Page 949 - 957

DOI: *https://doij.org/10.10000/IJLMH.115512*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 4

2023

Cyber Crime in India

NAWA UMAR[1]

ABSTRACT

Cybercrime is a growing concern worldwide, and India is no exception. With the rapid advancement of technology and increased internet penetration, the country has witnessed a surge in cybercriminal activities. This abstract provides an overview of the cybercrime landscape in India, highlighting its scope, impact, and measures taken to combat this menace. The abstract begins by addressing the significance of cybercrime in the Indian context. It outlines the various types of cybercrimes prevalent in the country, including hacking, online fraud, identity theft, cyber bullying, and data breaches. The abstract also sheds light on the motivations behind these crimes, such as financial gain, espionage, activism, and personal vendettas. The abstract discusses the consequences of cybercrime in India. It highlights the financial losses incurred by individuals, businesses, and the government due to cyber- attacks. It also emphasizes the potential risks to national security and the integrity of critical infrastructure systems. The impact of cyber bullying on individuals' mental health and the overall erosion of public trust in digital platforms are also addressed.

Keywords: *Cyber Crime, India.*

I. INTRODUCTION

Cybercrime refers to criminal activities that are committed using computers, networks, or digital devices. With the rapid growth of technology and the widespread use of the internet, cybercrime has become a significant concern worldwide, including in India. In this introduction, we will explore the issue of cybercrime in India.

India has experienced a significant increase in internet connectivity and digital adoption in recent years, with millions of people accessing the internet for various purposes such as communication, online transactions, and entertainment. While these advancements have brought numerous benefits, they have also given rise to new opportunities for cybercriminals.

Various forms of cybercrime exist in India, including hacking, phishing, online fraud, identity theft, cyber bullying, cyber stalking, online harassment, spreading malware, and unauthorized access to computer systems. These criminal activities often target individuals, businesses, and even government organizations, causing financial losses, reputational damage, and personal

[1] Author is a student at B.S. Anangpuria Institute of Law, Alampur, Faridabad, Haryana, India.

harm.

The motives behind cybercrimes can vary. Some perpetrators seek financial gain by stealing sensitive information, such as credit card details or bank account credentials, and using them for fraudulent purposes. Others may engage in cybercrimes for personal reasons, such as revenge, harassment, or blackmail. The Indian government has recognized the growing threat of cybercrime and has taken several steps to address it. The Information Technology Act, 2000, was enacted to provide legal frameworks for dealing with cybercrime and establishing penalties for offenses committed in the digital realm. Additionally, the establishment of dedicated cyber security agencies, such as the Indian Computer Emergency Response Team (CERT-In), has played a crucial role in combating cyber threats. Despite these efforts, cybercrime continues to be a significant challenge in India. Factors such as a lack of awareness, inadequate cyber security infrastructure, and limited digital literacy contribute to the vulnerability of individuals and organizations. Furthermore, the rapidly evolving nature of cyber threats makes it difficult for law enforcement agencies to stay ahead of the criminals. To effectively combat cybercrime, it is crucial to raise awareness about safe online practices, strengthen cyber security measures, and promote collaboration between government agencies, law enforcement, private organizations, and the public. By working together and staying vigilant, it is possible to mitigate the risks posed by cybercriminals and protect India's digital landscape.

II. TYPES OF CYBER-CRIME

- Phishing: The fraudulent attempt to obtain sensitive information, such as usernames, passwords, or financial details, by posing as a trustworthy entity in electronic communication.
- Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. This includes viruses, worms, ransomware, spyware, and Trojan horses.
- Hacking: Unauthorized intrusion into computer systems or networks to exploit vulnerabilities and gain access to sensitive information or control over systems.
- Identity Theft: The theft or misuse of personal information, such as Social Security numbers, credit card details, or bank account information, to impersonate someone else for financial gain.
- Cyber stalking: Persistent and unwanted online harassment, threats, or stalking behaviour targeting an individual or group, causing fear, distress, or emotional harm.

- Online Fraud: Various forms of fraudulent activities conducted online, such as online auctions scams, advance-fee frauds, credit card fraud, or investment fraud.
- Cyber bullying: The use of technology, such as social media platforms or instant messaging, to harass, intimidate, or humiliate others.
- Data Breach: Unauthorized access, acquisition, or disclosure of sensitive or confidential information, usually from a database or system, often resulting in the compromise of personal or financial information.
- Online Child Exploitation: The production, distribution, or consumption of child pornography, grooming, or engaging minors in sexually explicit activities through digital platforms.
- Financial Cybercrimes: Crimes targeting financial systems, including online banking fraud, ATM skimming, or hacking of financial institutions for monetary gain.
- Intellectual Property Theft: Unauthorized use, copying, distribution, or theft of copyrighted material, trade secrets, or intellectual property through digital means.

III. CAUSES OF CYBER CRIME

There are several factors that contribute to the causes of cybercrime. Understanding these causes can help in developing strategies to prevent and combat cybercriminal activities. Here are some common causes of cybercrime:

- Technological Advancements: While technology brings numerous benefits, it also creates opportunities for cybercriminals. The constant evolution of technology, including the internet, digital devices, and communication networks, provides new avenues for cybercriminals to exploit vulnerabilities and launch attacks.
- Anonymity and Impersonation: The anonymity offered by the internet makes it easier for cybercriminals to hide their identities and impersonate others. This anonymity allows them to carry out illegal activities without the fear of immediate consequences, making it challenging for law enforcement to track them down.
- Global Reach: The internet has a global reach, allowing cybercriminals to target victims across geographical boundaries. They can operate from one country while attacking individuals or organizations located in another, making it difficult for law enforcement agencies to coordinate efforts and apprehend offenders.
- Lack of Awareness: Many people are unaware of the potential risks and consequences

associated with cyber activities. This lack of awareness leads to individuals being less cautious and more susceptible to cyber threats such as phishing attacks, malware downloads, or falling for online scams.

- Inadequate Cyber security Measures: Insufficient security measures in computer systems, networks, and digital infrastructure create vulnerabilities that cybercriminals can exploit. Weak passwords, unpatched software, lack of encryption, and inadequate firewalls can make it easier for cybercriminals to gain unauthorized access and carry out their malicious activities.
- Financial Gain: Financial motives are one of the primary drivers behind cybercrime. Cybercriminals target individuals and organizations to steal sensitive financial information, such as credit card details or online banking credentials, which they can use for fraudulent purposes or sell on the black market.
- Lack of Legislation and Enforcement: In some cases, the absence of comprehensive cybercrime laws or weak enforcement mechanisms can embolden cybercriminals. When laws are not explicitly defined or enforced, cybercriminals may perceive lower risks and operate with a sense of impunity.
- Social Engineering: Cybercriminals often exploit human vulnerabilities through techniques such as social engineering. They manipulate individuals by using psychological tactics to deceive them into divulging sensitive information or performing actions that aid in their criminal activities.

IV. Legal framework

India has enacted laws to address cybercrime and provide a legal framework for dealing with various cyber offenses. The primary legislation governing cybercrime in India is the Information Technology Act, 2000 (IT Act), which has been amended over the years to keep up with technological advancements and emerging cyber threats. Information Technology Act, 2000: The IT Act is the main legislation governing cybercrime in India. It provides legal recognition to electronic records, digital signatures, and electronic transactions. The act also defines various cyber offenses, their penalties, and procedural requirements for investigation and prosecution.

- Section 43: This section of the IT Act deals with unauthorized access, damage, or disruption to computer systems, networks, or resources. It covers activities such as hacking, introducing viruses or malware, and causing damage to computer systems.

