

Cyber crime in India with special focus on cyber fraud : A critical analysis

Rakhi Tiwari

Student, Law college dehradun , Uttarakhand university ,Uttarakhand (India)

ARTICLE DETAILS

Article History

Published Online: 13 March 2019

Keywords

Ubiquitous , information technology , kali linux , Namp , Nessus , john the ripper , pOf , winzapper , mSpy , ikeymonitor.

ABSTRACT

Since from the beginning of the civilization, man is always been motivated by progress and technology . The nature of man always have been curious and eager to learn things which are helpful in making his life easier. The field of technology have always been fascinating towards making human life's easier. The field of technology is growing rapidly with new inventions ,which is contributing towards technological advancements. However, the technological advancements along with growth also raising several issues and challenges . Several issues have been raising from technological advancements among which cyber crime , which are committed through computer network , becoming a major threat in the world of technology crimes.

Basically, those crimes which are committed through computer network and in which computer is used as a tool for committing crime comes within the category of cyber crime . At present cyber crime is not defined in Information Technology act 2000 nor in the IT amendment Act 2008 and in any legislation of India but it is categorized in Information technology Act . Thus all computer related crimes are covered under cyber crime .Although India is developing country but still it has its separate law which only deals with cyber crimes. It shows that at present , countries either developed or developing are facing issues related to cyber crime. Countries throughout the world are evolving different approaches and methods to prevent and regulate cyber crimes .

In this article we will discuss Cyber crime in India with the help of leading books , leading case laws , leading statutory provisions .

1. Introduction

Now a days cyber crime becomes an industry itself which is known as cyber crime industry . Under this industry a huge world of cyber criminals is growing day by day where they don't need any arm force or equipments, weapons etc .. for committing crime. They earn money by trading information to the people who hired them and they have a supply chain through which they trade information . According to Wikipedia , *now ubiquitous* , in current usage the cyber space becomes an independent information technology infrastructure and telecommunication system by which online communication takes place .¹When internet was developed , its founders don't had any idea that in future it will be used for committing offences ,and will be misuse and will required legislation for its regulation . Today cyber world is governed and regulated by law which is known as cyber law . The country like India has it's own law viz. Information technology Act , 2000. This law has detailed provisions related to cyber space . Although India is developing country but still there are so many people who are being affected by cyber crime .

A large number of books and articles have been written on cyber law . The scope of the subject is changing rapidly itself with the evolution of *information technology* .Number of works have been done on this topic .²At present era cyber law become very hot topic among whole world , developed countries like Uk and USA have their own law related to cyber

space . These countries have their separate agencies which deals with cyber crimes .

Cybercrime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offence . Cyber crime includes phishing , hacking , spamming , child pornography , forgery , identity theft , extortion etc..Cyber criminals use hacking tools (for example *kali linux , Namp , Nessus , john the ripper , pOf , winzapper , mSpy , ikeymonitor*) to access in personal information , business secrets , and also use internet for malicious and fraudulent purpose .³Cyber crime is very wide term it includes all kinds of crimes whichever is committed through online process or internet or in which computer is required for committing offence .

2. Cyber Crime In India : Law Perspective

The Parliament of India enacted the Information Technology Act ,2000 in the fifty-first year of the Republic of India .This Act is based on the resolution A/ RES/51/162 adopted by the General Assembly of the United Nations on 30th January , 1997 regarding the Model Law on Electronic Commerce earlier adopted by the United Nations Commission on International Trade law (UNITRAL)in its twenty – ninth session .⁴ This resolution Recommends *that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law*

¹ <http://www.thefreedictionary.com>

² Anirudh Rastogi , *Law of Information Technology and Internet* ,Lexis Nexis

³ Wikipedia .

⁴ Vakul Sharma & Seema Sharma , *Information technology law and practice* , Universal law publication Co. Pvt. Ltd. Pg. no. 1 .

applicable to alternatives to paper-based methods of communication and storage of information.⁵

The Act deals with statutory provisions related to Information technology, hence it is known as Information technology Act. There are some noteworthy provisions which deal with classification of cyber crimes, these are as follows;

Section 43 penalty for damages to computer and its system – according to this section if any person commits any offence and found guilty of any offence mentioned under sub section (a) – (h) of section 43 is liable to pay damages by way of compensation not exceeding one crore to the person suffered.

Section 66 – hacking for computer system, alteration any data and information – when any person with the purpose of causing loss and damages to the public and person destroy, deletes or alter any data or information staying in computer and reduce its worth and usefulness through committing hacking.

Punishment - If any person found guilty of this shall be imprisonment upto 3 years and fine upto two lakh rupees, or both.

Broadly cyber crimes are categorized in 3 category viz.

- (1) Cyber crime against individual,
- (2) Cyber crime against organization,
- (3) Cyber crime against society.

Cyber crime against individual : These are those crimes which are made against person and his properties, for example – cyber - stalking, E-mail harassment, making fake facebook accounts, without permission enter in the computer and spreading obscene material, child pornography, cyber Fraud, cheating etc..

Cyber crime against organization : There are some examples of crimes against organization – cyber terrorism against a government organization, possessing unauthorized information, spam, phishing etc..

Cyber crime against society : There are some examples of crimes against society – trafficking, financial crimes, forgery, online gambling, distributing illegal articles, polluting youth by spreading obscene articles and matters.

In Indian history the Information technology Act, 2000 is the first act which stated provisions related to cyber crime.

3. Cyber Fraud (Computer Fraud)

Computer Fraud is broad locution and it includes data theft, forgery, virus or bot attacks, hacking, service attack which causes the failure of system, phishing etc.. In Computer fraud the act of using a computer to change electronic data, or to gain unauthorized use of a computer. Types of computer fraud includes:

- Sharing spam emails
- Entering in computer system without permission
- Engaging in data analysis through computer software

- Unauthorized entrance in personal information, such as credit cards or social security numbers
- Transmitting computer viruses or worms with the purpose of destroying or crashing another persons computer system.

4. Issues And Problems

There are so many issues and challenges in front of us in fighting against cyber crimes. Some of the challenges are as follows:

- Lack of awareness and the culture of cyber security
- Lack of knowledge regarding cyber crimes.
- Less effectiveness of Information Technology Act.
- Lack of trained and qualified persons who are capable of countering and executing measures.
- No email account policy especially for defense forces, police and the security against personal.

These are some of cyber crime challenges we are facing now a days.

5. Conclusion

Cyber crime is the only crime which can be done without physical presence. Cyber crime is a broad term it includes criminal activities committed on computer or on internet. Traditional crimes are being committed through modern medium for example theft, cheating, fraud, misrepresentation etc.. At present era to combat cyber crime becomes very difficult task for all of us. It has become a threat to mankind. To provide protection against cyber crime become vital part social, cultural and security aspect of a country. The government of India has enacted the Act of Information technology for prevention and regulation of cyber crimes. This Act further added the provisions from Indian penal code 1860, The Indian Evidence Act 1872, The Banker's Book's evidence Act 1891 and The Reserve Bank of India Act 1934.

The main purpose of writing this paper is to aware people regarding cyber crime. This is a very brief study of cyber crime with special focus on cyber fraud. People should aware themselves from cyber crime and also took actions against criminals. If anyone get attacked by criminals they should report it in nearest police station. If people avoid it because of lack knowledge then they are promoting these criminals who to commit cyber crime and they will never stop.

⁵Available at, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/763/57/PDF/N9776357.pdf?OpenElement>