the supply of the requisite information like the KYC (Know your Customer), associated IP addresses, transaction details, phone number involved and location of the accused in the said transaction to the concerned police personnel in the limited time frame. The police officer shall also attach a copy of the FIR to the email. The police officer shall further request the reversal of the funds to the source account after explaining the chain of transactions which have taken place. Similarly, a notice shall be served under sections 91 and 102 of the Code of Criminal Procedure 1973 to the concerned nodal officer of the mobile companies for obtaining the CDR (Call detail report), CAF, etc, using which the crime was committed, mostly in cases of vishing; such a report is to be mandatorily acquired.

A person posted an advertisement on OLX for selling his Honda City car. A buyer contacted the seller through OLX's messenger. Since the seller was selling his car at a reasonably low price, the buyer was quite interested in the transaction. The buyer requested that the seller show the vehicle, to which the seller replied that the car belongs to army personnel and is being transferred. In a hurry, the officer is offering the car at a throwaway price. He also sent the papers for the vehicle, along with the identity card of the army personnel, and further requested that 55,000 be deposited into an account linked to Paytm Bank. The buyer did so, in anticipation of getting a good deal, but this was a case of fraud, and the seller blocked him on those messengers and vanished. Further, the documents shared were all fake. In this particular case, the police refused to register the case in Ranchi, as it was not a case of cyber fraud. Had the police personnel registered the case and sent a notice under sections 91 and 102 of the Code of Criminal Procedure, 1973, to the concerned nodal officer, the nodal officer of Paytm and OLX would have been bound to supply the information to the officer. However, these steps were not taken, nor was the case registered. The seller visited the police station for a few days, attempting to register the case, but to no avail. Therefore, it becomes abundantly clear that the data we see is only part of the offences that are being committed, as many of these types of cases go unreported.

Even in this case, if the nodal officer supplied the information of the KYC, there are high chances that the KYC supplied to Paytm will be fake, and the criminals would be using some public *wifi* for the commission of the offence or even if the SIM card which is used may have been obtained by fake identity cards. Now, the rules are loosely applied, and most cybercrimes involve Paytm, which provides banking-like facilities after it was given the status. Still, they have not been adhering to the guidelines provided and flouting the rules, as most of the crimes involve Paytm as one of the mediums for committing the crime. Paytm shall be more cautious in getting the KYC than other scheduled commercial banks.

When acquiring a SIM card, the process initially required a photocopy of your identity card and one signature. This was the easiest way to acquire SIM cards for the commission of offences, and mostly, the crimes were committed using SIM cards issued in the name of a person who may not have known the SIM card was being issued or misused for different purposes. Then, the SIM cards were issued by linking them to the Aadhaar card, and subsequently, data theft became a concern, which was thereafter addressed. Currently, SIM cards are only provided with the Aadhaar card. Still, you need to carry the original Aadhaar card and get a SIM card issued, but thanks to the quality of the image captured in the Aadhaar card, offenders take advantage of this flaw. With the connivance of the SIM card distributor, they obtain SIM cards issued on lost Aadhaar cards. Again, the SIM card, which is often used for the commission of offences, may not have genuine KYC, and the person involved in the crime may not be confronted.

In case the information is not supplied by the nodal officer to the investigating officer of the offence in the time frame mentioned under Section 91 of the Code of Criminal Procedure 1973, the concerned court if thinks appropriate can initiate action and take cognizance against such officer under section 175 of the Indian Penal Code 1860, alternatively the investigating officer may if deem fit, file a complaint under section 195 (1) (a) Code of Criminal Procedure 1973 and make prayer to the concerned court to take cognizance under section 175 of the Indian Penal Code.

C. Procedure for Investigating Cyber Offences

The procedures for investigation and trial are outlined in the Code of Criminal Procedure, 1973. Section 4 of the Code of Criminal Procedure, 1973, provides details of the investigation and other trial processes. Section 4(1) of the Code of Criminal Procedure, 1973, provides that all offences under the Indian Penal Code are to be inquired into, investigated, and tried by the provisions mentioned in the Code of Criminal Procedure, 1973. Section 4(2) of the Code of Criminal Procedure, 1973, provides that any other law in force shall also be investigated, inquired into, and tried by the Code of Criminal Procedure, 1973. Still, an exception applies if the investigation process has been prescribed under special laws, in which case such exceptions will be allowed. The Code of Criminal Procedure, 1973, shall not apply to areas covered under special provisions. Thus, the offences mentioned under the Information Technology Act 2000 shall also be investigated, inquired into, and tried by the code, subject to the special provisions applicable under the special laws in force. The exceptions are contained in sections 78 and 80 of the Information Technology Act 2000. These sections, read in conjunction with section 81 of the Information Technology Act 2000, prevail over the provisions of the Code of Criminal Procedure, 1973. According to this section the investigation of the offence can be made by the police officer not below the rank of the inspector, which was amended under the amendment made to Information Technology Act 2000 in the year 2008 for before the investigation was to be made by the officer not below the rank of the Deputy Superintendent of Police (DSP). The investigation is to be conducted by a police officer not below the rank of an Inspector, which is also an exception to the Code of Criminal Procedure, 1973. In the other section, a police officer of the rank of inspector may enter any public place and search and arrest any person found therein who is suspected of having committed, is committing, or is about to commit an offence under this Act. Under the Indian Penal Code, the preparation is punishable when a person is about to commit dacoity or wage war against India. However, as mentioned under the Information Technology Act 2000, the person can be searched and arrested, even if the offence has not yet been committed and is not necessarily a completed act. It is pertinent to note that this section applies only to public places, not private ones.

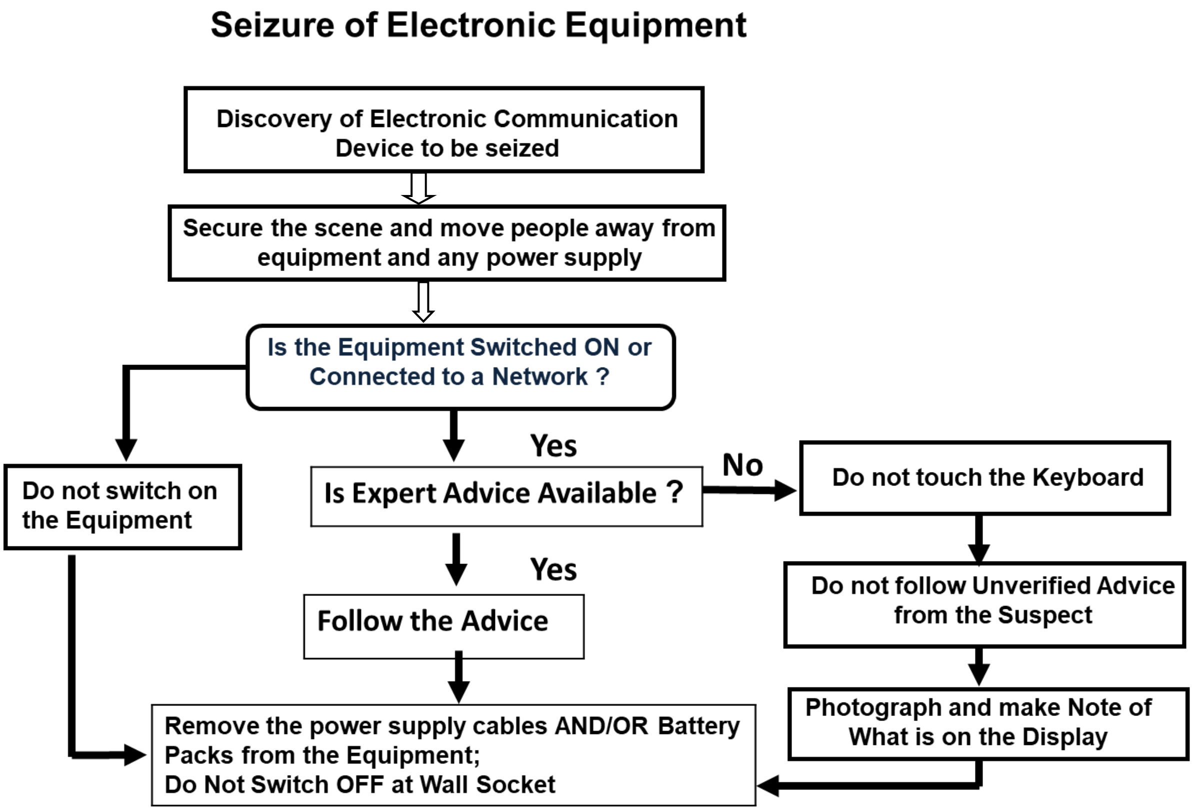
Apart from the two exceptions mentioned above under Sections 78 and 80 of the Information Technology Act, 2000, the procedure for investigation, inquiry, and trial for offences punishable under the Information Technology Act, 2000, is governed by the Code of Criminal Procedure, 1973. These two provisions are supplementary to the code, and both acts are applicable. In such cases, the procedure mentioned in the Information Technology Act 2000 will be appropriate, as the special provisions have an overriding effect in the event of inconsistency between the two legislations. Hence, Sections 78 and 80 of the Information Technology Act, 2000, will prevail over the Code of Criminal Procedure, 1973.

D. Search and Seizure in the case of the Information Technology Act 2000

Section 165 of the Code of Criminal Procedure, 1973, and Section 30 of the Information Technology Act, 2000, empower the Investigation Officer to collect and seize evidence. The search can be conducted in public places by the investigating officer, in this case, not below the rank of Inspector. Seizure procedures are essential in cases involving digital evidence, just like any other crime. However, the method for collecting evidence shall be different from the traditional form of evidence collection. Extra precautions must be taken when handling digital evidence. Generally, an IO trained in the field of forensics, along with competence in computer science, may be suitable for handling such evidence.

Retrieval Number:100.1/ijmcj.A114005010925
DOI:10.54105/ijmcj.A1140.05010925
Journal Website: www.ijmcj.latticescipub.com

Published By:
Lattice Science Publication (LSP)


Seizure of Electronic Equipment
Discovery of Electronic Communication Device to be seized
Secure the scene and move people away from equipment and any power supply
Is the Equipment Switched ON or Connected to a Network ?
Do not switch on the Equipment
Yes
Is Expert Advice Available ?
No
Do not touch the Keyboard
Yes
Follow the Advice
Do not follow Unverified Advice from the Suspect
Photograph and make Note of What is on the Display
Remove the power supply cables AND/OR Battery Packs from the Equipment;
Do Not Switch OFF at Wall Socket

[Fig.3: Flowchart Depicting the Procedure for Seizing the Digital Evidence [8]]

Filing a charge sheet in cases of cyber offences is one of the most important aspects of criminal investigation.

E. Jharkhand: Hub of Cyber offences

Jharkhand is now the most infamous state in India for the commission of cybercrimes across the country. According to Mr. Rajeev Gauba, I.A.S., it is reported that half of the total cybercrimes committed in India originate from the district of Jamtara in the state of Jharkhand. The development of Jamtara as a hotbed, or the epicentre of crime, is due to the high influx of population from the adjoining areas of West Bengal. The availability of a large number of identity cards for sale is also a contributing factor to the vulnerability of crimes in this area. The crime has a pan-India presence, and individuals engaged in various activities across different professions in the country, including those from the district, have also found their way to the district. They have mastered the local languages of other areas to facilitate the commission of cyber offences [9]. These fraudsters use different local dialects spoken in that particular area to mingle with the group and also commit the crime. According to the 2011 census, 58.7% of the population in this district has not been working for years, while the others are primarily engaged in agriculture. Many individuals have migrated to this area to engage in phishing activities nationwide. After the internet boom, cell phone towers witnessed more than 3,000 phone calls per day. Usually, the phone calls recorded in other towers are nearly 700 to 800, suggesting that cybercrime, in the form of phishing, has developed into a cottage industry, and people are being trained to commit such offences. The reports indicated by NCRB may not be adequate for understanding the scenario, as crimes registered in other states and arrests made in the Jamtara district may not be reflected in the statistics published by NCRB for the state of Jharkhand, which makes Jharkhand appear better [10].

The modus operandi of cybercrime is a crime that may also be referred to as an organised crime, as it involves a chain of people, each with a distinct role to perform during the action. The first step is the procurement of the SIM cards. After the SIM card is acquired, trained youngsters who have been provided with the number series start dialling the assigned number series to call [11]. They make 100 -300 calls for which they are paid five hundred rupees. If any information is procured, it is then transferred to the other group who have registered in different e- wallets available online, most of the KYC done on these electronic wallets are from the fake identity cards which are being procured through other group for the adjoining areas of West Bengal and also from the laborers who have been working in different parts of the country. The SIM cards and identification cards are also procured by the labourers from various places for a requisite amount. After the caller gets hold of an account detail, which is the 19 digit debit card number, CVV number and one time password they commit the fraud and transfer the amount from the victim's account to the electronic wallets, which is further transferred to bank accounts who has given his consent to be a party to the crime on a share basis and immediately after transferring the amount to the account the money is withdrawn from the bank, which would be distributed in the manner as previously decided between the parties involved in the commission of the crime. India has over 1.5 billion current and savings account, 29 million credit cards and around 820 million debit cards Further, sharing of the OTP (one-time password) to the people making the phone call on one pretext or the other, the chances of someone believing the call to be genuine are relatively high, and people get duped. The software and other developments in the field of Information Technology and cyber technologies have gained prominence. There are several software found after the investigation in these areas, that the software can clone the sim card if the phone is present in the vicinity and copy the sim cards in a matter of few seconds which is again a dangerous trend and people shall take all precautions about online transactions and also keep the smart phone safe [12].

The scamsters in Jamtara have consistently found new electronic wallets, such as Tapzo, TMW, and Kitecase, as more established ones have tightened their norms for KYC regulations and documentation. These cyber criminals have found a way out.

In the programme titled ***'Legal Awareness on Cyber Crime'*** organized by Judicial Academy Jharkhand, Ranchi and Jharkhand State Legal Services Authority Jharkhand Police have set up an interstate coordinating mechanism to probe the cyber offences, was revealed by the Inspector General of Police Shri Navin Kumar Singh. Jharkhand being the epicenter of cybercrimes, the investigating officer from all over India have requested for help in the investigation of cybercrimes registered in different parts of India, for making the accessibility easier the online investigation cooperative network platform for ensuring better interstate cooperation in curbing cybercrime has been set up in the backdrop of the large number of cyber culprits committing the act of cybercrimes all across the country are linked to Jharkhand and particularly Jamtara. The platform enables the Investigating officer to register their request for the area of cooperation. After receiving the information, the report is sent back within 7 days. A request for cooperation has been received from Jammu and Kashmir, extending to areas as far as Port Blair, for assistance in investigating alleged cybercrimes. In several cases, the Jharkhand Police have arrested cybercriminals and handed them over to the respective state police. The Jharkhand Police are also developing a database containing information about arrested cybercriminals, including their account details and e-wallet information, which will be analysed and used to generate actionable intelligence for apprehending cybercriminals.

III. SUGGESTIONS

A. Inclusion of Trained Manpower

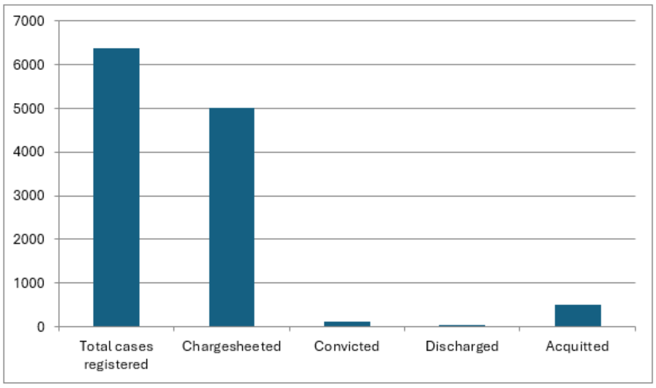
One of the main drawbacks of the criminal justice system is the lack of manpower for effective investigation; moreover, the lack of efficient manpower also contributes to defective investigation in our country. The primary agency responsible for conducting the investigation is the police, which is under the State List of the Constitution. No effective changes in the functioning of the police have been implemented since the legislation was first drafted. Several changes have been proposed for the country's police operations, but these have not been implemented. The changes in the police department, as indicated in the case of Prakash Singh vs. Union of India [13], were not effectively implemented by the states across the country. Since the subject falls under the purview of the State List, no effective directions can be imposed on the same. The cases of cyber offences are diverse, and the approach to investigation should also be tailored accordingly. The Information Technology Act 2000 mandates that investigations into cyber offences be conducted by a police officer not below the rank of Inspector. However, this clause is also one of the drawbacks, as police departments often lack the adequate number of officials required for this purpose. Moreover, personnel who have reached the position of Inspector have not been provided with regular training to tackle issues of cyber offences. The staff should be adequately trained and experienced in the field of cyber forensics, and explicitly recruited for the post of cyber experts to establish a strong framework of efficient manpower to control and investigate digital financial fraud threats.

B. Forensic Science Laboratories

The inclusion of the Forensic Laboratories under the Police department still raises questions about the inclusion of the forensic scientists to work along with the police, the FSL which has only three sanctioned posts for the Cyber Forensics division in the Jharkhand, which has the district of Jamtara, the sleepy area of district of *Santahal Pargana* is epicenter of cybercrimes in the country. Only one person is appointed to the three positions in the Forensic Science Laboratory, Hotwar, Ranchi, on a contract basis. The cyber forensics division of the Forensic Science Laboratory in Hotwar, Ranchi, is not even functional due to a scarcity of manpower. The forensic lab can be an agency that proves to be a milestone in containing offences related to digital and financial crimes. However, the lack of recruitment at the said agency and the deployment of contractual staff are major hindrances to the institution's efficient functioning. Some states in India have shown drastic improvement in their laboratories, handling such situations in a manner that has led to the arrest of criminals and the recovery of stolen assets in cases involving digital financial crimes.

C. Legislative Reforms

The lone legislation to curb digital offences is the Information Technology Act 2000, as amended in 2008. The legislation has failed to curb offences related to digital financial fraud. It has also failed to apprehend the offenders in a manner that can be remotely considered efficient. Most of the offences mentioned in the act are available, which provides an advantage to offenders in securing bail for these offences. Once bail is provided, it becomes relatively easy for offenders to erase digital evidence from online platforms, and thus, the crime rate is on the rise. According to NCRB data published for the year 2018, the statistics recorded a conviction rate of merely 2.4%, i.e., only 124 persons were convicted for the offence in 2018, out of a total of 5,383 registered cases. Cyber offences are one of the rare offences in which the rate of acquittal (10%) exceeds the rate of conviction (2.4%) [14].



[Fig.4: Cases Registered for Cyber Crime in the year 2018 [15]]

D. Infrastructure and Technology Enhancement

Governments have various steps for curbing cyber offences, but there are certain limitations to the government's functioning. Police and public order are a subject matter enumerated under the State List of the Seventh Schedule of the Constitution of India. Thus, the reforms that have been suggested from time to time have not been implemented, as they are challenging to implement in an organisation that has not undergone significant change since the British era. Even after independence, not much change has been made to this institution. With the recent rise in cyber offences, the Government cannot build the necessary infrastructure and hire the required manpower to curb the crimes effectively. Still, the public-private partnership can be a welcome move and a step towards reducing digital financial fraud offences, potentially leading to the tracking of funds and facilitating their recovery. The Infosys Foundation has committed Rs 22 Crores to build a lab for cybercrime investigation, as it has signed a Memorandum of Understanding (MoU) with the Karnataka Police to make this a reality. The Centre for Cyber Crime Investigation Training and Research (CCITR) will be established in Bangalore, and the Infosys Foundation will maintain the premises for five years. During this time, the Centre will train police, prosecutors, judicial officers, and other departments and investigative agencies involved in cybercrime investigations.

E. Cyber Courts

The IT Act mentions the establishment of Cyber Appellate Tribunals under Section 48 of the Information Technology Act, 2000; however, the purpose is not being achieved, as cyber offences have become more common in metro cities and the Silicon Capital of our country. The offences are now not only limited to these cities but have made their way to the laid back cities also, it may be a welcome move to assign special courts for monitoring the cyber offences, where in the judges and other officials of the criminal justice system to be provided special training to the persons involved in the administering the criminal justice system and hence improve the quality of the investigation and in turn prosecution rate in cases of cyber/ digital offences. Since the nature of cybercrime offences is quite different and the modus operandi changes within days, they need to be tackled in a manner that encompasses an efficient task force to provide adequate results and instil fear in the criminal justice system [15].

The offences of cybercrimes have taken a vast structure in our country and cannot be controlled by the existing infrastructure and the manpower involved in dealing with the crimes. However, the same cannot be achieved overnight. First and foremost, it is essential to educate people about all the possibilities of cybercrimes. They should refrain from providing details of a personal nature, even if there is a remotest possibility of intrusion of privacy and commission of digital financial fraud. Moreover the existing system is to be revamped along with substantial changed to made to the substantive and procedural laws associated with the offences of cyber nature, which will enable to control the offences, make efficient investigation, getting inputs from the Forensic Science Laboratories, securing the digital evidences, marinating the chain of custody, locating the trail of financial digital frauds and lastly the enhancing the rates of conviction in the offences related to cybercrimes.

IV. CONCLUSION

The rapid growth of cyberspace, driven by increasing internet access and the rise of smartphones, has completely reshaped how individuals in India interact, conduct business, and access services. While this digital shift has brought about significant convenience and economic opportunities, it has also made users vulnerable to serious threats, such as cyber fraud, identity theft, and digital financial crimes. The existing legal framework, particularly the Information Technology Act of 2000, provides a basic structure for tackling these issues. However, as technology continues to evolve and cybercrime becomes increasingly complex, we require ongoing legal updates and stronger enforcement measures to address these challenges. This study highlights the pressing need for enhanced digital literacy, robust cybersecurity policies, and legal reforms to ensure a secure and safe digital environment. Strengthening our legal and institutional responses to cybercrime is vital for protecting users and fostering trust as India advances in its digital journey.

