IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Cyber Crime in the Society: Problems and Preventions

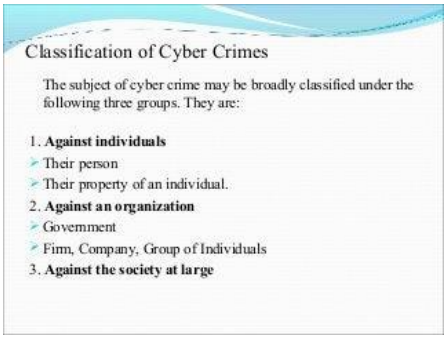
Pranjali Janardan Sheramkar
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *A parallel way of living and existing is the digital world of today. Things that the general public can now do that were unthinkable only a few years ago. Because of the increasing reliance of humanity on these computers, the Internet is quickly becoming a way of life and a means of living for millions of people. The internet has made it possible to use email, websites for communication, and many other anytime, everywhere IT solutions for the benefit of humanity. Cybercrime is becoming a significant threat. Governments, police forces, and intelligence agencies all across the world have begun to respond. Initiatives to reduce international cyber threats are beginning to take form. Special cyber cells have been established by the Indian police nationwide, and training has begun..*

Keywords: Cyber crime, Cyber Laws, Information Technology Act

I. INTRODUCTION

Man has a reputation for being a criminal due to his fall. In the face of development, crime is nevertheless elusive and constantly tries to elude detection. Depending on the type and severity of crime, different countries have implemented various tactics to combat it. A country with a high incidence of crime cannot thrive or flourish, that much is evident. Because crime is the polar opposite of growth, this is the case. It has detrimental social and economic repercussions. Cybercrime is characterized as crimes performed online using a computer as a tool or a specific target. Since many crimes change every day, it is quite challenging to divide them into discrete categories. Despite the fact that offences like.



It just depends on which of the two is the major objective whether the computer or the person using it are victims. So, for the sake of simplicity, let's just consider the computer as either a target or a tool. Attacks on the data and other resources of the computer, for instance, constitute hacking. It is crucial to keep in mind that overlapping occurs frequently and that there is no such thing as a flawless classification system. The phrase "cybercrime" is misleading. Any statute or Act passed or adopted by the Indian Parliament does not define this term in any way. Cybercrime and traditional crime have similar concepts that are not fundamentally different. Both comprise behaviour, whether an action or an inaction, that violates legal standards and is balanced by

II. COMPUTER AS A TOOL

Computers might be viewed as tools rather than targets in cybercrime when people are the primary targets. As the damage is visible in the real world, these crimes typically require less technological expertise. Usually, human shortcomings are taken advantage of. It is more challenging to take legal action against the versions since the harm is primarily psychological and intangible. These offences have been committed for ages offline. Even before the advancement of high-tech technology, scams, thievery, and similar crimes existed. Simply put, the same offender has been handed a tool that broadens his possible victim base and makes him more difficult to track down and capture.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

III. COMPUTER AS A TARGET

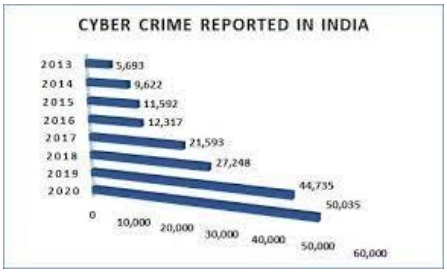
A particular set of criminals are responsible for these crimes. These crimes call for technical expertise from the offenders, unlike crimes that use computers as tools. Since computers have only been around for a short while, these crimes are relatively new, which explains how unprepared society and the rest of the world is to confront them. This kind of crime is frequently performed online every day. However, it is important to note that Nigerians and other Africans have not yet acquired the necessary technical know-how to support and commit this type of crime.

IV. CONVENTIONAL CRIME

As long as there has been human society, crime has existed as a social and economic reality. Crime is a legal notion with legal consequences. "A legal error that can be followed by criminal proceedings and lead to punishment" is what is known as a crime or an offence. Criminal activity is characterized by a violation of the law. According to Lord Atkins, there is only one test that may determine if an act is criminal: whether it is illegal and subject to punishment. Any behavior that is accompanied by a legal act or omission, the violation of which results in penalties, is said to constitute a crime.

V. CYBER CRIME

"Those species, of which the genus is the conventional crime, and where either the computer is an object or the subject of the behavior constituting crime," is the definition of cybercrime. Any criminal activity that uses a computer, whether as a tool, a target, or a means of committing other crimes, is considered a cybercrime. Generally speaking, "criminal action in which a computer is either a tool, a target, or both" is what is meant by cybercrime. Only a few examples of the activities that the computer may be used for include financial crimes, the selling of illegal goods, pornography, online gambling, crimes involving intellectual property, email spoofing, forgery, cyber defamation, and cyber stalking.



However, the computer may be used in the following illegal activities: unauthorized access to computers, computer systems, or computer networks; theft of information stored in electronic form; e-mail bombing; data theft; salami attacks; logic bombs; Trojan attacks; theft of computer systems; and physical damage to computers.

VI. CAUSES OF CYBER CRIME

Cybercriminals always choose the fastest path to huge profits. They target wealthy individuals or wealthy institutions where a lot of money is transacted daily, such as banks, casinos, and financial corporations, and they hack private data from these targets. It is challenging to apprehend such crooks. As a result, there are now more cybercrimes occurring worldwide. Because of their vulnerability, computers must be protected and secured from cybercriminals by regulations. The following reasons for computers' susceptibility could be listed:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

- **Capacity to store data in comparatively small space**: Data can be stored on a computer in an unusually little amount of space. It is made considerably simpler by the ability to remove or derive information using either a physical or virtual medium.
- **Easy to access**: The difficulty in protecting a computer system from unauthorised access is that there is always a chance of a breach caused by complex technology rather than by human error. Key loggers that can steal access codes, sophisticated voice recorders, retina imagers, etc. that can trick biometric systems, and firewall-bypassing logic bombs can all be used to get past numerous security systems.
- **Complex:** Operating systems, which are made up of millions of lines of code, are what allow computers to function. It is unlikely that there will never be a lapse because the human mind is flawed. These gaps are exploited by the online criminals, who gain access to the computer system.
- **Negligence:** Negligence and human behaviour are intimately related. Therefore, it is highly likely that mistakes could be made when protecting the computer system, allowing a cybercriminal to access and take control of the computer system.
- **Loss of evidence:** Since all the data are frequently destroyed, loss of proof is a very frequent and visible issue. This system of crime investigation is further crippled by the continued acquisition of data outside of the territorial range.

VII. TYPES OF CYBER CRIMES

There are many types of cyber-crimes and the most common ones are explained below:

- **Hacking:** It is a straightforward phrase that denotes delivering unauthorised commands to any other computer or network. In this instance, a person's computer has been compromised, allowing access to personal or sensitive data. The offender may not be aware that his computer has been accessed remotely since he utilises a variety of software to break into the victim's PC.

Because they assist them obtain reputation, which is then fueled by aggressive media attention, government websites are frequently a top target for hackers. This differs from ethical hacking, which is a technique employed by many firms to assess the effectiveness of their Internet security measures.

- **Child pornography and Abuse:** The use of the internet to sexually abuse minors is very common. This is another sort of cybercrime, where criminals use chat rooms to recruit children for the production of child porn.Every country's cyber security division spends a lot of time watching chat rooms that are popular with kids in an effort to curtail and stop child abuse and solicitation.
- **Piracy or Theft**: When someone downloads illegally and breaches copyrights, they are committing this crime. Even peer-to-peer websites exist that support software piracy, and the FBI is currently targeting a number of these websites. The legal system is currently dealing with this criminality, and there are rules that forbid unauthorised downloading. Film directors and producers are frequently the targets of this crime.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

