Study about Cyber Law of India

Somia Malik, Research Scholar
BPS University, Knanpur Kalan, Sonipat

ISSN 2454-308X
9 770024 543081

Introduction: In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

Key Words: Cyber law, unlawful, fraud, penal code

We can categorize Cyber crimes in two ways

- The Computer as a Target :-using a computer to attack other computers.
  e.g. Hacking, Virus/Worm attacks, DOS attack etc.
- The computer as a weapon :-using a computer to commit real world crimes.
  e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Technical Aspects

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as

a. Unauthorized access & Hacking:-

Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. By hacking web server taking control on another person`s website called as web hijacking.

b. Trojan Attack:-

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. The most popular name is Trojan Horse. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan.

c. Virus and Worm attack:-

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.

Programs that multiply like viruses but spread from computer to computer are called as worms.

d. E-mail & IRC related crimes:-

- Email spoofing.
- Email Spamming
- Sending malicious codes through email
- Email bombing
- Defamatory emails

- Email frauds
- IRC related

Distributed DOS

A distributed denial of service (DoS) attack is accomplished by using the Internet to break into computers and using them to attack a network. Hundreds or thousands of computer systems across the Internet can be turned into "zombies" and used to attack another system or website.

Types of DOS

There are three basic types of attack:

a. Consumption of scarce, limited, or non-renewable resources like NW bandwith, RAM, CPU time. Even power, cool air, or water can affect.
b. Destruction or Alteration of Configuration Information.
c. Physical Destruction or Alteration of Network Components.

e**. Pornography:-**

The literal mining of the term 'Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc." Adult entertainment is largest industry on internet. There are more than 420 million individual pornographic web pages today. Research shows that 50% of the web-sites containing potentially illegal contents relating to child abuse were 'Pay-Per-View'. This indicates that abusive images of children over Internet have been highly commercialized.

Effects of Pornography

Research has shown that pornography and its messages are involved in shaping attitudes and encouraging behavior that can harm individual users and their families. Pornography is often viewed in secret, which creates deception within marriages that can lead to divorce in some cases.

Marriage and children are obstacles to sexual fulfillment.

Everyone is involved in promiscuous sexual activity, infidelity and premarital sex.

g. Forgery:-

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Also impersonate another person is considered forgery.

h. IPR Violations:-

These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations. etc.

Cyber Squatting- Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws.

i. Cyber Terrorism:-

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical and fire etc.

Cyber terrorism is an attractive option for modern terrorists for several reasons.

1. It is cheaper than traditional terrorist methods.
2. Cyber terrorism is more anonymous than traditional terrorist methods.
3. The variety and number of targets are enormous.
4. Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
5. Cyber terrorism has the potential to affect directly a larger number of people.

j. Banking/Credit card Related crimes:-

In the corporate world, Internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information. Use of stolen card information or fake credit/debit cards are common. Bank employee can grab money using programs to deduce small amount of money from all customer accounts and adding it to own account also called as salami.

k. E-commerce/ Investment Frauds:-

Sales and Investment frauds, An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

l. Sale of illegal articles:-

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. Research shows that number of people employed in this criminal area. Daily peoples receiving so many emails with offer of banned or illegal products for sale.

m. Online gambling:-

There are millions of websites hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

n. Defamation: -

Defamation can be understood as the intentional infringement of another person's right to his good name.

Cyber Defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. Information posted to a bulletin board can be accessed by anyone. This means that anyone can place Cyber defamation is also called as Cyber smearing.

Cyber Stacking:-

Cyber stalking involves following a persons movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. In general, the harasser intends to cause emotional distress and has no legitimate purpose to his communications.

p. Pedophiles:-

Also there are persons who intentionally prey upon children. Specially with a teen they will let the teen know that fully understand the feelings towards adult and in particular teen parents. They earns teens trust and gradually seduce them into sexual or indecent acts. Pedophiles lure the children by distributing pornographic material, then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions.

q. Identity Theft :-

Identity theft is the fastest growing crime in countries like America. Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud.

r. Data diddling:-

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also include automatic changing the financial information for some time before processing and then restoring original information.

s. Theft of Internet Hours:-

By gaining access to an organisation's telephone switchboard (PBX) individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties. Additional forms of service theft include capturing 'calling card' details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards.

t. Theft of computer system (Hardware):-

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

u. Physically damaging a computer system:-

Physically damaging a computer or its peripherals either by shock, fire or excess electric supply etc.

v. Breach of Privacy and Confidentiality

Privacy refers to the right of any individual to determine when, how and to what extent his or her personal data will be shared with others.

Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.

w. Confidentiality

It means non disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected. Generally for protecting secrecy of such information, parties while sharing information forms an agreement about the procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties. Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality.

References:

1. http://www.cyberlawsindia.net/index1.html
2. http://www.infosecawareness.in/cyber-laws-india
3. https://www.hg.org/information-technology-law.html
4. https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm