UNIT- I: Introduction to Cybercrime

Introduction, Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes

1. Introduction

"Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber attacks".

- **"Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.**

Cybercrime: Definition and Origins of the Word

Cybercrime : "A crime conducted in which a computer was directly andsignificantly instrumental."

Alternative definitions of Cybercrime are as follows:

1. **Any illegal act where a special knowledge of computer technology is essential for its perpetration (*to commit a crime*), investigation or prosecution**.

2. **Any traditional crime that has acquired a new dimension or order of magnitude *through the aid of a computer*, and abuses that have come into being because of computers.**

3. **Any financial dishonesty that takes place in a computer environment.**

4. **Any threats to the computer itself, such as theft of hardware or software, damage anddemands for money.**

Other Synonym terms of cybercrime are

- **Computer-related crime**
- **Computer crime**
- **Internet crime**
- **E-crime**
- **High-tech crime**, etc.

The legal systems around the world introduce laws to combat cybercriminals attacks. Two types of attack are as follows.

1. Techno-crime: An act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system.

2. Techno-vandalism: These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. "Tight internal security" and "strong technical safeguards" should prevent the vast majority of such incidents.

Cybercrimes differ from mostcrimes in four ways:

(a) how to commit them is easier to learn,
(b) they require few resources relative to the potential damage caused,
(c) they can be committed in a jurisdiction without being physically present in it
(d) they are often not clearly illegal.

Important Definitions related to Cyber Security

a. Cyberterrorism

Cyberterrorism is defined as "*any person, group or organization who, with **terrorist intent**, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism*."

b. Cyberspace

- "cyberspace" is where users mentally travel through matrices of data. Conceptually, "cyberspace" is the "nebulous place" where humans interact over computer networks.
- The term "cyberspace" is now used to describe the Internet and other computer networks.
- In terms of computer science, "cyberspace" is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data.
- Cyberspace is most definitely a place where you chat, explore, research and play.

c. Cybersquatting

- The term is derived from "squatting" which is the act of **occupying an abandoned space**/ building that the user does not own, rent or otherwise have permission to use.
- Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process.
- Cybersquatters usually ask for prices far greater than those at which they purchased it. Some cybersquatters put up derogatory or defamatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them.
- Cybersquatting is the practice of buying "domain names" that have existing businesses names.

d. Cyberwarfare

- *Cyberwarfare* means information **attacks against an unsuspecting opponent's computer networks, destroying and paralyzing nations**.
- This perception seems to be correct as the terms cyberwarfare and cyberterrorism have got historical connection in the context of attacks against infrastructure.
- The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population.
- These type of Cyberattacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare.

3. Cybercrime and Information Security

These are closely related concepts that deal with the protection of computer systems, networks, and data from unauthorized access, misuse, or damage. Here's an overview of each:

Cybercrime:

Cybercrime refers to criminal activities conducted through or targeting computer systems or networks. It encompasses a wide range of illegal activities, including:

1. **Hacking:** Unauthorized access to computer systems or networks to gain sensitive information or disrupt operations.
2. **Malware:** Creation and distribution of malicious software (e.g., viruses, worms, ransomware) to exploit vulnerabilities and compromise systems

   .**Phishing:** Attempting to deceive individuals into revealing sensitive information, such as passwords or financial details, through fraudulent emails or websites.
3. **Identity theft:** Stealing personal information to impersonate someone else for fraudulent activities or financial gain.
4. **Cyber fraud:** Online scams, financial fraud, or theft conducted through the internet or digital platforms.
5. **Cyberstalking and harassment:** Persistent online harassment, threats, or stalking behaviors.
6. **Distributed Denial of Service (DDoS) attacks:** Overloading a system or network with a flood of traffic to make it inaccessible to legitimate users.
7. **Data breaches:** Unauthorized access or disclosure of sensitive information, often resulting in the exposure of personal data.

Information Security:

Information security focuses on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing measures to ensure the **confidentiality, integrity,** and **availability** of information. Key components of information security include:

1. **Risk assessment and management**: Identifying potential threats, vulnerabilities, and risks to information systems and implementing appropriate safeguards.
2. **Access controls**: Restricting access to information and systems based on user roles, authentication, and authorization mechanisms.
3. **Encryption:** Using encryption techniques to secure data in transit and at rest, preventing unauthorized access or interception.
4. **Network security**: Implementing firewalls, intrusion detection systems, and other technologies to protect networks from unauthorized access and attacks.
5. **Incident response and management**: Establishing procedures to detect, respond to, and recover from security incidents or breaches promptly.
6. **Security awareness and training**: Educating users about security best practices, policies, and procedures to minimize human-related security risks.
7. **Regular updates and patches:** Keeping software, operating systems, and security tools up to date to address known vulnerabilities.
8. **Physical security:** Protecting physical assets, such as servers, data centers, and storage devices, from unauthorized access or theft.

Effective information security practices are crucial in mitigating the risks posed by cybercrime and protecting sensitive data, intellectual property, and critical systems. Organizations and individuals need to stay vigilant, implement security measures, and stay informed about emerging threats to maintain a secure computing environment.

4. **Who are Cybercriminals?**

- Types of Cybercriminals
    1. **Type I: Cybercriminals – hungry for recognition**
        - Hobby hackers;
        - IT professionals (social engineering is one of the biggest threat);
        - Politically motivated hackers;
        - Terrorist organizations.
    2. **Type II: Cybercriminals – not interested in recognition**
        - Psychological perverts;
        - financially motivated hackers (corporate espionage);
    3. **Type III: Cybercriminals – the insiders**
        - Disgruntled or former employees seeking revenge;
        - Competing companies using employees to gain economic advantage through damage and/or theft.

The term "cybercriminals" can include:

1. **Hackers:(I)** Skilled individuals who gain unauthorized access to computer systems or networks to steal sensitive information, disrupt operations, or cause damage. They may have different motivations, such as financial gain, political activism, ideological reasons or personal gratification.
2. **Malware Developers: (II)** Individuals or groups who create and distribute malicious software, such as viruses, worms, trojans, or ransomware. Their aim is often to compromise systems, steal data, or extort money from victims.
3. **Phishers(III):** Cybercriminals who use deceptive techniques, such as fraudulent emails or websites, to trick individuals into revealing sensitive information like passwords, credit card details, or personal data.
4. **Identity Thieves(III):** Individuals who steal personal information, such as social security numbers, bank account details, or login credentials, with the intent of assuming someone else's identity for financial gain or fraudulent purposes.
5. **Scammers:(II)** Cybercriminals who engage in various online scams, such as advance-fee fraud, lottery scams, romance scams, or business email compromise. They deceive victims to extract money, sensitive information, or valuable assets.
6. **Cyber Extortionists(II):** Criminals who employ tactics like ransomware attacks or distributed denial of service (DDoS) threats to extort money from individuals, businesses, or organizations.
7. **State-Sponsored Hackers(II):** Cybercriminals who operate on behalf of or with the support of nation-states. They conduct espionage, sabotage, or disruptive activities targeting other nations, organizations, or individuals.
8. **Cyber Espionage Agents(II):** Individuals or groups involved in gathering sensitive information for political, economic, or military purposes. They may target governments, organizations, or individuals to obtain classified or proprietary data.

It is important to note that cybercriminals can range from individual hackers acting alone to organized criminal syndicates or even state-sponsored groups. Their motivations can vary, including financial gain, political objectives, personal vendettas, or ideological reasons. The evolving nature of technology and the internet presents ongoing challenges in combating cybercriminals and protecting individuals, organizations, and critical infrastructure from their activities.

5. Classifications of Cybercrimes

*"**Crime** is defined as "an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the off ender liable to punishment by that law"*

Cybercrimes are classified as follows:

Cybercrime against individual

a. Electronic mail (E-Mail) Spoofing and other online frauds:

- A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source.

b. Online Frauds

- Online Scams. There are a few major types of crimes under the category of hacking:
- **Spoofing website and E-Mail security alerts**, false mails about virus threats, lottery frauds and Spoofing.
- In Spoofing websites and E-Mail security threats, fraudsters create authentic looking websites that are actually nothing but a spoof.

c. Phishing, Spear Phishing and its various other forms such as Vishing and Smishing

- **"Phishing"** refers to an attack using mail programs to deceive or coax (lure) Internet users into disclosing confidential information that can be then exploited for illegal purposes.
- **"Spear Phishing"** is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. Here
- **"Vishing"** is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward.
- **"Smishing"** is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from "SMS PhISHING." SMS – Short Message Service – is the text messages communication component dominantly used into mobile phones.

