International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Crime and Its Impact in the Indian Society: An Analytical Study

Ruth Lalrinliani[1], Dr. Mridula Devi[2]

[1]Research Scholar, University School of Law & Research, University of Science & Technology, Meghalaya
[2]Associate Professor, University School of Law & Research, University of Science & Technology, Meghalaya

Abstract:
Advancement in technology brings various growths in the society. Even though due to improvements of new technologies positive impact has been found in different areas of life, but also rates of cyber crimes becomes substantially increased. Easy accessibility of computer and internet changes many areas of our life and also crime rates become increasing as cyber criminals discovered new ways to commit cyber crime which we never known before. Cyber crime is easily committed as the criminals can easily committed this type of crimes from anywhere and any place. It is now a multi-trillion dollar business for criminal organizations all around the world. India could not easily escape from this type of crime as the advance technology greatly took place in different areas of life. By committing cyber crime the perpetrators whether being an individual or group of individuals by using computer or computer technology can easily threatened or take money and property of the victims without their knowledge and permission. Even though various initiatives have been taken from different angles this type of crime still remains a threat to the development of society.

Keywords: computer, criminals, cyber crime, society, technology

INTRODUCTION

One of the greatest ability a human possesses is the ability to learn from others. Since the history of mankind everyone tries to learn from others, tries of becoming the best and the concept of 'survival of the fittest' made them to strive to achieve their goals lawfully and unlawfully. The society mostly depends on those who are in the center of more power and the powerful leaders have the ability to control the whole community. During the period of industrialization the power to control the society shifted from a single leader to a few industrialists. During this time powers were measured in terms of money. More money led to more powers and the rich people have great ability to control the society. In modern times most of the human activities depend on technology. Charles Babbage known as the father of Computer designed the Analytical Engine in the 1830s[1]. Since then various developments took place in the field of computer and communication technology. With the greatest development in technology, information technology now becomes the largest contributor to shift power in the hands of rich

[1] Charles Babbage - British inventor and mathematician (2024, July 23) https://www.britannica.com/biography/Charles-Babbage

industrialist to those possessing information. The internet and the computer network provided an efficient technique of transferring instant information globally and now we are living in a global village. Our time zone, language and even nationality never separate us and anyone from any parts of the globe can be easily connected through computer and internet connectivity.

Invention, technologies and discoveries not only enlarge our prospect but also pose some new challenges to the legal world.[2] Due to advancement in technology, the information and communication technologies have been transformed and the discovery computer has been a blessing to students, teachers, scholars, lawyers, business tycoons, doctors and many other professionals.[3] The information technology brings massive changes in our way of life. Before we got up from our bed in the morning and till we sleep at night, we deeply dependent on technology in one way or the other. It defines our new way of life; not only trained professionals but everyone can gain by using this new system. It is a blessing in life if we use it as ethical, helpful and without violating any rules and regulations. Not only landing of a man on moon or sending satellite into space numerous development and improvement happens in our day to day life. However, those improvements also bring negative impact in the society and become a curse at the same time. Internet offers innumerable opportunities for common people for a number of usages but in turn also makes it a haven for criminals to engage in a variety of criminal activities.[4] Computer and internet paved ways for cyber criminals to commit various fraud and criminal offences which involves huge amount of money as compared to the conventional crimes.

The first recorded cyber crime took place in the year 1820.[5] Since then various cyber crimes took place in different parts of the world. Cyber crime is a widespread issue; as computer and internet users are increasing every year new crimes have also emerged. It is very important to understand that the computer itself does not commit a crime but the people do. It is the human beings, not machines, who misuse, destroy and corrupt information.[6] Cyber criminal activities may take place in different scopes and areas but one common thing happens in every parts of the world is cyber crime not only affect individual but the society as a whole.

Statement of the problem

Cyber crime is one of the most common crimes worldwide, the criminals used advanced technology and the victims sometimes unaware of the loss caused to them. As compared to traditional crime committing of cyber crime is easier because face to face meeting with the victims are not necessary. Sometimes, when the victims find out the criminal activities happened to them many days has gone and it is burdensome to track the culprit as this type of crime does not have definite space or area. As crime is committed through computer or computer devices, it is difficult to catch the criminals red handed and the actual crime rate is difficult to record by the officials. The data provided by various agencies are only those reported by the victims and targeted person; it is undoubtedly true that the actual numbers of cyber crime incidents are much higher than the total reported case.

Objective of the Study

The objective of the study is to find out different types of cyber crime which largely affect the society, the impact of various cyber crime cases in the Indian society, the role of Judiciary in the criminal justice

[2] Singh, Y. (2002). *Cyber Laws.* The Indian Law Institute, Vol. 44.
[3] Khan, N. P. (2004). *Cyber crimes and the adequacy of the existing laws*. Indian Bar Review, Vol. XXXI (1&2), (2004).
[4] Verma, A. (2009). *Cyber Crimes & Law.* Central Law Publications.
[5] Nagpal, R. (2008). *Evolution of Cyber Crimes*. Asian School of Cyber Laws.
[6] Supra Note 4.

system and different steps taken by the Government to tackle this crime. The study will also make suggestions for improvement in the control and management of cyber crime cases in India.

Methodology

The methodology of this study is doctrinal legal research methodology based on different Acts, reports and judicial decisions passed by various courts in India. Records of the Government authority were used as secondary sources.

NATURE OF CYBER CRIME

There is no universal accepted definition of cyber crime. The term is used to describe criminal activity in which computers or computer networks are a tool, a target, or a place of cri minal activity and includes everything from electronic cracking to denial of service attack.[7] One distinct nature of cyber crime is it could easily be committed from anywhere without physically reach the victim and no eyewitnesses is needed. Physical violence and physical harm are not required. It may also be committed without the knowledge of the victim, but leaving him totally incapacitated at the same time. In many cases the victim recognizes the crime only after a huge loss or continual commission of crimes by the criminals.

CLASSIFICATION OF CYBER CRIMES

On the basis of the nature and purpose of offence, cyber crime may be broadly classified into three categories:

1. Cyber crime against individuals
2. Cyber crime against property
3. Cyber crime against society at large

The first category relates to which the effect mainly caused onto individuals or persons, some examples are:

- Harassment via e-mail - This type of cyber crime does not physically harm the victim but it may cause psychological harm and mental torture. It may be committed by sending unwanted, offensive, or intimidating electronic mails to another person.
- Cyber stalking – This is also known as ‘cyber teasing’. It involves following a person through various applications by using internet connection. It is an online course of conduct of a person by which the targeted person is terrorized, embarrassed, ashamed, molested, outranged of frightened.[8] The most common platforms used by the criminals are – Facebook, Instagram, X (previously known as twitter).
- Cyber defamation – Cyber defamation occurs when defamation takes place with the help of computer or by using internet. It has a deep negative impact as compared to traditional type of defamation because the criminals may easily spread defamatory matters widely by using internet connection. The results not only hurt the victim but it may harm their reputation forever.

The second category which is called as cyber crime against property does not caused direct harm to the individuals, but it greatly affect the property of the victims which results in a great loss due to the criminal acts. Some examples are –

[7] Chaubey, M.K. (2017). Cyber Crimes & Legal measures. Regal Publications.
[8] Ahmad, F. (2019). *Cyber Law in India (Law on Internet).* New Era Law Publication

- Intellectual property crimes – Intellectual property consists of a bundle of rights. The common forms of intellectual property rights violations are software piracy, copyright infringement, trade-mark and service mark violations, theft of computer source code etc.[9]
- Financial crime – Various cyber criminal activities involving financial loss to the victims are known as cyber financial crime. This type of crime includes cheating, credit card fraud, money laundering etc.
- Transmitting computer virus – 'Computer virus' means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.[10] Here the term 'damage' means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.[11] A person who introduces virus without the permission of the owner or in charge of computer or computer system etc., and that virus causes damage, etc. to such computer, computer system or computer network.

The third category is cyber crime against the society at large. In this type of crime the intention of the cyber criminals are threatening the Government or organizations as a result to fulfilling their demand. Those crimes mainly affect not a single individual but the society as a whole.

Cyber terrorism against the Government organization is the most common crime under this category. In cyber terrorism, a particular is not affected but it has its vicious impact on the community at large. This is a matter of global concern having both domestic as well as international implications.

Distribution of pirated software from one computer to another with an intend to destroy the data and official records of the government and accessing important information of Government or Organizations are the common types of crime under this category.

CYBER CRIME AND INDIAN SOCIETY

India witnesses various developments in communication and Information Technology. This also brings enormous growth in economy and financial status of the country. However, this technological improvements result in various criminal activities. India was placed on the 80th position in a report focusing on local threats in the year 2023.[12] Judiciary in India plays a significant role by various judicial pronouncement and many culprits are serving their punishment according to the relevant laws.

State of Tamil Nadu v. Suhas Katti[13] is the first case in India to set a benchmark on cyber harassment. This case was filed by a woman on the grounds of being harassed and getting obscene messages on various groups with the intention of offending her, which was sent by the man who was very keen in marrying her but she rejected him for which that person then started sending these kinds of obscene messages. The case involved questions of cyber chase/stalking and harassment of women. After taking all relevant evidences the Court convicted the accused under Sections 469 and 509 of Indian Penal Code, 1860 and Section 67 of the Information and Technology Act, 2000.

[9] Paranjape, V. (2023). *Cyber Crimes & Law.* Central Law Agency.
[10] Explanation (ii) to Section 43 of Information Technology Act, 2000.
[11] Explanation (iv) to Section 43 of Information Technology Act, 2000.
[12] The Hindu (2024, 21 February) https://www.thehindu.com/sci-tech/technology/india-the-80-most-targeted-country-worldwide-in-cybercrime/article67869960.ece
[13] CC No. 4680 of 2004

In the case of *State v. Salman Ansari*[14], Salman Ansari was charged under various Sections of Indian Penal Code, 1860 including Section 471 and also Sections 66B, 66C and 66D of Information Technology Act, 2000. He possessed many forged SIMs and he used to obtain ATM No., CVV No. and OTP No., from innocent account holders by impersonating himself to be bank officer and thereby he used to transfer the money in the forged bank accounts by creating several e-wallets. Court finds that he had committed offences under section 471 of the Indian Penal Code, 1860 and Section 66 of Information Technology Act, 2000. Therefore, court punished him under the said sections.

Vyakti Vikash Kendra, India Public Charitable Trust & Ors. v. Jitender Bagga and Anr.[15] is a case regarding removal of defamatory contents from blogging site. A defamation case has been filed against Google and Jitender Bagga who allegedly posted the derogatory content on blogger.com. The Court held that Google is an intermediary as per the law and that the Information Technology (Intermediary Guidelines) Rules, 2011 will be applicable on it. According to the rules, the court directed to remove the defamatory content against the applicants from Google's blogging website. The Delhi High Court held that Google has a deadline of 36 hours within which it has to remove derogatory content posted by blogger against art of living founder Sri Sri Ravi Shankar.

Ram Singh & Ors. v. State of NCT Delhi[16] is famously known as Nirbhaya case. In this case CD containing the media interview telecast on Zee News on January 4, 2013 was rejected by the learned Additional Sessions Judge on the grounds that the interview being a violation of section 327(3) of the Code was illegal, thus it could not be used as any evidence or previous statement. Here question arises whether the said CD is admissible or not. The High Court however permits the use of video CD in the trial court as evidence.

GOVERNMENT INITIATIVES

Progress in technology in turn results to threats in cyber space. The rapid changes and digitization of various sectors paved ways for cyber criminals to commit crimes not only to individuals but also to exploit and steal valuable data of the Government and organizations. The Indian Government feels the urgency to take positive efforts to battle this serious crime by providing various steps to mitigate the rising trends of cyber threats. Brief analyses of different Government initiatives are discuss below:

Information Technology Act, 2000:

The Information Technology Act, 2000 is the first and only Act passed by the Indian parliament which deals with electronic commerce and different modes crimes committed by the cyber criminals. This Act aimed to provide legal recognition for transaction carried out by means of electronic data exchange and other means of electronic communication, commonly referred to as 'electronic commerce' which involve the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing documents with the Government agencies.[17] The Act is comprises with 13 chapters spread over 94 sections and 4 schedules. After enforcing the Information Technology Act, 2000 four related important Acts – The Indian Penal Code, the Indian Evidence Act, the Banker's Books Act and the Reserve Bank of India Act were amended.