- **Cyber Stalking**: This is a form of internet harassment where the victim receives a deluge of emails and messages. These stalkers typically know their targets, so instead of engaging in offline stalking, they turn to the Internet. To make the victims' lives worse, they start offline stalking in addition to cyber stalking if they observe that it is not having the desired impact.
- **Cyber Terrorism:** Information warfare, also referred to as cyber terrorism, is an act of Internet terrorism that involves planned, extensive, and disruptive attacks on computer networks using computer viruses, or actual physical attacks using malware, in order to target specific people, governments, and organizations. The purpose of terrorism is to instill fear in the minds of its victims. This idea makes it simpler to tell between cyber attacks carried out for financial or narcissistic gain from cyber terrorism. Cyber terrorist'spriorities causing harm and destruction in all of their operations.
- **Identity Theft**: With more individuals using the Internet for banking and currency transactions, this has grown to be a significant issue. In this type of cybercrime, a perpetrator gains access to information about a victim's bank account, credit cards, debit card, Social Security number, and other sensitive data in order to steal money or make purchases online in the victim's identity. It may cause the victim to suffer significant financial losses and possibly damage their credit history.
- **Computer Vandalism:** Computer vandalism is a form of harmful behaviour that involves disrupting businesses and perhaps causing damage to computers and data in various ways. The construction of malicious software intended to carry out damaging actions like deleting hard drive data or stealing login credentials is a common method of computer vandalism. Computer theft is distinct from viruses, which affix themselves to already-running software.
- **Malicious Software**: These are software or programmers that run through the Internet and are used to interfere with networks. The software is used to break into a system in order to steal confidential data or information or to harm any installed software.
- **Fraud Calls/e-Mails:** You must have read and heard a lot about this crime, and you might have even received a call from a con artist. Vising, also known as voice phishing, is the term for it. This form of crime involves a criminal contacting you via bogus texts, calls, or emails in which he claims to be a bank employee and tells you that the call is about your bank account or credit cards. He requests private information, such as the PIN for an ATM card, an OTP, a password, etc., or he requests that you click on a URL that he has supplied. You will lose the money in your account if you give them the information out of a misplaced sense of confidence. Remember that no bank will ever ask you for critical information; never share any information related to your account on the internet or to an unknown person.
- **Fake news sharing in social media:** Some online predators only use social networking sites to disseminate social, religious, and political rumors. Because they are impressed by this, regular people unintentionally share links or posts shared by strangers on social media. Remember that publishing any unauthorized links or posts on social media falls under the area of cybercrime, which exposes the user to legal punishment. Therefore, stay away from them and avoid working on social media on someone else's behalf because doing so could wreck your entire life.
- **Online illegal selling (Dark Web):** On an illicit online marketplace, a criminal sells the victim illegal weapons, drugs, smuggled items, or personal information while also conducting the transaction using crypto currency. It encourages both black marketing and terrorism. This is content from the World Wide Web that is available on Darknets, networks, for instance, but requires particular software, configuration, or authorization to access. On this website, every unlawful activity is transacted. You could be thinking that if something is illegal, very few people would use it. However, you would be wrong because there are millions of users worldwide, and that number is growing every day.

VIII. THE ABOVE-MENTIONEDOFFENCES MAY DISCUSS IN BRIEF AS FOLLOWS:

1. **Harassment via E-mails:** Email harassment is not a novel concept. It is quite comparable to letter-based harassment. I recently got a mail from a woman complaining about the same thing. Her ex-boyfriend was

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

sending her emails on a regular basis, sometimes threatening her and using them as a sort of emotional blackmail. This is a very typical form of email harassment.

2. **Cyber-stalking:** According to the Oxford Dictionary, stalking is "pursuing covertly." Cyberstalking entails tracking a person's online travels via sending emails to the victim nonstop, frequenting chat rooms the victim frequents, putting messages (often threatening) on bulletin boards the victim frequents, etc.
3. **Dissemination of obscene material/ Indecent exposure/Pornography (basically child pornography) / Polluting throughindecent exposure:** Online pornography can take many different forms. It can also entail hosting websites that contain these forbidden materials. These offensive things are created using computers. Downloading offensive content off the Internet. The adolescent's mind could be harmed by these offensive topics, which have a tendency to deprave or corrupt it. The BalBharati case in Delhi and the Bombay case, in which a Swiss couple used to compel slum children to pose for pornographic photos, are two instances of pornography that are well-known. Later, the Mumbai police detained them.
4. **Defamation:** It is a crime to accuse someone of something with the goal to damage their standing among right-thinking people in general, to have them avoid them, or to expose them to hatred, contempt, or ridicule. Except for the use of a virtual medium, cyber defamation is identical to traditional defamation. For instance, Rohit's email account was hacked, and emails about his relationship with a female were shared to some of his classmates with the intention of slandering him.
5. **Unauthorized control/access over computer system:** Hacking is a frequent term used to describe this action. To avoid confusion, we will not use the terms "unauthorised access" and "hacking" interchangeably because the terms used in the Act of 2000 have a considerably broader definition than hacking and the Indian law has given the term hacking a different connotation.
6. **E-mail spoofing:** One that falsely claims to be from someone else is referred to as a faked email. It demonstrates that the origin of the thing is not where it actually comes from. Recently, fraudulent emails with Mr. Na. Vijayashankar's (naavi.org) name were sent out and carried viruses. Rajesh Manyar, a graduate student at Indiana's Purdue University, was detained after making threats to set off a nuclear weapon on the university's property. The purported email was sent to the vice president for student services from the account of another student. However, it was discovered that Rajesh Manyar's account was used to send the email.
7. **Computer vandalism:** Vandalism refers to the willful destruction or damage of another's property. Therefore, any physical injury done to a person's computer falls within the definition of computer vandalism. These behaviours can include physically harming a computer or its peripherals or stealing a computer, a component of a computer, or a peripheral connected to the computer.
8. **Intellectual Property crimes / Distribution of pirated software:** A collection of rights comprise intellectual property. An offence is any unlawful conduct that wholly or partially denies the owner their property rights. Software piracy, copyright infringement, trademark and service mark infringement, theft of computer source code, etc. are examples of prevalent IPR violations. In a landmark decision, the Hyderabad Court found three people guilty of illegally duplicating and selling pirated software and sentenced them to six months in jail and fines of 50,000 apiece.
9. **Cyber terrorism against the government organization:** It might be necessary at this point to make a distinction between cyber terrorism and cybercrime. Both actions are unlawful. However, it is imperative to distinguish between the two of these offences. Cybercrime is typically a domestic problem with potential worldwide repercussions, but cyber terrorism is a global problem with both domestic and global repercussions. These terrorist assaults on the Internet typically take the shape of distributed denial of service attacks, attacks on sensitive computer networks, attacks on hate websites and emails, etc. Terrorists that are adept at using technology are employing 512-bit encryption, which is nearly hard to decrypt. One recent instance is Osama Bin Laden's LTTE attack on the American army's deployment system.
10. The employment of disruptive activities, or the threat of doing so, in cyberspace with the goal to achieve social, intellectual, religious, or political objectives, or to terrorise anyone in promotion of such objectives, is known as cyber terrorism. Another definition might be made an attempt to encompass all cyber terrorism

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

within its scope.In order to: i. instill fear in the public or any section of the public; ii. adversely affect the harmony between various religious, racial, linguistic, or regional groups, castes, or communities; iii. coerce or overthrow the government established by law; or iv. cause property damage; a terrorist is defined as someone who engages in wanton killing of people, violence, disruption of services or means of communications essential to the community, or any combination A cyber terrorist is someone who uses a computer system to further the aforementioned goals. Every action taken in support of it constitutes a cyber terrorist act.

11. **Trafficking:** Different types of trafficking exist. It could involve the trafficking of drugs, people, weapons, etc. Because these types of trafficking operate under aliases, they are not being stopped. In Chennai, a ring that was selling drugs under the alias "honey" was arrested.
12. **Fraud & Cheating:** One of the most lucrative industries expanding in the internet nowadays is online fraud and cheating. It could take on several shapes. The Court of Metropolitan Magistrate in Delhi recently found a 24-year-old engineer working in a call centre guilty of fraudulently obtaining the details of Campa's credit card and purchasing a television and a cordless phone from Sony's website. These are just a few of the cases of online fraud and cheating that have come to light. Others involve credit card crimes, contractual crimes, offering jobs, etc. Azim was found guilty of cheating under the IPC by Metropolitan Magistrate Gulshan Kumar, however he was not imprisoned. Azim was instead released after a year on probation and asked to post a personal bond of Rs 20,000.

IX. STATUTORY PROVISIONS

1. The Information Technology Act, 2000
2. The Indian Penal Code, 1860
3. The Indian Evidence Act, 1872
4. The Banker's Book Evidence Act,1891
5. The Reserve Bank of India Act, 1934.

Chapters IX and XI of the Information Technology Act address numerous cybercrimes. The crucial paragraphs are Ss. 43, 65, 66, and 67. In particular, Section 43 addresses instances of illegal access, unauthorized downloading, virus attacks, or other contaminants that cause harm, interruption, denial of access, or interference with a person's usage of a service. As a remedy, this clause offers a fine of up to Rs. 1 crore. Section 65, which deals with "tampering with computer source documents," has a maximum sentence of 3 years in jail, a maximum fine of 2 years, or both. Section 66, which deals with "hacking with computer systems," carries a maximum sentence of 3 years in prison, a maximum fine of 2 years, or both. Section 67 also addresses.

X. ANALYSIS OF THE STATUTORYPROVISIONS

At a time when there was no regulation governing this specialized area, the Information Technology Act 2000 was unquestionably a positive development. The Act, however, has in some ways proven to be insufficient when put into practice. The Act's many gaps include the following:

The legislation's hasty passage, without much public discussion, did not really achieve the desired result. The haste with which the legislation was approved by the parliament, according to experts, and the fact that not enough time was granted for public debate are both contributing factors to its insufficiency.

1. **Cyber laws**: They explicitly mention that their goal is to support e-commerce and that they are not intended to control cybercrime in their prologue and purpose. According to Mr. PavanDuggal, the I.T.Act 2000 was created with the primary goal of establishing legislation to govern e-commerce, which is also one of the reasons it is insufficient to address instances of cybercrime.
2. **Cyber torts:** Recent instances of cyber defamation, cyber stalking, cyber harassment, and cyber nuisance have demonstrated that the I.T.Act 2000 does not address these offences. Furthermore, it is argued that new types of cybercrime will develop in the future and will need to be addressed. India should therefore ratify the cybercrime convention. However, these felonies are subject to the I.T.Act 2000 when read in conjunction with the Penal Code.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

XI. PREVENTION OFCYBERCRIME

Prevention is always preferable to treatment. It is usually advisable to exercise some caution when using the internet. They should be integrated into A's online life. The mantra for online security, according to SaileshkumarZarkar, technical advisor and network security consultant to the Mumbai Police Cyber Crime Cell, is Precaution, Prevention, Protection, Preservation, and Perseverance. A netizen should be aware of the following:

1. Avoid revealing any details about oneself online to avoid being stalked. This is equivalent to telling whole strangers who you are in public.
2. As there have been instances of photographs being misused, it is best to avoid sending any photos online, especially to strangers and chat pals.
3. To protect yourself from malware attacks, always use the most recent and updated antivirus software.
4. Constantly maintain backup volumes to prevent data loss in the event of virus contamination.
5. Never enter your credit card information on an unsecured website to avoid fraud.
6. Since leaving the cookies unprotected could be fatal, it is preferable to use a security application that gives control over the cookies and sends information back.
7. Website owners need to monitor traffic and look for any anomalies on the site.This could be achieved by installing host-based intrusion detection systems on servers.
8. Using firewalls could be advantageous.
9. Internal company networks must be physically separated from web servers hosting public website Adjudication of a Cyber Crime - In accordance with the Bombay High Courts directives. Government determined, by notification dated March 25, 2003, that each state's. as the AO

XII. CONCLUSION

The human mind has an incomprehensible capacity. Cybercrime cannot be completely eradicated from the internet. You can definitely check them. History demonstrates that no piece of legislation has ever been able to completely eradicate crime from the world. Making individuals aware of their rights and responsibilities as well as tightening the law's enforcement are the only steps that can be taken to reduce crime.

XIII. ACKNOWLEDGMENT

We would like to acknowledgment the University of Mumbai, Mumbai, India to give us the opportunity to do the research work under the title ***"Cyber crime in the society problem and prevention".*** We would like to acknowledge the college L.B.H.S.S.T's ICA Bandra East, Mumbai, India to support us during the research process. I would like to express my gratitude to Professor Sandhna Pande. For this continuous support during the research process.

REFERENCES

[1]. Cyber Crime Today &Tomorrow, ThiruDayanithiMaran.
[2]. Duggal Pawan – The Internet: Legal Dimensions
[3]. Mehta Dewang- Role of Police in Tackling Internet Crimes
[4]. Nasik Police play big boss for internet voyeurs, Hindustan Times, Sunday, Oct 28, 2007.
[5]. Nowa Pune base for net's cyber cops The Hindu Sunday Nov 26 2006.
[6]. Youth in jail for sending email threat, The Hindu Friday August 10, 2007.