3. Cyber Crimes and Law in India

Prof. Anarase Lalasaheb P.
Dada Patil Mahavidyalaya, Karjat, Dist Ahmednagar.

Abstract

The social, political and economic aspect of this new cyber technology is a little known and properly understood phenomenon1. In the cyber space there is a net of web sites and they are busy day and night in disseminating useful information but it has generated some problems also. A number of frauds are committed at web site. People are cheated by the misuse of information technology and the security of electronic record is also at stake.

The problems of developed countries are more acute than the problems of developing countries, because more the advancement, more are the use of the web and more are the chances of its misuse. Law violators always like to go one step ahead from law makers. Indeed the cyber criminals have put a challenge to all scientists and law makers for the control of cyber crimes rampant all over the globe.

Cyber Crimes : Definition

Cyber crimes are crimes committed on the electronics mediums where means is not a requirement. The 'Cambridge Dictionary' defines 'Cyber crimes' as crimes committed with the use of computers or related to computers especially through the internet.

Classification of Cyber Crimes

Cyber crimes can be classified on the basis of nature and purpose of the offence committed. It can be broadly grouped in three categories based on the target of the crimes. It may be against person, property or

Government, David L. Carter classifies computer related crimes into three categories.

a. Where computer is the target of crime.
b. Where computer facilitate commission of crime.
c. Where computer is incidental to the crime.

a. Computer as a Target Crime

This aims at damaging computer system or stealing valuable information stored on the system which includes.

i. Sabotage of Computer

ii. Theft of Data

iii. Unlawful access to Govt. Records.

b. Computer as an instrument of Crimes

These are crimes committed using computer as a medium and includes –

1. Fraudulent use of ATM cards and accounts.
2. Credit Card frauds
3. Frauds involving electronic fund transfers.

c. Computer as incidental

This may be classified in the two categories.

a. Internet Crime

b. Web based Crime.

1. Cyber Crime against Individuals

This variety of crimes includes transmission of child pornography, harassment of any one with the use of a computer such as e-mail and cyber stalking. The trafficking distribution, posting and dissemination of obscene material, pornography, indecent exposure and child pornography constitute various important cyber crimes known today. The potential harm of such crimes to humanity can hardly be overstated.

B. E-Mail Spoofing

A spoffed e-mails is one that appears to originate from one source but actually has been sent from another source e.g. Pooja has an e-mail address Pooja@Asianlaw.org. Her enemy, Sameer sports her e-mail and send obscene message to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends could feel offended and relationship could be spoiled for life. E-mail spoofing can also cause monetary damage.

C. Cyber Stalking

The Oxford dictionary defines stalking as " pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posing messages on the bulletin boards constantly bombarding the victims emails etc.

2. Cyber Crime against Property

The second category of cyber crime is that of cyber crimes against all forms of property. These crimes include unauthorized computer trespassing through cyberspace. Computer

vandalism, transmission of harmful programs and unauthorized possession of computerized information comes under it. Hacking and cracking are amongst the gravest cyber crimes known till date.

Software piracy is also another distinct kind of cyber crime which is perpetuated by many people online who distribute illegal and unauthorized pirated copies of software.

A. Financial Crimes

This would include credit card trends, money laundering etc. To cite a recent case, a website offered to sell alphorns mangoes at a throwaway price. Disbelieving such a transaction, very few people responded to and supplied to the website their credit card numbers. Though small in number, these people were sent the alphorns mangoes to create belief. The fame of this website now spread like wildlife.

B. Hacking

Audit Commission Reports defined hacking as "Deliberately gaining unauthorized access to an information system". A variety of motives lie behind hacking attacks and not all hackers and virus writers pose the same threat. The vast majority of incident is nuisance attacks, rather than serious, malicious assaults. Though victims of the former may still suffer financially, perpetrators can be from the traditional criminal world exploiting the power of the new tool which disgruntled employees are using with their inside knowledge.

C. E-Mail Bombing

E-mail bombing refers to sending large number of e-mails to the victim resulting in blocking the victim's email account or blocking the mail servers. In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates.

D. Denial of Service Attackers

This involves flooding a computer resource with more requests that it can handle. This causes the resources to crash merely by denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a 'Distributed Denial of Service' (DDOS) attack wherein the perpetrators are many and are geographically wide spread. It is very difficult to control such attacks.

3. Cyber Crime against Government

Cyber Terrorism is a distinct kind of crime in this category. The growth of the Internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the International government as also to terrorise the citizen of any country.

Salient Features of the Information Technology Act, 2000

India has enacted the Information Technology Act in the year, 2000 based on the modern law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. The preamble of the Act gives a very clear picture about the aims, objectives and salient features of the Act. The salient features of the

Information Technology Act, 2000 are ;

1. The Act provides for authentication of electronic records and also it legally recognize electronic records and digital signatures.
2. The Act provides for regulation of Certifying Authorities. The Central Govt. may appoint controller or the other officers for the purpose of issuing license for digital signature certificates and also for granting and the renewal of licenses. The Act also empowers the Certifying Authority to issue Digital Signature Certificate.
3. The Act provides for penalties for damage to computer, computer system and also penalty for failure to furnish information.
4. The Act provides for establishment of cyber Appellate Tribunal.
5. The Act completely bars the jurisdiction of Civil Court.

This Act consists of 94 Sections with 4 Schedules. There are 13 chapters that deal with preliminary aspects, digital signature, electronic governance, security of electronic records, regulation of certifying authorities, digital signature certificate, penalties, adjudication, offences etc.Four schedules are appended to make some amendments in the Indian Penal Code, Indian Evidence Act, Banker Books Evidence Act. And Reserve Bank of India Act. Cyber Crimes punishable under Indian Penal Code.4

Relevant provisions of the Indian Penal Code have been amended in accordance with the schedule appended with IT Act and following activities have been made punishable.

1. Fabricating false evidence by making fictitious entry in electronic book or record is made punishable.

2. Destruction of electronic record to prevent its production as evidence in court is punishable.
3. Forgery by making false electronic record is also an offence.
4. Counterfeiting electronic record is made punishable.
5. Judges and police officers and lawyers must be given appropriate training about cyber laws and its enforcement.
6. A subject on Cyber Law should be introduced in both school and college.
7. Both the Central and State Govt. should allocate more funds for conducting researchers on cyber law.
8. Cyber crimes must be declared as a crime against the entire humanity,.

The law Commission of India has stressed the need for enactment of more cyber laws and for establishment of electronic courts to deal with cyber crimes. It is suggested that the scope of existing law may be extended to cover variety of cyber activities but enforcement aspect should not be ignored. Crime conception ought to be in consonance with the prevailing social mores and value system of the contemporary society as well as the sacrosanct limits imposed by the Constitutional tenets.

References

Books & Journals

1. Farooq Ahmed - Cyber Law in India (Law on Internal) Carter David - Computer Crime Categories – How Techno – Criminals Operate, F BI Law enforcement, Bulletin,July, 1995
2. Joseph Polony -Computer Trends – Law Enforcement Response – CBI Bulletin Vol. VI No. 5 May, 1998.

Websites

- http /cyber laws.net / cyber.india / why cyber law.htm.
- http./cyber crime / Planet India Why Cyber net / intro.htm.
- http/www.legal service India.com / articles.