[14] Cyber Case No. 21 of 2021
[15] CS(OS) No. 1340 of 2012
[16] Crl. Rev. P. 124 of 2013
[17] Mishra, J.P. (2014). *An Introduction to Cyber Law.* Central Law Publication.

Information Technology (Amendment Act) 2008:

When time comes new methods of cyber crimes were committed by the criminals and various new techniques becomes relevant in the information communication world so that some provisions of the Information Technology Act, 2000 becomes ineffective to the present conditions. Therefore, the Information Technology (Amendment) Bill was passed by Lok Sabha on 22nd December, 2008 and by Rajya Sabha on 23rd December, 2008. The amended Act has omitted several sections, substituted for some other sections, expands the definition of cyber crime and new penalties for some offenses were added.

Establishment of the Indian Computer Emergency Response Team (Cert-In):

The Indian Computer Emergency Response Team (CERT-In) is the Indian Government's established nodal agency to response computer security incidents as and when they occur. This agency is situated inside the Department of Information and Communications Technology. The main objective of this agency is establishment of incident response as provided under Section 70B of the Information Technology Act, 2000. Operating a 24x7 incident response Help Desk, CERT-In ensures timely responses to reported cyber security incidents. The organization offers comprehensive Incident Prevention and Response services alongside Security Quality Management Services to enhance cyber security measures across the nation.[18]

The CERT-In plays an imperative role in safeguarding India's cyber landscape. According to the Information Technology Amendment Act, 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:[19]

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Co-ordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed.

The Indian Computer Emergency Response Team (CERT-In) since its operation in the year 2004 has registered several cyber crimes cases. The following table shows the cases registered by the agency during the last three years –

Table 1: Cases Registered by the Indian Computer Emergency Response Team between 2021 - 2023

Sl. No.	Year	Phishing incidents	Network scanning and probing	Virus/Malware incidents	Website hacking incidents	Cyber Security incidents
1.	2021	215	86585	9203	18	122764
2.	2022	1145	10220	2559	57	27482
3.	2023	401	12330	1185	39	23158

[18] Ministry of Electronics & IT (2024, 25 July). Safeguarding India's Digital Landscape Key Government's Initiatives to Enhance Cybersecurity Awareness https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2037115#

[19] Indian Computer Emergency Response Team https://www.cert-in.org.in/

(The above data was provided by Minister of State Electronics & Information Technology (MoS) Jitin Prasada on 24th July, 2024 in Lok Sabha)

Indian Cyber Crime Coordination Centre:

Indian Cyber crime Coordination Centre (I4C) is an initiative of the Ministry of Home Affairs, Government of India to deal with cyber crime in the country in a coordinated and comprehensive manner. I4C focuses on tackling all the issues related to Cyber crime for the citizens, which includes improving coordination between various Law Enforcement Agencies and the stakeholders, driving change in India's overall capability to tackle cyber crime and to improve citizen satisfaction levels.

National Cyber Crime Reporting Portal (NCRP):

The Government of India with the initiatives of Ministry of Home Affairs created the National Cybercrime Reporting Portal (NCRP) and was launched on 30th August, 2019. By log in to **"www.cybercrime.gov.in"** the users can access online portal to make complaints of all types of cyber related cases to the concern authority. Other than lodging complaints users can also upload relevant evidence, and track the progress of their cases. The portal also offers resources, including cyber safety tips and guidelines to help users prevent cyber incidents. Managed by law enforcement agencies, the National Cyber Crime Reporting Portal aims to safeguard digital infrastructure, promote cyber security awareness, and ensure prompt action against cyber offenders to uphold digital safety across India.[20]

Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS):

Financial fraud is one of the most common types of cyber crime in India. To prevent citizens from various cyber financial fraud and to take effective actions the Government of India established Citizen Financial Cyber Frauds Reporting and Management System. Whenever cyber financial fraud happens the victims can quickly report the case and through this system effective steps could be easily taken by the officials. Any victim of financial cyber fraud can dial toll free helpline number "**1930"** or report the incident on National Cybercrime Reporting Portal **"www.cybercrime.gov.in".** Not only individual but also Bank or financial intermediary or payment wallet can also report financial cyber fraud through this reporting system.

