ROLE OF POLICE IN PREVENTING, DETECTING AND INVESTIGATION OF CYBER CRIME IN INDIA

Manish Kumar Attry, Research Scholar, Sardar Patel Subharti Institute of Law, Swami Vivekananda Subharti University, Meerut.
Dr. Prem Chandra, Associate Professor, Sardar Patel Subharti Institute of Law, Swami Vivekananda Subharti University, Meerut.
Ms. Kaushiki Roy, Assistant Professor, IIMT College of Law, Greater Noida.

Abstract

Online cracking and denial of service assaults are only two examples of the wide range of illegal activities that fall under the umbrella term of "cybercrime" in India. Before the year 2000, there was no statute that dealt specifically with cybercrimes. When it comes to electronic administration, electronic trade, and electronic banking, the Information Technology Act of 2000 (IT Act) covers it all which then finally came into place. The legislation also specifies punishments for those who commit cybercrime, a growing problem in India. The rise in online activity has made it more difficult to prevent illegal activity and apprehend those responsible for cybercrime, posing new problems for Police. As applicable for any crime, the role of police is very important in not just checking for cases but also in prevention. The main aim of the research paper is to examine the current role of Police in detecting and investigating the cybercrimes in India and critically examining the legislation available. There is an urgent need for new laws and policies to be formulated in the area of cybercrime investigation, which the author of this study hopes to draw attention to and also provides suggestions to make it an efficient administration process.The problem of possible internet abuse is becoming steadily worse, therefore lawmakers, judges, and government officials need to make sure the legislation reflects recent changes in order to combat the growing threat of cybercrime.

Keywords: Cyber Crime, Government, Police, Investigation, Legislation, Threats

Introduction

With the rise of cybercrime, the meaning of the word "space" in reference to criminal activity has changed. We are no longer limited to a purely geographical understanding of crime and criminality. Unlike with many traditional crimes, a criminal in cyber space is not limited by physical location.[1]

After the number of people increased, the difficulties for our police department increased as well. Adopting new techniques to combat crime in the virtual world is a necessity of the hour for both the prevention of cybercrime and the apprehension of the criminals who are involved in it. Because financial institutions are worried that their customers will lose faith in the safety of their computer systems, they do not always disclose crimes perpetrated against their customers. This is because they do not want to lose their customers' confidence. Since of this, it is difficult for law enforcement agencies to adequately recognise and comprehend the dangers, hazards, and harm that are posed by cybercrime because they do not have access to all of the information that they require. Complaints should only be filed at the designated police station for the cyber security cell, rather than at any other station, because a combination of circumstances, including a lack of understanding and distance, causes a significant number of incidents to go unreported to the fast deployment team. This is the most recent of the national threats that call for a coordinated reaction on the part of the police force. Either the accumulation of numerous smaller cybercrimes or the execution of a single malicious cyberattack could be the root cause of a widespread cyber disaster. We need to categorise the threat according to the degree of its potential impact.[2]

The advancements that have been made in the field of information and communication technology (ICT) have been extremely beneficial to the human race in a variety of different ways. On the other

[1]Elena Martellozzo, *Cyber Crime and its victims* (ebook edn, Taylor & Francis 2017) 45.
[2]Roderic Broadhust, *Cyber-Crime: The Challenge in Asia* (Hong Kong University Press 2005) 243.

hand, it has simultaneously presented us with enormous obstacles and opened the door to new opportunities for criminals to commit crimes with highly advanced technological instruments. The same information and communication technology tools are being used by criminals to engage in harassing behaviour, making threats, being duped, damaging reputations, extortion, engaging in illegal trade, recruiting terrorists, and carrying out security problems and acts of terrorism, among other illegal activities. As a consequence of this, society now views "Cyber Crime" as a big threat, and there is an urgent need for governments to respond promptly and forcefully.[3] The world's governments have reacted to the difficulties posed by the cyber world by developing laws and setting up institutional mechanisms to combat such challenges. Despite this, there is a significant amount of work that needs to be done in the areas of cyber policing and the investigation of cybercrime. The online world is a fluid world. The prevalent acts are not fully covered, and the laws that now exist in order for the police to intervene in the digital world do not cover all of the offences that are taking place in the online world.

The Evolution of cyber crime

The first major cybercrime was documented in 1820. Multiple other nations, including China and Japan, have also adopted this policy. Joseph-Marie Jacquard, a French textile manufacturer, invented loom that same year. As a result, this steered the concepts of inventing new materials, which generated unbelievable fear among Jacquard's personnel that their positions identically as their standard were becoming subverted, thereby causing their principles to fall apart. From the Morris Worm to the more recent ransomware, many different types of digital worms have been discovered. Companies have taken numerous steps to protect their customers' right to privacy and quiet.[4]

In 1997, cybercrime attacks were as commonly used frameworks as infections such as the Morris code worm. The attacks that took place in 2004 took the form of malicious programmes, advanced worms, and Torjan horses. They were known as digital cheaters and phishers in the year 2007. The year 2010 was marked by the proliferation of botnets, SQL assaults, and DNS attacks. In 2013, the most common forms of cyberattack were ransomware attacks, distributed denial of service attacks, botnets, social engineering, and malicious emails. At this time, the types of cybercrimes that are being tackled include Android hacking, cyber battling, key lumberjacking, Bitcoin wallet theft, Bitcoin wallet theft, key lumberjacking, stealing phones, and stealing banking information.

Yahoo v. Akash Arora[5] was one of the earliest first cases of cybercrime to be brought up in the Indian court system. 1999 was the year that this incident took place. In this particular instance, the defendant, Akash Arora, was accused of making unauthorised use of the trademark or domain name "yahooindia.com," and an application for a decree of permanent injunction was submitted. The other case is called *Vinod Kaushik and others v. Madhvika Joshi and others*,[6] and it is now being heard in court. In this case, it was decided that it was unlawful to access the e-mail accounts of the husband and father-in-law without first obtaining authorization from those individuals under section 43 of the Information Technology Act of 2000. The verdict in this case was handed down in 2011. All of these incidents bring up the question of how cybercrime has developed over time, with a particular focus on how it has progressed in India.[7]

As time went on, and social networks became more widespread, the rate of cybercrime began to rise, perhaps because of the increased ease with which criminals could access the private lives of users.[8] One of the most savage types of criminal activity, known as the non-consensual sharing of intimate

[3]Kamini Dashora, 'Cyber Crime in the Society: Problems and Preventions' (2011) 3(1) JAPSS 240, 244.
[44]Jonathan Lusthaus, 'How organised is organised cybercrime' (2013) 14(1) GC 54.
[5]*Yahoo v. Akash Arora* 1999 IIAD Delhi 229, 78 (1999) DLT 285.
[6]*Vinod Kaushik and others v. Madhvika Joshi and others*, Appeal No 2 of 2020 in the Cyber Appeallate Tribunal (decided on 29 June 2011).
[7]Vinit Kumar Gunjan, Amit Kumar and Sharda Avdhanam, 'A survey of cyber crime in India' (2013) IEEE <https://ieeexplore.ieee.org/document/6710503> accessed 11 February 2023.
[8]Susheel Bhatt and Susheel Chandra and Durgesh Pant, 'Cyber Crime in India' (2011) 2(5) IJARCS 153, 154.

images, emerged as a result of this development (NCSIA). There has been an uptick in the number of crimes reported recently, highlighting the need for a more proactive response.[9]

Police and Cyber crime

The advent of the digital world brought with it a new paradigmatic change in terms of connectedness, ease of offering services, and swiftness of transactions. On the other hand, there is a concurrent increase in both vulnerabilities and dangers. These have presented issues that have never been seen before for the apparatus of law enforcement. This scenario raises questions regarding the preparedness of the Police to face these challenges, the swiftness of policymakers to adapt or amend the framework according to the needs of the time, and the capability of various governments and institutions to collaborate and coordinate with each other.

The Information Technology Act, in its different sections, has provided a legislative framework that has outlined the broad parameters for cyber policing in India. This framework is known as the Information Technology Act. Under the Information Technology Act, Section 69 grants the government or other agencies the authority to intercept, monitor, or decrypt any information that is generated, transmitted, received, or stored in any computer resource, provided that they comply with the procedure that is laid out in that section. This authority can be exerted if the Central Government or the State Government, depending on the circumstances, is satisfied that it is necessary or appropriate in the interest of the sovereignty or integrity of India, the defence of India, the security of the State, closer ties with foreign States, or public order, or for the purpose of preventing provocation to the commission of any cognizable offence pertaining to the aforementioned matters, or for the purpose of investigating any offence (The Information Technology (Amendment) Act, 2008).

The order shall direct any agency of the competent Government to take such action, in accordance with such procedure as may be established, and to document in writing the reasons for doing so.[10] When requested, the subscriber or intermediary must provide all necessary facilities and technical help. These include:

(i) creating, transferring, receiving, or storing the data; granting access to or securing the use of the computer resource containing the data; or
(ii) catching it in the act of being sent, monitored, or decrypted; or
(iii) supplying information that has been stored in a computer resource.

Failure to provide the aforementioned facilities and technical help is punishable by imprisonment for a term of up to seven years, as well as a fine [The Information Technology (Amendment) Act, 2008]. Section 69A of the Information Technology Act of 2008 grants the Central Government or one of its officials the authority to give directives prohibiting public access to any information via any computer resource under the same conditions as described above.

Section 69B deals with the authority to permit monitoring and collection of traffic data or information via any computer resource for cyber security purposes. By publishing a notification in the Gazette, the Central Government may authorise any Government agency to supervise and gather traffic data or information produced, transmitted, received, or stored in any Computer Resource in order to enhance Cyber Security and to identify, analyse, and prevent any invasion or spread of computer pollutant in the country [The Information Technology (Amendment) Act, 2008]. Regarding the matter of cooperation between various agencies and governments, the problem of cybercrime takes us beyond the realm of merely intra-state or inter-state but also transnational levels. A number of resources have discussed the importance of international cooperation between law enforcement organisations that are attempting to combat or investigate digital crime at one of three different levels: macro, meso, or micro. On a more systemic scale, collaboration occurs most frequently between national governments and other international organisations, especially through the conduits of Europol and Interpol. At the meso level, the collaboration is most likely to occur

[9]Rob McCusker, 'Transnational organised cyber crime: distinguishing threat from reality' (2006) 46(4) Crime Law and Social Change 258.
[10]Debarati Halder and K Jaishankar, *Cyber Crimes against women in India* (ebook edn, Sage Publications 2016) 112.

between police forces or agencies of law enforcement that are located in different nation states. For instance, the PcEU in the United Kingdom and the FBI in the United States might work together. At the most local level, cooperation will typically take the form of communication between individual investigators and will be of an informal nature.

Convention on Cybercrime, also identified as the Budapest Convention on Cybercrime, is the first international treaty that seeks to address Internet and computer crime by harmonising national laws, enhancing investigative techniques, and increasing cooperation among nations. This convention was held at the international level and is also known as the Convention on Cybercrime. On July 1, 2004, the Convention was officially put into effect. The Convention has not yet received agreement from the international community, as evidenced by the fact that India, which was not engaged in the writing of the Convention, has also declined to adopt it, as have a few other countries, on the grounds that it may infringe their sovereignty.

According to the prevalent school of thought, maintaining order in the virtual world is the responsibility of the public police, and it is primarily a government duty. However, academics have pointed out that the surveillance of the cyber world can be carried out not just by publicly sponsored or state-supported police forces, but also by private police forces and non-governmental police forces as well. Building linkages between public policing, corporate policing, and non-governmental policing is essential to the success of cyber policing, which is dependent on all three types of policing. The ease with which offenders can move throughout the internet is making it nearly hard to maintain law and order in this arena. In addition, in spite of the cybercrime conventions, a hostile relationship between two countries may make it very impossible for law enforcement to investigate and prosecute cross-jurisdictional cybercrimes. The existence of the culprit in many jurisdictions, particularly if the offender chooses to remain anonymous, makes it exceedingly difficult to conduct cyber policing.[11]

Investigation methods

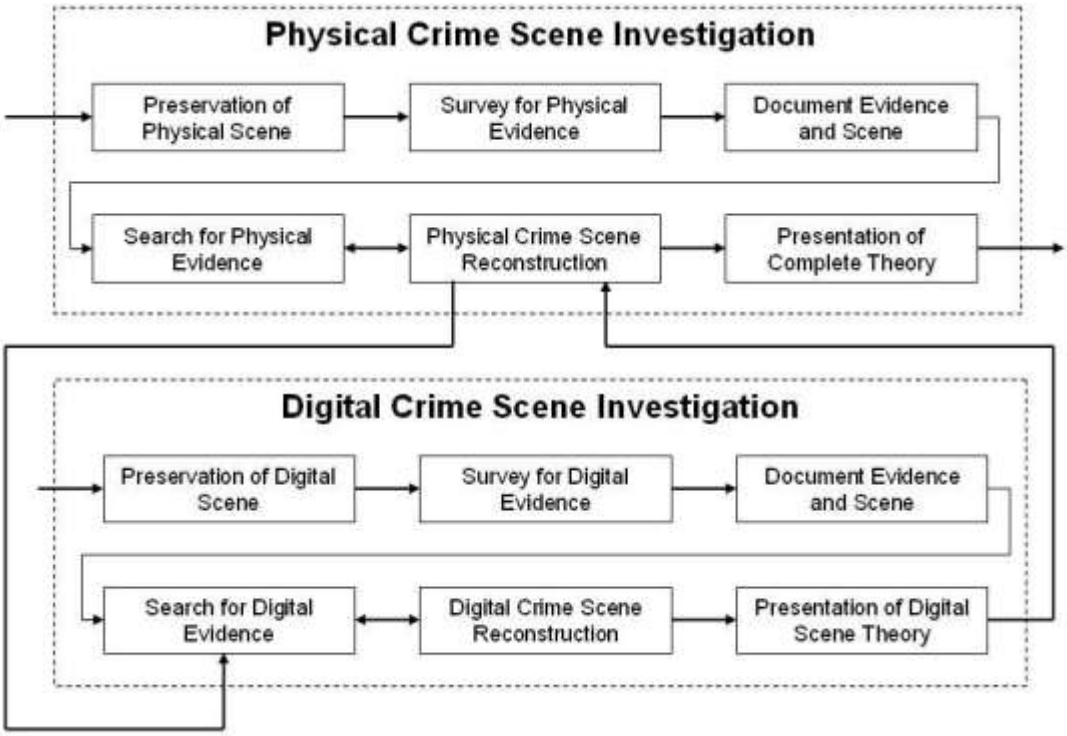
One could argue that "a good model of cybercrime investigations is important" because it serves as a "neutral ground" on which to discuss the methods and tools that can aid in the investigation of cybercrime, regardless of the specific technologies or organisational settings in which they might be implemented. In 2004, a British scholar named Ciardhuáin put forth a model that has one of the firmest theoretical foundations. His "Extended Model of Cybercrime Investigations" consists of the 13 steps outlined below:

(1) Understanding - Realizing that you need to look into something
(2) Permission, such as that granted by a warrant
(3) Preparation - Putting the researcher's data to good use
(4) Disclosure - Letting everyone involved know that an investigation has begun
(5) Find and identify evidence; tracking down a suspect's computer, for instance.
(6) Gathering Possible Evidence - Acquiring Possible Evidence
(7) Proof transported to the proper location
(8) Evidence storage - Methods should be used to prevent contamination between samples
(9) Analysis of evidence - Recovery of lost data through specialised methods
(10) A hypothesis is a testable explanation for a phenomenon.
(11) Argumentation of a Hypothesis, as in Front of a Jury
(12) Argumentation for and against a hypothesis: competing theories will be taken into account
(13) Information sharing - This may have an impact on future inquiries.

Role of Police in detecting any crime scene investigation

[11]Debarati Halder and K Jaishankar, *Cyber Crime and the victimization of women* (ebook edn, Information Science Reference 2012) 105.

Police plays a major role in any crime scene. But the question that comes to any mind would be a digital scene as to how any police personnel will move ahead with their observations. For understanding in depth the same, the below image shows the difference:



Source 1: This image is taken from http://www.dynotech.com/articles/images/crimescene.jpg

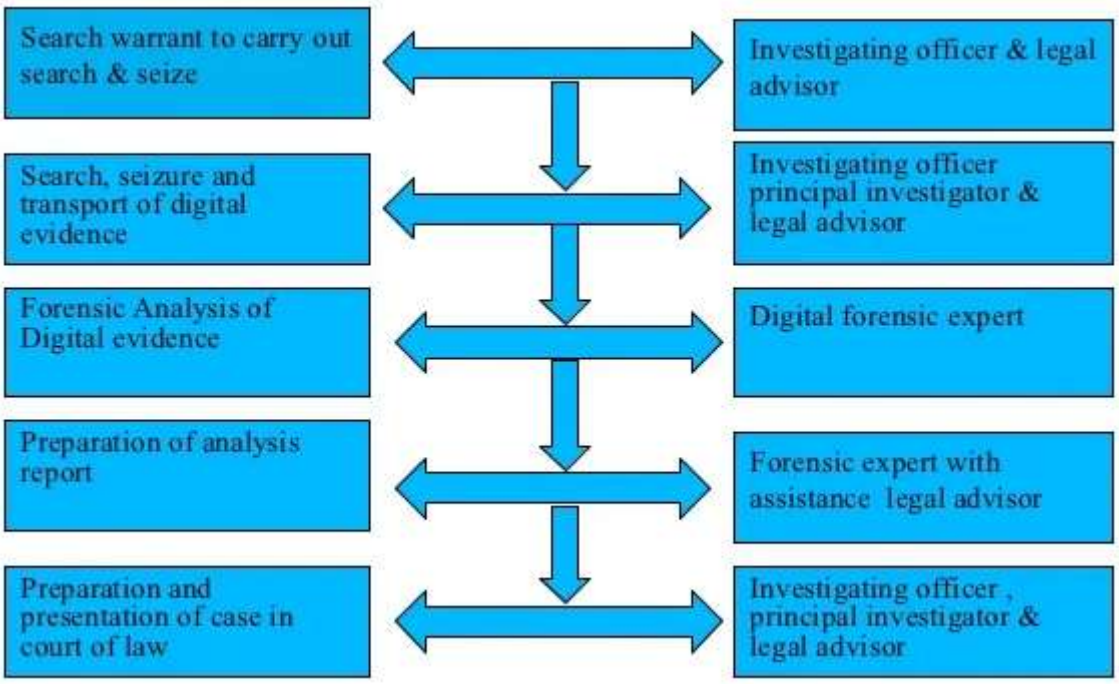
Section 78 of the IT Act discusses the authority of law enforcement to conduct investigations into computer crimes, and Section 80 grants law enforcement the authority to enter and search premises for the purposes of such investigations. A rise in conviction rates would make sense given the rise in major cases of reported cybercrime. However, many probes and prosecutions have stalled before they even begin. The incapacity of major stakeholders in criminal justice systems to understand the basics of technology-aided crime, along with trans-jurisdictional hurdles and covert operations, are likely to blame for this result.

The majority of states are conducting investigations into cybercrime with only one or a very small number of specialised cybercrime police stations, which may not be able to keep up with the extraordinary growth in the number of offences committed in the online world. Additionally, victims experience difficulties in contacting the appropriate police stations in order to file a complaint about the crime:

Investigation of computer crimes presents a number of fundamental difficulties such as:

- There is a lack of trained cyber investigators currently available.
- Forensic labs often only have access to a limited number of cyber forensics facilities.
- As a result of the enormous backlog, there are delays in obtaining reports.
- There is not currently an institutional structure to acquire the assistance of cyber experts from the private sector.

The below figure can be seen to study the process of police investigation in any cyber crime scene.



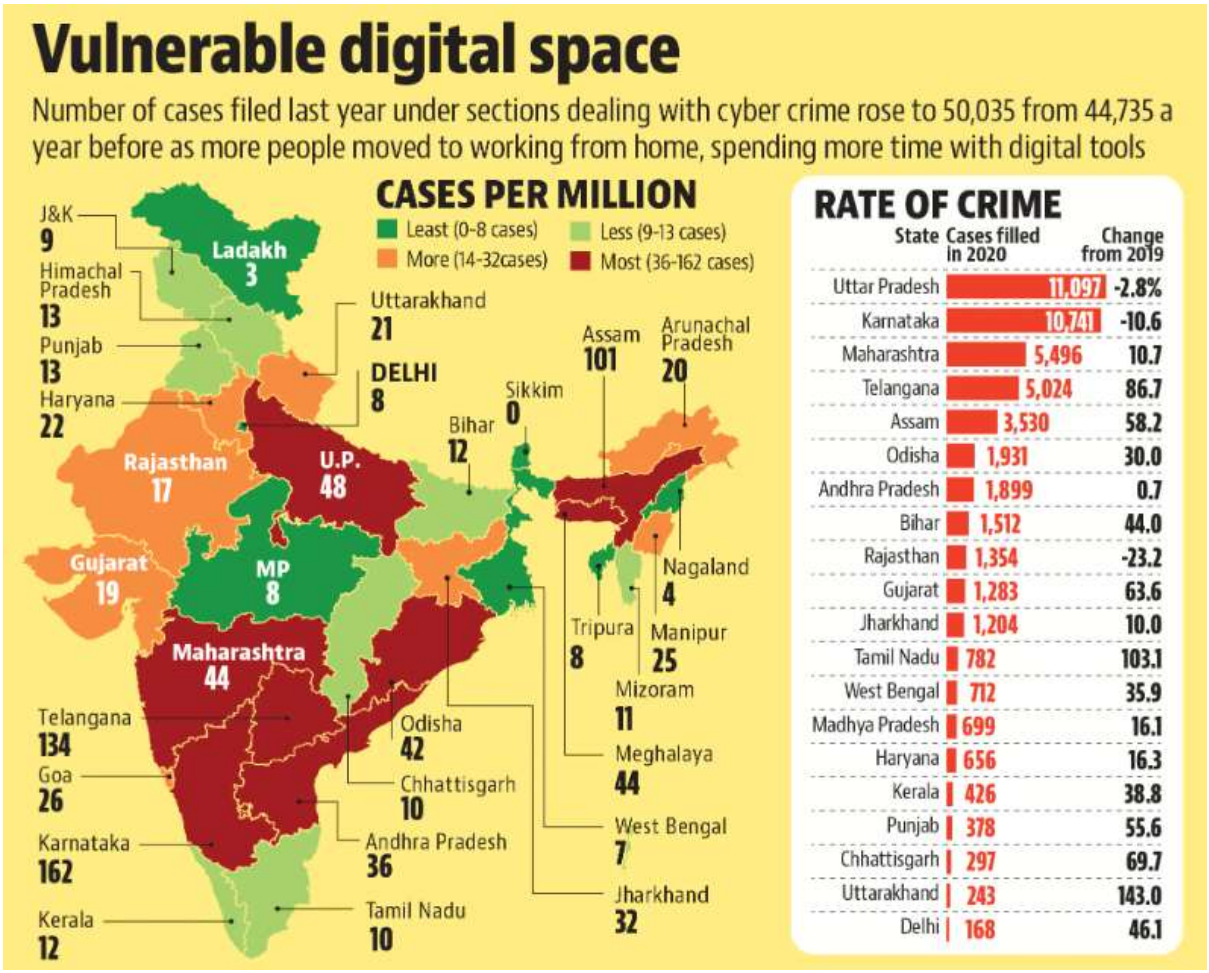
Source 2: The source of the image is as https://image.slidesharecdn.com/cyberforensicstandardoperatingprocedures-111212225028-phpapp01/95/cyber-forensic-standard-operating-procedures-8-728.jpg?cb=1323730615

Legal aspects focussing on Prevention of Cyber Crimes

The Indian Penal Code, enacted in 1860, is the primary piece of Indian law addressing the criminal penalties and punishments for cybercrime. The legal framework within which cyber policing and criminal investigation occur is the primary concern. In the Indian context, the cyber world was uncontrolled and law enforcement officials were unsure of how to respond to crimes committed in cyber space until the Information Technology (IT) Act, 2000 was passed.[12] Only after legislative action resulted in the creation of the IT Act, 2000 were cybercrime definitions and cyber policing and investigation made a reality. Its inherent fluidity also necessitated 2008's revisions to the Act's requirements. The Act expanded the jurisdiction of the Deputy Superintendent of Police who was previously permitted to investigate cyber offences to an Inspector, and it also added new cybercrimes such child pornography and cyber terrorism.

When it comes to cyber policing and the investigation of cybercrime, one of the most important questions that needs to be answered concerns the capabilities of the machinery. The efficacy of the cybercrime investigation cells and units is strongly influenced by the skill sets of the individuals who are assigned to work in those units. The country's overall recruitment standards for the police force are not going to be of any assistance in solving the problem. In order to combat the dangers posed by inventive but criminal brains, Indian law enforcement agencies need to recruit and work with the most qualified individuals in the field of information and communications technology (ICT).

[12]Dr Amita Verma, *Cyber Crimes and Law* (1st edn, Universal Publication 2009).



Source 3: Image source is https://www.hindustantimes.com/india-news/cyber-crimes-registered-11-8-increase-last-year-ncrb-101631731021285.html

According to the most recent NCRB data, the number of cybercrime-related complaints filed increased to 50,035 in 2017 from 44,735 in 2016. This is consistent with global trends showing an increase in people working and/or attending school from home while using digital tools. Total cybercrime rates per 100,000 individuals rose from 3.3 in 2019 to 3.7 in 2020. Bharatpur in Rajasthan, Deoghar in Jharkhand, Gwalior-Chambal region in Madhya Pradesh, Palgar in Maharashtra, and Noida in Uttar Pradesh are only few of the hotspots identified by state police authorities.[13]

The state of Rajasthan has reported that since January 2021, officers from at least twenty-two different states have visited the Bharatpur cyber police facility on the border between Rajasthan and Uttar Pradesh. Bharatpur was identified as the source of 40% of the cyber fraud instances recorded in Hyderabad. Bharatpur's neighbouring districts of Agra and Meerut in Uttar Pradesh, Nuh in Haryana, and the Gwalior-Chambal belt in Madhya Pradesh have also been implicated in multiple cases of cyber fraud, according to police officials.cybercrime.gov. in is the new reporting platform set up by India's Ministry of Home Affairs. Since the website's inception in January 2020, around 200,000 complaints have been submitted. In November of 2020, the department requested that all states file FIRs for complaints submitted through this website. In January 2021, MHA reported that out of nearly 2,00,000 complaints submitted through the portal in 2020, just 5,000 had resulted in cases being lodged.[14]

[13] Chetan Chauhan, 'Cyber crimes registered 11.8% increase last year: NCRB' *Hindustan Times* (New Delhi, 16 September 2021).
[14]Kirit Mehta and Aparna Nair, 'Cyber Crime and its penetration in India' (2021) ResearchGate 16.

Few important cases dealing with the role of police

(a) The Bank NSP Case[15]

For this specific event, a banking industry intern tied the knot. Only after drawing attention to their wedding did the couples admit that they had been communicating through work channels all along. For instance, "Indian bar affiliations," whereby they pretended to be government officials in email correspondence with their clients. These actions were taken inside of the banking systems. They lost customers and began receiving complaints about the bank's effectiveness later. The bank took some heat for unauthorised texts sent from their accounts. This was possible only through a clear investigation done.

(b) Avnish Bajaj v. State[16]

Disk was moreover concurrently sold-out in the market of Delhi, and in December of 2004 the CEO of Bazee.com was detected marketing a limited plate (CD) having unfavourable material on the site. The police in Delhi and Mumbai worked together to investigate the situation, but the CEO was eventually released on bail.

(c) State v.navjotsandhu @ afsan master[17]

This matter had been handled by the Hyderabad branch of the Bureau of Police Research and Development. The manipulator who launched the attack on the Parliament was found to be in possession of a framework. The Computer Criminology Division of BPRD received the framework that had been hidden from the two fear-based oppressors who were gunned down on December 13, 2001, as the Parliament was under attack. There were a few confirmations in the framework that called for the two manipulators' ways of thinking; the sticker from the Ministry of the created a phoney ID with fake Indian administration seal that was made in Jammu and Kashmir stood out as particularly telling.

(d) Andhra Pradesh State Road v. Income-Tax Officer[18]

An owner of a plastics company was busted with a large sum of cash that vigilance officials later determined to be untraceable. Once the deal was finalised between the owner's agents, it was discovered that the owner had filed roughly 6,000 duplicates of documentation confirming the authenticity of the trade that he had carried out. The owner was discovered by the watchful cops after he tried to pass off his one firm as five by using phoney online tools to make it look like he was overseeing all of them.

(e) CBI v. Arif Azim[19]

There had never been a conviction for cybercrime in India before this. When Sony established a new site under the Sony India pvt ltd domain, non-resident Indians (NRIs) could buy and sell Sony products to anyone in India, and all financial transactions took place online. She gave out her transaction information and MasterCard credentials when someone posing as Arif Azim in Noida had a contract with her in 2002. Arif oversaw the sale of the items later on. All of these exchanges and deposits were being documented. However, complications arose, and eventually the visa authority refused to accept the items and denied admission. Arif Azim was charged with web cheating under IPC sections 418, 419, and 420 after it was determined that he had engaged in unfair play. The police apprehended the criminals and looked into his network in Noida and his use of the internet. The CBI had the evidence they needed to prove their case, thus the accused admitted his guilt in this instance. The court convicted Arif Azim of violating Code Sections 418, 419, and 420 for the first time ever in a case involving cybercrime. The court concluded that a measured approach was warranted because the litigant was a juvenile

[15]*State by Cyber Crime Police v. Abudakar Siddique in Nidhi Arya*, 'Cyber crime scenario in India and judicial response' (2019) 3(4) IJTSRD 1108, 1111.
[16]*Avnish Bajaj v. State* 2005 (79) DRJ 576.
[17]*State v. navjot sandhu @ afsan master* Criminal Appeal Case No 373-375 of 2004 (decided by Supreme Court on 4 August 2005).
[18]*Andhra Pradesh State Road v. Income-Tax Officer* 1964 AIR 1486, 1964 SCR (7) 17.
[19]*CBI v. Arif Azim* (2008) 105 DRJ 721, (2008) 150 DLT 769.

(just 24 years old) and a first-time offender. Thus, the respondent was placed on a year's probationary status by the court.

(f) Harsh Sharma v. The State of Maharashtra[20]

Some employees have been charged with theft of data and programming from their superior, under sections 408 and 420 of the IPC, as well as sections 43, 65, and 66 of the IT Act. Except for that particular provision of the IPC, all of these subsections have already been dissected. Criminal infiltrate of trust by associate or labourer is governed by Section408 of the IPC, which states, "whoever, being a delegate or specialist or used as a specialist or specialist, and being in any capacity enriched in such cutoff with property, or with any space over property, completes criminal break of trust in respect of that property, will be repulsed with restriction of one or the other depiction for a term which may contact seven years."

Conclusion and Suggestions

Criminology, police science, law enforcement, and policing all face new challenges in the online world. Experts in the sector have seen cybercrime develop since the 1990s. The scale and character of crime and victimisation are shifting as a result of this rapid pace. The study of "the cause of crimes that occur in the cyber domain and their impact in the physical world" is the focus of a new field called Cyber Criminology, which arose in the 1990s. Legislative framework is crucial and requires periodic updates. Besides the legal framework, the National Cyber Security Strategy is also crucial. The ultimate goal is to provide a safe and reliable online environment in India for all users. A nation's cyber security document should detail its priorities in this area and explain how it plans to achieve its stated goals. Other crucial factors in cybercrime policing and investigation include the creation of Cyber Crime Investigation Modules, training for cybercrime investigators in Cyber Crime Investigation and Forensics, and the availability of equipment needed with the State Forensic Science Laboratories and infrastructure.[21]

Because of how the Internet has shrunk the world, crimes committed by psychological oppressors online are now receiving attention from all across the globe. Presently, cyberspace is used as a paradise by cyber fear mongers; large psychological militant organisations are exploiting data advancements, where they may select targets, choose weapons, and carry out their plans of attack both in the real world and online. The unique nature of cyber terrorism makes it difficult for law enforcement agencies to combat it using the same tools they use to combat more conventional crimes.[22]

In this millennium, cybercrime has become the most lethal pandemic the world has ever faced.[23] A cybercriminal can destroy websites and accounts by hacking and planting infections, carry out online fakes by moving assets from one corner of the globe to the other, gain access to extremely secret and delicate data, provoke recipients with email threats or offensive content, engage in charge cheats, engage in cyber sexual entertainment that includes children, and commit countless other crimes. Therefore, it is claimed that in the online world, nobody is safe.

Suggestions

There are certain suggestions that the author would like to propose for the effectiveness of the role of police. They are as follows:

- Increasing the amount of money allocated for training once every two years is one way to combat the threat posed by cyber terrorism. It is imperative that law enforcement officers receive improved training on the various sorts of criminal activity that can be found on the internet.

[20]*Harsh Sharma v. The State of Maharashtra* 2019 Cri LJ 1398 (High Court, Mumbai).
[21]Amritanshu Sharma and Dr Deepika Bhatnagar, 'A study of need for Police reforms in India in Cyber Crime Manner' (2020) 10(7) IJESC 26801.
[22]Hemraj Saini, Yerra Shankar Rao and TC Panda, 'Cyber Crimes and their Impacts: A Review' (2018) 2(2) IJERA 202.
[23]Used from the judgment of *Shreya Singhal v Union of India* AIR 2015 SC 1523.

- Every state should set up a specialised cybercrime investigation cell to investigate high-tech crimes.
- In order to establish methods that will assist in reducing the backlog of digital evidence, it is necessary to construct a platform that will track the timings of the reaction that the cyber security team provides to reports of criminal conduct online.
- a capacity to view the FIR that has been made available on police citizen portals in accordance with recommendations from the Supreme Court
- Encouraging People Who Have Been Victimized by Cybercrime to File Complaints
- The Necessity of Providing Officials with Training in Order for Them to Investigate Cybercrimes
- The Application of Data Analytical Tools in the Control and Supervision of Social Networking Sites.