- Section 66: Section 66 of the IT Act focuses on various cyber offenses, including hacking with the intent to cause wrongful loss or damage, dishonestly receiving stolen computer resources, identity theft, and cyber stalking.
- Section 66A: This section, which was repealed by the Supreme Court of India in 2015, dealt with the offense of sending offensive or false messages through communication services. However, it was widely criticized for its potential misuse and infringement of freedom of speech, leading to its removal.
- Section 66B: Section 66B addresses the offense of dishonestly receiving stolen computer resources or communication devices.
- Section 66C: This section pertains to the offense of identity theft, where someone dishonestly uses another person's electronic signature, password, or any other unique identification feature.
- Section 66D: Section 66D deals with the offense of cheating by personation using a computer resource. It covers fraudulent acts committed online, such as impersonating someone else for financial gain or deceiving others through online platforms.
- Section 66E: This section addresses the violation of privacy by capturing, publishing, or transmitting the image of a private area of any person without their consent.
- Section 66F: Section 66F deals with cyber terrorism and provides penalties for offenses related to terrorist activities carried out through a computer resource.

V. PENALTIES

The penalties for cybercrime in India are primarily governed by the Information Technology Act, 2000 (IT Act), and its amendments. The severity of penalties depends on the specific cyber offense committed. Here are some of the common penalties prescribed under the IT Act:

- Unauthorized Access and Hacking:
    - Section 43: Penalty for unauthorized access, damage, or disruption to computer systems or resources is a fine of up to INR 5,00,000 (Indian Rupees) or imprisonment for a term that may extend up to 3 years or both.
    - Section 66: If hacking is committed with the intent to cause wrongful loss or damage, the penalty is imprisonment for a term that may extend up to 3 years and a fine that may extend up to INR 2,00,000.
- Identity Theft and Fraud:

  - Section 66C: Penalty for the offense of identity theft is imprisonment for a term that may extend up to 3 years and a fine that may extend up to INR 1,00,000.
- Cyber Stalking and Harassment:
  - Section 66A (repealed): Previously, under Section 66A, the penalty for sending offensive or false messages online was imprisonment for a term that may extend up to 3 years and a fine. However, this section has been repealed by the Supreme Court of India in 2015.
- Publication of Private Images:
  - Section 66E: The penalty for capturing, publishing, or transmitting the image of a private area of any person without their consent is imprisonment for a term that may extend up to 3 years and a fine.
- Cyber Terrorism:
  - Section 66F: For offenses related to cyber terrorism, the penalty is imprisonment for a term that may extend to life imprisonment.

VI. Prevention of cybercrime

Preventing cybercrime requires a proactive approach and the implementation of various preventive measures. Here are some key strategies and best practices for preventing cybercrime:

- Strong Cyber security Measures:
  - Use up-to-date antivirus software, firewalls, and intrusion detection systems to protect computer systems and networks.
  - Regularly update operating systems, software, and applications with the latest security patches and fixes.
  - Implement strong and unique passwords for all accounts, and consider using two-factor authentication for an added layer of security.
  - Encrypt sensitive data and use secure data storage and transmission methods.
  - Restrict user access rights and implement user authentication protocols.
- Cyber security Awareness and Training:
  - Educate individuals and organizations about common cyber threats, safe online practices, and the importance of data privacy.
  - Conduct regular cyber security awareness training programs for employees to

promote responsible online behaviour and help them identify and report potential cyber risks.

  - Encourage the use of secure browsing habits, such as avoiding suspicious websites, not clicking on unknown links or attachments, and being cautious while sharing personal information online.

- Data Protection and Backup:
  - Regularly back up important data and store backups in a secure location. This helps mitigate the impact of data loss or ransom ware attacks.
  - Implement data protection measures, such as encryption and access controls, to safeguard sensitive information from unauthorized access.
- Incident Response and Reporting:
  - Establish an incident response plan to effectively respond to and mitigate the impact of cyber incidents.
  - Encourage individuals and organizations to report cybercrime incidents to appropriate authorities, such as law enforcement agencies and computer emergency response teams (CERTs).
- Secure Online Transactions:
  - Ensure the use of secure and trusted websites for online transactions, especially for financial transactions.
  - Look for secure payment gateways and use encrypted connections (HTTPS) for transmitting sensitive information.
  - Be cautious about sharing financial information and use trusted payment methods.
- Regular System Audits and Vulnerability Assessments:
  - Conduct regular system audits to identify and address security vulnerabilities in computer systems and networks.
  - Perform vulnerability assessments and penetration testing to identify potential weaknesses and proactively address them.
- Collaboration and Information Sharing:
  - Foster collaboration between government agencies, law enforcement, private

organizations, and the public to share information about emerging cyber threats and preventive measures.

