IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER CRIME AND SOCIETY: AN ANALYSIS

Neeraj Kumar Rai
Asst.Professor
Govt.Girls Degree College
Dhindhui,Patti,Pratapgarh

ABSTRACT: Cyber-crime is a crime that involves a computer and networks .The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health. There are many privacy concerns surrounding Cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including financial theft and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyber warfare. Research Paper is based on secondary sources.

KEY WORD: Cybercrime, Computer related offences, Computer source

The concept of crime is not a modern one but it has been existing from time immemorial. However, time to time, the concept and nature of crimes have changed. In addition, the definition of crimes has been changed accordingly. In the era of 20th century and with the advent of computer, the criminals have changed the mode of committing the crimes from conventional methods to computer based methods. The first recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. Indian legal system is now in a developed stage. Indian Legal system is enacting the law along with the changing situation. The definition of cyber is not possible because there are different forms of misuse of information technology. The ways of misusing information technology if finalize, then new ways can be drawn by the expert. Therefore, the particular definition of cyber crime can affect the interest of the large society. Therefore, it is not possible to define the term cyber crime. The conventional definition and types of crime covers almost all cyber crimes. Because the basic thing in the crime is same and one. However, the changes and development in society has hampered to enact the new laws as like Information Technology Act 2000.

Cybercrime has been defined as the act of creating, distributing, altering, stealing, misusing and destroying information through the computer manipulation of cyberspace; without the use of physical force and against the will or the interest of the victim. As a concept, information can be anything from electronic money, to government secrets, and the victim can be an individual, a corporate person, or as criminal law is defined: the state

and society as whole. However, the term cybercrime is also used to denote all those objectionable activities misuse or abuse that are either conducted in the cyber world, or through or against a computer, it is an umbrella term and may have different meanings in different situations. Again it is clarified that the word crime used in this term does not have the traditional meaning attached to it. Even objectionable activities that are civil rather than criminal, in the real world sense, are included in its purview. Warren Buffet describes Cybercrime as the "number one problem with mankind" and "poses real risks to humanity." A report (sponsored by MacAfee) published in 2014 estimated that the annual damage to the global economy was $445 billion. A 2016 report by Cybersecurity ventures predicted that global damages incurred as a result of cybercrime would cost up to $6 trillion annually by 2021 and $10.5 trillion annually by 2025.

Cybercrime are the crime unknown to the legal world prior to the birth of the Internet and include not only acts which are employed to commit traditional crimes using the Net but also those crimes which are committed thoroughly and exclusively using the Internet. It is however interesting to note that even Information Technology Act, 2000 too omits to define cybercrime or computer crime. Even the major cyber laws of the U.S. and the U.K. do not contain a definition of cybercrime. However the, the taxonomy of these elusive crimes would give a circumventing and exhausting comprehension of cybercrimes. In India, the recent amendment in the IT Act 2008 has used the term 'computer related offences' whereby a good number of cybercrimes have been added to the list of crimes already existing. Cyber Crime can be classified as follows:

A. Cyber Crime against Persons

There are certain offences which affects the personality of individuals and which are as follows:

(i) **Harassment via-E-Mails:** It is very common type of harassment through sending letters attachment of files and folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.

(ii) **Cyber Stalking:** It means expressed or implied physical threat that creates fear through the use to computer technology such as Internet, e-mail, phones; text messages, webcam, websites or videos.

(iii) **Dissemination of Obscene Material:** It includes indecent exposure. Pornography (basically child pornography) hosting of website containing these prohibited materials. There obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

(iv) **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

(v) **Hacking:** It means unauthorized control/access over computer systems and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network. Hacking is done by hackers who are basically regarded as learners and explorers who want to help rather than cause damage and who often have very high standards.

(vi) **Cracking:** It is amongst the gravest cyber crimes known till date. It is dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

(vii) E-mail Spoofing: A spoofed e-mail may be said to be one which misrepresents its origin. It shows its origin to be different from which actually it originates.

(viii) Carding: It means false ATM cards i.e. Debit and Credit Cards used by criminals for their monetary benefits through withdrawing money from the victims bank account malafidely. There is always unauthorized use of ATM cards in this type of cyber crimes.

(ix) Cheating and Fraud: It means the person who is doing the act of cybercrimes i.e. stealing password and data storage has done it with having guilty mind which lead to fraud and cheating.

(x) Child Pornography: It involves the use of computers networks to create, distribute or access materials that sexually exploit underage children.

(xi) Assault by Threat: It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. e-mail, videos or phones.

B. Cyber Crime Against Property

As there is rapid growth in the international trade where business and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affect property which are as follows:

(i) Intellectual Property Crime: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of Intellectual property right violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code etc. It is the most controversial and contentious area related to the Net. It is the most widely breached and the least fully understood by anybody but the intellectual property lawyers.

(ii) Cyber Squatting: It means where two person claim for the same Domain Name either by claiming that they had registered the name first by right of using it before the other or using something similar to that previously.

(iii) Cyber Vandalism: Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.

(iv) Hacking Computer System: It generally attacks the famous people using twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer.

(v) Transmitting Virus: Viruses are program that attack themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer either by altering or deleting it. Worm attacks plays a major role in affecting the computerize system of the individuals.

(vi) Cyber Trespass: It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse or damage data or system by using wireless internet connection.

(vii) Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person of the Internet hours paid for by another person.

C. Cyber Crime Against Government

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

(i) Cyber Terrorism: Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorists' attacks on the Internet is disturbed by denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc.

