CYBER CRIMES

INTRODUCTION

- Activity in which computers or networks are a tool, target, or a place of criminal activity.
- cyber crime is a subset of computer crime. In a cyber crime, the computer network can be;

- The tool of a crime
- The target of a crime
- Used for purpose incidental to a crime

DEFINITIONS

- Offences that are committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such a s internet.
- Cyber crime is a term for any illegal activity that uses a computer as its primary means of communication. The U.S. department of Justice expands the definition of cyber crime and includes any illegal activity that uses a computer for the storage of evidence.
- Cyber crime also stated as any use of a computer as an instrument of further illegal ends, such as;

- Committing fraud
- Stealing identities
- Violating privacy

HISTORY

- The first recorded cyber crime took place in the year 1820, when , Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom.
- The firm spam e-mail took place in 1978 when it was sent out over the Arpanet.
- The first Virus was installedon an Apple computer in1982.
- A Sixteen years old student nicknamed “Data Stream”, arrested by UK police (1994).

- Denial of Service (DoS) attacks by ‘Mafia Boy’ on eBay, Yahoo! And other popular sites (2000).
- FBI’s e-mail system was hacked (Feb, 2005).
- Travelling documents of NATO forces were hacked in Afghanistan.

TARGETS OF CYBER CRIMES

- **Against individual property**
- Transmitting virus
- Un-authorized control/access over computer
- Intellectual property crimes
- Internet time thefts
- **Against Organization**
- Possession of un-authorized information
- Cyber terrorism against the government organization
- Distribution of pirated software,etc

❑Against Social at Large

- Pornography (basically child pornography)
- Trafficking
- Financial crimes
- Online gambling
- Forgery
- Sale of illegal articles

SOME COMMON CYBER CRIMES

- **Computer Virus**: A computer virus is a computer program or attaches itself to application programs or other executable system software causing damage to the files.
- **Phishing**: Phishing occurs when the perpetrator sends fictitious e-mails to individuals with links to fraudulent websites that appear official and thereby cause the victim to release personal information to the perpetrator.

- **Hacking**: The act of penetrating or gaining unauthorized access to or use of data unavailable in a computer system or a computer network for the purpose of gaining knowledge, stealing or making unauthorized use of the data.
- **Spoofing :** Spoofing is the creation of TCP/IP packets using somebody else's IP address.
- **Netsplonage:** Netsplonage occurs when perpetrators back into online systems or individual PCs to obtain confidential information for the purpose of selling it to other parties.

- **Cyber stalking:** Cyber stalking refers to the use of the internet, email or other electronic communications device to stalk another person. It is an electronic harassment that involves harassing or threatening over a period of time.
- **Cyber Terrorism:** Cyber terrorism occurs when terrorists cause virtual destruction in online computer system.

MOTIVES OF CYBER CRIMINALS

- Desire for entertainment
- Profit
- Infuriation or revenge
- Political agenda
- Sexual motivations
- Psychiatric illness

CYBER LAWS

- Cyber law is a term used to describe the legal issues related to use of communication technology, particularly cyber space, i.e. internet.
- Cyber law is an attempt to apply laws designed for the physical world to human activities on internet.

Cyber laws in the world

- Electronic Commerce Act (Ireland)
- Electronic Transactions Act (UK, USA, Australia, New Zealand, Singapore)
- Electronic Transactions Ordinance (Hong Kong)
- Information Technology Act (India)
- Information communication Technology Act (Bangladesh)

Cyber laws in India

- India has enacted the first I.T. Act, 2000 based on the UNCIRAL model recommended by the general assembly of the United Nations.
- Offences under IT acts are:

- Tampering with computer source document
- Hacking with computer systems, data alterations
- Publishing obscene information
- Un-authorized access to protected systems
- Breach of confidentiality and privacy
- Publishing false digital signature certificates.

ROLE OF PAKISTAN IN CYBER WORLD

It is no surprise that Pakistan is not free from the cyber space dilemma. The availability of computers and Internet connections provides unprecedented opportunities to communicate and learn in Pakistan. However, certain individuals do exploit the power of the Internet for criminal purposes as well.

Domestic cyber laws in Pakistan

Pakistan has a legal framework in place to address cyber crimes.

- Prevention of Electronic Crimes Ordinance, 2007
- Electronic Transactions Ordinance, 2002
- Pakistan Telecommunication (Re-organization) Act, 1996
- Wireless Telegraphy Act, 1933
- Telegraph Act, 1885
- Federal Investigation Agency Act, 1974
- Payments & Electronic Fund Transfers Act, 2007

Electronic transaction ordinance, 2002

Important sections are:

36 .Violation of privacy information.

37. Damage to information system, etc

Electronic/ cyber crime bill, 2007

- It deals with the electronic crimes included:
  - Cyber terrorism
  - Data damage
  - Electronic fraud
  - Electronic forgery
  - Cyber stalking
  - Cyber spaming
  - Un-authorizes access to code

PREVENTION

- Use hard to guess passwords
- Use anti-virus software and firewalls-keep them up to date
- Don’t open email or attachments from unknown sources
- Back up your computer on disk or CD often

RECOMMENDATIONS

- **Fostering Linkages:**
  - Creation liaison with international community will create sharing of experiences and good practices.
  - The value of fostering co-operation internationally with other countries/regions and parties needs to be enhanced.
  - Co-operation between governments and the private sector in combating cyber crime.

- **Building National level Partnerships and Creating Awareness:**
  - Create specialized forums for exchange of experiences and information which would entail initiating and promoting literary, technical and scientific activity.
  - Setting up a cyber crime cell consisting of experts to deal with cyber-crime will encourage reporting and evolve into a process online with the legislature.

❑Training and Awareness Raising :

- ❖It is essential to educate and empower youth to safely and responsibly take control of their Internet experience.
- ❖Disseminate general awareness of cyber crimes and user laws/rights by arranging symposia, seminars, lectures, classes, demonstrations, and presentations, briefings, to educate the society and gain their comfort level.
- ❖People need to be aware of the appropriate law enforcement investigative authorities at the local, state, federal, or international levels.

CONCLUSION

It is not possible to eliminate cyber crime from the cyber space in its entirety. However, it is quite possible to check it. Any legislation in its entirety might be less successful in totally eliminating crime from the globe. The primary step is to make people aware of their rights and duties and further making the application of the laws more stringent to check crime.

However, in any draft legislation it is important that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive.

THANK YOU