  - Participate in forums, workshops, and conferences focused on cyber security to stay updated on the latest trends and best practices.

- Regulatory Compliance:
  - Ensure compliance with relevant laws, regulations, and industry standards related to cyber security and data protection.
  - Regularly review and update internal policies and procedures to align with evolving cyber security requirements.

VII. Conclusion

Cybercrime poses a significant and evolving threat in today's digital age, including in India. The rapid growth of technology and the widespread use of the internet have created new opportunities for cybercriminals to carry out illegal activities, such as hacking, phishing, online fraud, and identity theft. The causes of cybercrime are diverse, including technological advancements, anonymity, and lack of awareness, inadequate cyber security measures, financial motives, and social engineering. To combat cybercrime effectively, it is crucial to have comprehensive legislation and enforcement mechanisms in place. In India, the Information Technology Act, 2000 (IT Act), serves as the primary legislation for cybercrime, defining various offenses and prescribing penalties. However, the landscape of cyber threats is constantly evolving, requiring continuous updates to laws and regulations to keep pace with emerging challenges. Preventing cybercrime requires a multifaceted approach that includes implementing strong cyber security measures, raising awareness about safe online practices, promoting cyber security education and training, establishing incident response plans, and fostering collaboration between government agencies, law enforcement, private organizations, and the public. By combining these preventive measures, we can strive to create a safer digital environment and protect individuals, businesses, and government entities from the devastating effects of cybercrime.

*****

VIII. REFERENCES

- R.K. Yadav, "Cybercrime in India: A Comprehensive Analysis," Indian Journal of Criminology and Criminalistics, Volume: 41 (2020).
- Neha Gupta, "Cybercrime and its Impact on Indian Society" Journal of Cybersecurity and Information Management, Volume: 8 (2019).
- Alok Gupta, "Emerging Trends in Cybercrime: A Study of Indian Cases" *International Journal of Cyber Criminology,* Volume: 13 (2019).
- Shalini Bhaskar, "Legal Framework and Challenges of Cybercrime in India" Journal of Indian Law Institute Volume: 60 (2018).
- Rajesh Kumar, "Cybercrime in India: An Analysis of the Role of Social Engineering," International Journal of Computer Science and Information Security Volume: 16 (2018).
- Priya Soni, "Cybercrime and Cybersecurity in India: A Review" Journal of Advances in Mathematics and Computer Science Volume: 30 (2018).
- Anupam Nagar, "Cybercrime Investigation and Challenges in India" International Journal of Advanced Research in Computer Science and Software Engineering Volume: 8 (2018).
- K. Jaishankar, "Cybercrime in India: Current Trends and Challenges" *Indian Police Journal* Volume: 65 (2018).
- K. Jaishankar, Cyber Crime: Concepts, Cases, and Controversies (Taylor & Francis, 2019).
- Debarati Halder and K. Jaishankar, Cyber Crimes in India: A Legal Perspective (Taylor & Francis, 2019).
- Pavan Duggal, Cyber Crime and Digital Evidence: Materials and Cases (LexisNexis, 2017).
- Debarati Halder and K. Jaishankar, Cyber Crimes Against Women in India (Sage Publications, 2017)
- Vivek Sood, Cyber Security and Cyber Laws (McGraw-Hill Education, 2017).
- N Suresh Kumar, Cyber Crimes: Law and Practice (CCH India, 2016).

*****