(ii) Cyber Warfare: It refers to politically inactivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as an analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

(iii) Distribution of Pirated Software: It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.

(iv) Possession of Unauthorized Information: It is very easy to access any information by the terrorist with the aid of Internet and to possess that Information for political, religious, social, ideological objectives.

D. Cyber Crimes Against Society

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

(i) Child Pornography: It involves the use of computer networks to create distribute or access materials that sexually exploit underage children.

(ii) Cyber Trafficking: It may be trafficking in drugs, human beings, arm, weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a grave crime.

(iii) On-line Gambling: Online fraud and cheating is one of the most lucrative businesses that are growing today is the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs etc.

(iv) Financial Crimes: This type of offence is common as there is a rapid growth in the users of networking sites and phone networking where culprits will try to attack by sending bogus mails or ménages through internet.

(v) Forgery: It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need in today's lifestyle.

E. Cyber Crimes Against Women

Amongst the various cyber-crimes committed against individuals and society at large, crimes that are specifically targeting women are as follows;

1. Cyber-stalking.
2. Harassment via e-mails.
3. Cyber Bullying
4. Morphing.
5. Email spoofing.
6. Cyber Defamation.

Cyber Laws in India prevent any crime done using technology, where a computer is a tool for cybercrime. The laws for cybercrime protect citizens from dispensing sensitive information to a stranger online. Ever since the introduction to cyber laws in India happened, IT Act, 2000 was enacted and amended in 2008 covering different types of crimes under cyber law in India. The Act explains the types of cybercrime and punishment. The realm of cyberspace which is largely dependent upon the internet and use of technology, incidents of cyber crimes are reported to have increased. To protect one from cybercrime, there was a need for cyber laws and so the implementation of cyber laws in India began in the year 2000, with the IT Act as an introduction to Indian cyber

law. The Indian parliament considered it necessary to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information Technology Act, 2000 was passed and enforced on 17th May 2000. The preamble of this Act states its objective to legalise e-commerce and further amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891and the Reserve Bank of India Act, 1934. The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000. So that, they may regulate and control the affairs of the cyber world in an effective manner. The Information Technology Act deals with the various cyber crimes in chapters IX & XI. The important sections are Ss. 43,65,66,67. Section 43 in particular deals with the unauthorized access, unauthorized downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. This section provide for a fine up to Rs. 1 Crore by way of remedy. Section 65 deals with 'tampering with computer source documents' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Further section 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs.

Information technology continues to have an ever-growing impact upon society and the way that society conducts its affairs. Information and communications technologies have spread out in almost in every professional, commercial and industrial activity and most organizations would find it difficult, if not impossible, to function without relying heavily on these technologies. On the other hand, information and communications technologies have posed and continue to create novel and complex social and legal problems. Frequently, the law has been found wanting when dealing with the issues raised by these constantly evolving technologies, and legislators and the courts have often struggled to come to terms with the challenges raised by them. Now a days, cyber crime is going to be a great challenges in the society. Due to the cyber crime, people of the society are suffering from so many problems. Cyber communication is society's newest way to intract. Online social networking websites, text massages and emails provide users with an effective, quick way to communicate with people all over the world. Teen in particular spend hours online every day, on computers or personal electronic device. Excess use of these devices are very dangerous for youths. Now a days youths are playing online games and some games are dangerous for their life because some youths are loss their life during online games so it's a dangers things for the society. The Information Technology (Amendment) Act, 2008 has made it a base for committing various cybercrimes openly. Therefore the cyber laws in India are not effective instead it is counter-productive. India is the only country in the world that has the provision of bail in cybercrime cases. It means even if a person commits cybercrime like posing, hacking or any similar cybercrime or contravention and is somehow caught by the police force, he would be released on bail as a matter of right .The provision of cybercrime has made India a safe place for cyber criminals. It is admitted that capacity of human mind being unfathomable.

CONCLUSION: It is not possible to eliminate crimes from cyberspace but it is certainly possible to prevent them by generating information awareness among the people related to government and non-government agencies of the nations about the tools, techniques and modes which the cybercriminals invariably use to commit cybercrimes so that they may be countered by using protective and preventive devices. The menace of cybercrime is not the sole responsibility of the state and the instrumentalities .Citizens as well as netizens is equally under a solemn obligation to fight against the cybercrimes.

REFERENCES:

1.S.V. Joga Rao, Law of Cyber Crime and Information Technology, Wadhwa and Co., Nagpur, p. 6.

2.Sieber Ulrich, The International Emergence of Criminal Information Law, Information Technology Crime, Kolu, 1992.
3.Sterling Bruce, The Hacker Crackdown: Law and disorder on the electronic frontier, London: Penguin Books, 1994.
4.Encyclopedia of Information Technology Law, Sweet and Maxwell, 2001. Available at www.webopedia.com,
5.Dan L Burk, "Jurisprudence in a World Without Borders", I Va. J.L. and Tech 3 (Spring 1997).
6.Talat Fatima, Cyber Crimes, Eastern Book Company, Lucknow (2011), p. 70.
7.Donn B. Parker, Crime by Computer, Charle's Scribner's Sons, New York, 1976.
8.Richard C. Hollinger, "Computer Crime" in Clifton D. Bryant (Ed.).
9.Warren Buffett: Cyber poses real risks to humanity, finance yahoo com ,retrieved 17 may 2021
10.Singh Anand K. "Cyber Crime, Law and Social Challenges", in Neeraj K.Rai (Ed.) Social Media: Issues and Challenges, Avon Publishing House,Delhi,2020