Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0017

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

Cyber Crime in an India: An Observational Study

Prof.Kalpana S. Mukunde
Librarian,
Orange City College of Social Work, Nagpur,

Abstract:
The term "illegal act in which a computer is a tool or a goal or both" refers to cybercrime. Computer use has been incredibly widespread and popular in recent years. However, cybercrime has increased both domestically and abroad as a result of technology abuse in cyberspace. The law on technological information, 2000, was enacted by the Indian parliament with the goal of safeguarding the advancement system and controlling illegal activity in the cyber world. It was India's first international law to address technology in the areas of electronic banking, e-commerce, and e-governance, as well as sanctions and penalties for cybercrimes. The common forms of cybercrime and ways to prevent them will be covered in this document.

1.1 Introduction:

Cyber Crime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognized by the Information Technology Act. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation, it can be said that, Cyber Crime includes any illegal activity where computer or internet is either a tool or target or both. Cyber Crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Some of the newly emerged cybercrimes are cyber-stalking, cyber terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber-defamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet (Chaubey, 2012). Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber Crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds (Nayak, October 2013). Cybercrime is growing and current technical models to tackle cybercrime are inefficient in stemming the increase in cybercrime. This serves to indicate that further preventive strategies are required in order to reduce cybercrime. Just as it is important to understand the characteristics of the criminals in order to understand the motivations behind the crime and subsequently develop and deploy crime prevention strategies, it is also important to understand victims, i.e., the characteristics of the users of computer systems in order to understand the way these users fall victim to cybercrime. Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of

computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is Cyber Crime by the use of Internet (Hemraj Saini, 2012). Cyber Crime is a bi-product of the ever-increasing development in the areas of information and communication technology (ICT). The attackers mainly attack the confidential data of the organizations or personal information thereof. The most targeted organizations are hospitals, government offices, and police stations, financial. Institutions, Research and Development (R&D) organizations and other telecommunication firms etc (Shusmoy Kundu1, 2018).

2. Literature Review:

2.1 Goni, Osman, Md. Haidar Ali, Showrov, Md. MahbubAlam, Md. Abu Shameem(2022)authors of the papers are stated that Cyber Crime is a widespread issue globally. It encompasses a range of activities where individuals disrupt networks, steal sensitive and private information, compromise bank accounts, and unlawfully transfer funds for their own gain. As the computer has become integral to business, entertainment, and government, the significance of Cyber Crime, particularly through the Internet, has increased. Also known as computer crime, it involves using a computer to facilitate illegal activities, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or infringing on privacy. The issue of cybercrime and its effects on society manifest in various ways, including economic disruption, psychological issues, and threats to national security. Effectively reducing cybercrime relies on a thorough examination of its behaviours and understanding their consequences at different societal levels. Nowadays, the prevalence of cybercrime is steadily rising, causing significant distress for individuals. It not only inflicts suffering on people but also impacts other areas of life. Therefore, cybercrime is a significant offense perpetrated by those skilled in computing. This paper outlines the fundamental concepts surrounding cybercrime.

2.2 Khan, Saquib Ahmad (2020) Cybercrime refers to an "illegal activity where a computer is utilized as a tool or a target, or both." Recently, the use of computers has become increasingly widespread and popular. Nevertheless, the improper use of technology in cyberspace has resulted in cybercrime, both at a national and international level. To regulate criminal behaviour in the digital realm and safeguard technological advancements, the Indian Parliament enacted the Information Technology Act in 2000. This was India's first comprehensive legislation addressing technology in areas such as e-commerce, e-governance, electronic banking services, and the associated penalties and punishments for computer-related offenses. This document will explore the common forms of cybercrime and strategies for preventing it.

2.3 Jain, Neelesh andshrivastava, vibhash (2014) The Internet is frequently portrayed as an incredible tool, an engaging space, and a freeing experience… but for whom? Many of us face the risk of becoming targets of a rising number of criminals who adeptly manoeuvre through the Net. Cyberspace, commonly referred to as the Web, is an environment that is both intangible and ever-changing. This paper contends that Cyber Crime or e-crime represents a novel form of enterprise and advanced technology criminals. This paper provides an overview of cybercrimes, examining the individuals who commit them and their motivations. Additionally, I aim to discuss various cybercrimes in depth, as well as the distinct challenges and response issues that may arise

in prevention, detection, and investigation. I will also outline the different sections of the IT Act 2000 of India and suggest new provisions for this legislation.

4. Cybercrime Categories:

4.1 Cryptocurrency Crime

4.1.1 Cryptojacking: A cybercrime known as "crypto jacking" occurs when a criminal surreptitiously creates crypto currency using a victim's computer power.

4.1.2 Cryptocurrency-mining & Cloud Mining Scams: The resources of compromised computers are stolen by cryptocurrency-mining malware, which has a major negative impact on the machines' performance, power usage, and wear and tear.