The Cyber Surakshit Bharat Initiatives:

The Cyber Surakshit Bharat Initiative is one of the most important initiatives of the Ministry of Electronics and Information Technology (MeitY), Government of India. One important mission of CSB is to spread awareness about cyber crime and the main objectives of the programme was to educate & enable the Chief Information Security Officers (CISO) & broader IT community of Central/State Governments, Banks and Public Sector Undertaking to address the challenges of cyber security in partnership with the Industry. The key objectives thus defined were:[21]

- Create awareness on the emerging landscape of cyber threats
- Provide in-depth understanding on related solutions
- Applicable frameworks, guidelines & policies related to cyber security
- Share best practices to learn from success & failures
- Provide key inputs to take informed decision on Cyber Security related issues in their respective functional area.

[20] National Government Services Portal https://services.india.gov.in/service/detail/national-cyber-crime-reporting-portal
[21] The Cyber Surakshit Bharat Initiative https://thegfce.org/initiative/the-cyber-surakshit-bharat-initiative/

It is noteworthy to mention here that between June 2018 and February 2024, the National e-Governance Division (NeGD) has efficaciously conducted 42 batches of CISO deep-dive training programmes for over 1,574 CISOs and frontline IT officials.[22]

CONCLUSION & SUGGESTIONS

Due to greatest development in the field of Information Technology, cyber crimes in various forms become universal issue. Even in India, data shows that the various crime rates are increasing year by year and involvement of monetary value become huge amount. 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India so that States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of cyber crimes in their respective area through their Law Enforcement Agencies. The Central Government is taking various initiatives to mitigate cyber crime by organizing trainings, conducting awareness campaigns, establishing cyber crime reporting portal, creating toll free help line for the needy. However, those steps taken by the Central Government could only become more effective by providing good cooperations between the Central and State Governments. From the given data among 36 States and UTs all over the country a total number of 8 States/UTs Government does not set up separate Cyber Crime Police Station in their territory; 17 States/UTs have less than 5 Cyber Crime Police Stations and only 8 States/UTs have more than 10 Cyber Police Stations in their respective areas. From this analysis it is clear that the mechanism of the Law Enforcement Agencies needs to strengthen to discharge their functions more effectively. Not only by establishment of separate Cyber Crime Police Station but also recruiting more Officers and qualified Staff possessing computer knowledge, upgrading investigating tools and techniques, spreading awareness among general public is sine qua non. The Judiciary plays an extensive role in bringing justice between the criminals and the victims; however, there is still a room for advancement in criminal justice system. It is also necessary to allocate more budgets for cyber crime department in all States and Union Territories. Everyone irrespective of gender, age, occupation or region have a fundamental duty to fight back this social evil. Our skills and ability might be different but giving our greatest efforts will surely make positive change.

BIBLIOGRAPHY & REFERENCES:

1. Ahmad, F. (2019). *Cyber Law in India (Law on Internet).* New Era Law Publication.
2. Charles Babbage - British inventor and mathematician (2024, July 23) https://www.britannica.com/biography/Charles-Babbage
3. Chaubey, M.K. (2017). Cyber Crimes & Legal measures. Regal Publications
4. Indian Computer Emergency Response Team https://www.cert-in.org.in
5. Khan, N. P. (2004). *Cyber crimes and the adequacy of the existing laws*. Indian Bar Review, Vol. XXXI.
6. Ministry of Electronics & IT (2024, 25 July). Safeguarding India's Digital Landscape.
7. Key Government's Initiatives to Enhance Cybersecurity Awareness https://pib.gov.in/PressRelease
8. Mishra, J.P. (2014). *An Introduction to Cyber Law.* Central Law Publication.
9. Nagpal, R. (2008). *Evolution of Cyber Crimes*. Asian School of Cyber Laws.
10. National Government Services Portal https://services.india.gov.in/service/detail/national-cyber-crime-reporting-portal

[22] Ministry of Home Affairs (2023) https://pib.gov.in/PressRelease

11. Paranjape, V. (2023). *Cyber Crimes & Law.* Central Law Agency.
12. Singh, Y. (2002). *Cyber Laws.* The Indian Law Institute.
13. The Cyber Surakshit Bharat Initiative https://thegfce.org/initiative/the-cyber-surakshit-bharat-initiative/
14. The Hindu (2024, 21 February).
15. The Information Technology Act, 2000.
16. Verma, A. (2009). *Cyber Crimes & Law.* Central Law Publications.