DECLARATION STATEMENT

I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed solely.

REFERENCES

1. Central Bureau of Investigation. (2025, July 7). CBI cracks down on transnational cybercrime syndicate; Noida call centre busted. The Times of India. https://timesofindia.indiatimes.com/city/delhi/cbi-cracks-down-on-transnational-cybercrime-syndicate-noida-call-centre-busted/articleshow/122323303.cms
2. PwC India. (2017). *Securing the nation's cyberspace*. https://www.pwc.in/assets/pdfs/publications/2017/securing-the-nations-cyberspace.pdf
3. Kasturi, Y., & Dar, M. A. (2024, December 30). Cybercrime in the digital age: Challenges and legal gaps in India's cybersecurity landscape. *African Journal of Biomedical Research, 27*(6S). https://africanjournalofbiomedicalresearch.com/index.php/AJBR/article/view/5724
4. NCRB. (2023). Crime in India 2022 (data on cybercrime jump and Karnataka's position). https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf
5. Taskin, B. (2025, June 12). A 24% spike in cybercrime in India, as shown by NCRB data. Fraud, extortion & sexual exploitation top motives. *The Print*. https://theprint.in/india/24-spike in-cybercrime-in-india-shows-ncrb-data-fraud-extortion-sexual-exploitation-top-motives/1871498/
6. NSO. (2025). Comprehensive Modular Survey: Telecom, January–March 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2132330
7. Tripathy, S. S. (2025, April 21). *A comprehensive survey of cybercrimes in India over the last decade* [Preprint]. arXiv. DOI: https://doi.org/10.48550/arXiv.2505.23770
8. National Crime Records Bureau. (2017). *Crime in India 2017 – Volume 2*. Ministry of Home Affairs, Government of India. http://NationalCrimeRecordBureau.gov.in/StatPublications/CII/CII2017/pdfs/Crime%20in%20India%202017%20-%20Volume%202.pdf
9. Barnwal, S.K. (2019). *A survey report on the growing cybercrime in Jamtara, Jharkhand (India)*. ARKA Jain University. https://www.researchgate.net/publication/332874459
10. The Hindu. (2017, October 18). The cyber con 'artists' of Jharkhand's Jamtara district. https://www.thehindu.com/news/national/other-states/the-cyber-con-artists-of-jamtara/article19874869.ece
11. Ministry of Home Affairs. (2024). *Annual report on cybercrime trends in India*. Government of India. https://www.mha.gov.in/en/documents/annual-reports
12. Murugan, S. (n.d.). *Electronic evidence: Collection, preservation and appreciation*. Vigilance and Anti-Corruption, Chennai. https://nja.gov.in/Concluded_Programmes/2018-19/P-1125_PPTs/6.Electronic%20Evidence-%20Collection%20Preservation%20and%20Appreciation.pdf
13. Times of India. (2019, July 22). 800 nationwide requests for help in probing cybercrime linked to Jharkhand. *The Times of India*. https://timesofindia.indiatimes.com/city/ranchi/800-nation-wide-requests-for-help-in-probing-cyber-crime-linked-to-jharkhand/articleshow/70326267.cms
14. National Crime Records Bureau. (2019). *Crime in India – 2018: Statistics*. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/en/crime-india
15. National Crime Records Bureau. (2018). *Crime in India 2018 – Volume 2*. Ministry of Home Affairs, Government of India. http://ncrb.gov.in/StatPublications/CII/CII2018/pdfs/Crime%20in%20India%202018%20-%20Volume%202

AUTHOR'S PROFILE

Dr. Siddhant Chandra completed his Graduation in Zoology from St. Columba's College Hazaribagh and thereafter studied LL.B. from Campus Law Centre, University of Delhi, New Delhi. After a brief Law practice in the District Courts of Delhi and the Delhi High Court, he went on to pursue his Master of Laws (LLM) from NALSAR, Hyderabad. He has completed his Doctorate from the West Bengal National University of Juridical Sciences (WBNUJS). He has also completed a Master of Business Laws (MBL) from NLSIU, Bengaluru. He has over 9 years of teaching experience in both State and Private institutions.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Lattice Science Publication (LSP)/ journal and/ or the editor(s). The Lattice Science Publication (LSP)/ journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.