4.1.3 Cryptocurrency Investment Frauds: Schemes that promise large returns on bitcoin investments, such as "pump and dump" schemes and giveaway scams.

4.2 Cyber Terrorism

The purpose of "Cyber Terrorism" is to incite fear in the populace or in any segment of the populace by threatening India's unity, integrity, security, or sovereignty.

* Preventing or causing someone who is authorized to access computer resources from doing so; or

* Trying to access or breach a computer resource without permission or going beyond what is permitted; or

* Introducing, or causing to be introduced, any computer contamination, and by doing so, causes or is likely to cause death, injury, or property damage or destruction, or damages or disrupts supplies or services that are necessary for community life, or has a negative impact on the vital information infrastructure.

4.3 Hacking / Damage to Computer Systems

Unauthorized access to a computer system or account is the act of compromising computer resources. Getting access to a computer system without the owner's explicit or tacit consent is known as this. Hacking is committed by anybody who destroys, deletes, or modifies any information included in a computer resource, reduces its value or utility, or otherwise negatively impacts it with the knowledge that he is likely to cause unjust loss or damage to the public. Computer system damage or hacking includes:

* Damage to computer, computer systems, etc.
* Email Hacking.
* Tampering with computer source documents.
* Unauthorised Access / Data Breach.
* Website Defacement / Hacking.

4.4 Online and Social Media Related Crime

The nation has seen an increase in online and social media crimes, which presents new difficulties as cybercriminals continue to develop their strategies and use cutting-edge technology. The following are some of the cybercrimes that are listed in the portal's Online and Social Media Related Crime category:

*Cheating by Impersonation
*Cyber Bullying / Stalking / Sexting

*E-Mail Phishing
*Fake/Impersonating Profile
*Impersonating Email
*Intimidating Email
*Online Job Fraud
*Online Matrimonial Fraud
*Profile Hacking / Identity Theft
*Provocative Speech for unlawful acts

4.5 online financial fraud

Unauthorized access, sabotage, or usage of computer systems with the goal of causing financial gain for cybercriminals or financial loss for victims are examples of online financial cybercrimes. It could entail computer fraud or forgeries, as well as hacking to get valuable or personal information for profit. Online financial frauds are on the rise as more people utilize the internet and mobile banking.

The following are some examples of cybercrimes that fall under the umbrella of online financial fraud:

*Business Email Compromise/Email Takeover
*Debit/Credit Card Fraud/Sim Swap Fraud
*Demat/Depository Fraud
*E-Wallet Related Fraud
*Fraud Call/Fishing
*Internet Banking Related Fraud
*UPI Fraud

4.6 Publishing/ Transmitting Explicit Material in Electronic Form

Section 67 or 67A of the IT Act punishes anyone who publishes, transmits, or causes to be published or transmitted in electronic form any material that contains sexually explicit acts or conduct, or that is lascivious, appeals to the prurient interest, or has the effect of tending to degenerate and corrupt individuals who are likely to read, see, or hear the matter contained or embodied in it, taking into account all relevant circumstances.

4.7 Ransomware

Cybercriminals remotely compromise and encrypt computer systems using ransomware, a fast developing type of cybercrime, and then demand a ransom to restore and/or protect data. Attacks using ransomware target both people and organizations.

A ransomware attack prevents users from accessing data that is stored on computer systems. Files and folders on local disks, connected devices, and even networked PCs can be encrypted by more dangerous ransomware variants.

4.8 Child Pornography/ Child Sexually Abusive Material (CSAM)

Any content that includes sexual images of a child who has been mistreated or sexually exploited is considered child sexually abusive material (CSAM). Publishing or sending any kind of electronic content that shows children engaging in sexually explicit behaviour is illegal. Section 67B of the IT Act 2000 addresses it.

One type of child sexual exploitation is child pornography. It is illegal to create, distribute, import, receive, or possess any kind of child pornography. A major offense is breaking the laws against child pornography and CSAM.

In April 2019, the National Crime Records Bureau (NCRB) in India and the National Centre for Missing and Exploited Children (NCMEC) in the USA signed a Memorandum of Understanding (MoU) to receive Cyber Tipline Reports on Child Sexual Abuse Material (CSAM) pertaining to India. This agreement paved the way for the establishment of a novel mechanism for information sharing and the prosecution of such offenders.

5. Statistics on Cyber Crime in India:

Cyber Crime in India has been increasing in recent years. In 2023, India was the third most targeted country in the world for cyber-attacks.In 2023, India reported over 11 million Cyber Crime complaints. In the first four months of 2024, India reported over 740, 00. 0 Cyber Crime complaints. India reported over 65,000 Cyber Crime cases in 2022. India reported over 1,400,000 Cyber Crime cases in 2021.

6. Actions to avoid cybercrime:

Adequate provisions are in place to address prevalent computer crimes under the Information Technology Act of 2000 and the Indian Penal Code. It stipulates sanctions in the form of fines or punishments based on the nature of cybercrime, with sentences ranging from two years to life in jail.

Nonetheless, the following actions have been taken by the government to stop cybercrime:

- The cybercrime cells were established in the States and territories of the Union to report and investigate cases of cybercrime.
- The government has set up IT research and forensic training laboratories in the states of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu and Kashmir for the training of the police and the judiciary in these states.
- To raise awareness and provide training, Cyber Forensic Labs were set up in Mumbai, Bangalore, Pune, and Calcutta in partnership with the Data Security Council of India (DSCI), NASSCOM.
- Programs for investigating cybercrimes. Court officials participate in a variety of awareness-raising and training initiatives on law and cybercrime from NALSAR University of Law in Hyderabad and National Law School in Bangalore.
- Police and judicial officers receive training in government-established training laboratories.
- The Universalization of Women Helpline initiative was authorized to offer all women impacted by the violence a 24-hour emergency and non-emergency response.

7. A Decade of Digital Threats and Legal Interventions:

India has seen a sharp increase in cybercrime between 2014 and 2024, which is indicative of both the nation's quick digital transition and the growth in cyberthreats that has coincided with it. The frequency of reported cyber incidents has sharply increased as a result of cybersecurity vulnerabilities becoming more evident as more people and companies adopt digital technologies. The severity of the problem is demonstrated by the fact that, although there were only about

9,622 cases of cybercrime in 2014, by the end of 2024, it is anticipated that there will be over 80,000. The extensive use of mobile phones, digital financial systems, and internet services are major factors contributing to this growth. While the growth of the economy has benefited from this expansion of digital infrastructure, cybercriminals have also benefited. Common forms of cybercrime during this period have included identity theft, ransomware attacks, data breaches, phishing schemes, and online fraud.

The Indian government has responded by taking a number of significant actions to fight cybercrime. The creation of the Indian Cyber Crime Coordination Centre (I4C), a central location for coordinating responses to cyber threats, has been one of the most important interventions. The National Cyber Crime Reporting Portal has also been introduced to enable citizens to report cyber incidents directly, with a particular focus on crimes against women and children. To strengthen the legal framework, the Information Technology Act (2000) has been amended multiple times to better address the complexity of modern cybercrimes. Law enforcement agencies have been trained to handle digital crimes more effectively, but challenges remain in terms of cybersecurity awareness and resources across the country. Stronger cybersecurity measures are urgently needed, as evidenced by the increasing number of attacks that target important sectors like government, healthcare, and finance. Government, business, and individual collaboration is essential to creating a resilient digital ecosystem in India, and as the nation continues to adopt new technologies, securing its digital future will depend on having strong cyber defences.

The Information Technology Act, 2000, was enacted to address crimes that arise from technological advancements, establishing a legal framework to combat the evolving landscape of cybercrimes. It specifically targets offenses such as hacking, data theft, and online fraud, providing necessary provisions for digital transactions and electronic records. Conversely, the Indian Penal Code (IPC) is a comprehensive legal document that encompasses traditional crimes like theft, assault, and fraud, which can also apply to cyber-related offenses when they occur in a digital context. Together, these laws ensure a robust legal approach for prosecuting offenders and delivering justice in cybercrime cases.

Conclusion:

These days, one of the most important issues facing nations worldwide is cybercrime. Includes violating security measures like passwords and privacy, as well as granting illegal access to information to anyone using the Internet. Cybercrime, or robbery carried out through a computer or the Internet, includes cyber theft. As the frequency of cybercrimes and frauds rises, the government is creating more stringent regulations to safeguard citizens' rights and shield them from any unfavourable online experiences. To further ensure data security and privacy, stronger regulations pertaining to the protection of "confidential personal data" have been developed in the hands of intermediaries and service providers (corporate bodies).

References:

- AnimeshSarmahand and AmlanJyotiBaruah (2017), Volume 04, Issue 06, PP. 1633-1640.
- Chaubey, P. R. (2012). An Introduction to Cyber Crime and Cyber law. In P. R.K.Chaubey, An Introduction to Cyber Crime and Cyber law. Kamal Law House.

- Cyber Crime: Rise, E. a. (2020, July 1). Retrieved July 1, 2020, from https://www.researchgate.net/publication/34434 9620
- Hemraj Saini, Y. S. (2012). Cyber-Crimes and their Impacts: A Review. 2(2).
- Nayak, S. D. (October 2013). IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES. 6(2).
- National Crime Records Bureau. (2024). Cybercrime statistics report: 2014-2024. Ministry of Home Affairs.
- Shusmoy Kundu1, 2. K. (2018). Cyber Crime Trend in Bangladesh, an Analysis and Ways Out to Combat the Threat. Dhaka-1216, Bangladesh: International Conference on Advanced Communications Technology (ICACT).
- Tripathy,SudhanshuSekhar (2024). A comprehensive survey of cybercrimes in India over the last decade, International Journal of Science and Research Archive, 2024, 13(01), 2360–2374
- https://aag-it.com/the-latest-cyber-crime-statistics/