d. Spamming:

- People who create electronic Spam are called *spammers*.
- Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages indiscriminately.
- Although the most widely recognized form of Spam is E-Mail Spam, the term is applied to similar abuses in other media:
    - instant messaging Spam,
    - web search engine Spam,
    - wiki Spam,
    - online classified ads Spam,
    - junk fax transmissions,
    - social networking Spam,
    - file sharing network Spam,
    - video sharing sites, etc.
- Spamming is difficult to control because it has economic viability – advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings.

e. Cyber defamation:

"Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person."

- Cyberdefamation happens when the above takes place in an electronic form.
- In other words, "cyberdefamation" occurs when defamation takes place with the help of computers and/or the Internet,

f.* Cyberstalking and harassment*:

- Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.

g. Computer sabotage:

- The use of the Internet to stop the normal functioning of a computer system through the introduction of worms, viruses or logic bombs, is referred to as computer sabotage.
- It can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists or to steal data or programs for extortion purposes.
- Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs.
- Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date

h. Pornographic offenses:

- As the broad-band connections get into the reach of more and more homes, larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of pedophiles.
- "Pedophiles" a person who is sexually attracted to children.
  Here is how pedophiles operate:
- **Step 1:** Pedophiles use a false identity to trap the children/teenagers (using "false identity" which in itself is another crime called "identity theft").
- **Step 2:** They seek children/teens in the kids' areas on the services, such as the Games BB or chat areas where the children gather.
- **Step 3:** They befriend children/teens.
- **Step 4:** They extract personal information from the child/teen by winning his/her confidence.
- **Step 5:** Pedophiles get E-Mail address of the child/teen and start making contacts on the victim's E-Mail address as well. Sometimes, these E-Mails contain sexually explicit language.
- **Step 6:** They start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
- **Step 7:** At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.

- This is the "digital world"; in physical world, parents know the face of dangers and they know how to avoid and face the problems by following simple rules and accordingly they advice their children to keep away from dangerous things and ways.
- However, it is possible, even in the modern times most parents may not know the basics of the Internet and the associated (hidden) dangers from the services offered over the Internet. Hence most children may remain unprotected in the cyberworld.
- Pedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is right/wrong for them while browsing the Internet.
- Legal remedies exist only to some extent; for example, **Children's Online Privacy Protection Act** or **COPPA** is a way of preventing online pornography.

i. Password sniffing:

This also belongs to the category of cybercrimes against organization because the use of password could be by an individual for his/her personal work or the work he/she is doing using a computer that belongs to an organization.

Cybercrime against property

a. Credit card frauds:

- Information security requirements for anyone handling credit cards have been increased dramatically recently.
- Millions of dollars may be lost annually by consumers who have credit card and calling card numbers stolen from online databases.
- Security measures are improving, and traditional methods of law enforcement seem to be sufficient for prosecuting the thieves of such information. Bulletin boards and other online services are frequent targets for hackers who want to access large databases of credit card information.
- Such attacks usually result in the implementation of stronger security systems.
- Security of cardholder data has become one of the biggest issues facing the payment card industry.

b. Intellectual property (IP) crimes:

Basically, IP crimes include

- software piracy,
- copyright infringement,
- trademarks violations,
- theft of computer source code, etc.

c. Internet time theft:

- Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person.
- Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.
- However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent.
- The issue of Internet time theft is related to the crimes conducted through "identity theft."

Cybercrime against organization

a. Unauthorized accessing of computer:

Hacking is one method of doing this and hacking is a punishable offense

b. **Password sniffing:**

- Password Sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site.
- Whoever installs the Sniffer can then impersonate an authorized user and login to access restricted documents.
- Laws are not yet set up to adequately prosecute a person for impersonating another person online.
- Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs.

c. Denial-of-service attacks (known as DoS attacks):

- The goal of DoS is not to gain unauthorized access to systems or data, but **to prevent intended users** (i.e., legitimate users) **of a service from using it**. A DoS attack may do the following:
  1. Flood a network with traffic, thereby preventing legitimate network traffic.
  2. Disrupt connections between two systems, thereby preventing access to a service.
  3. Prevent a particular individual from accessing a service.

d. Virus attacks:

- Virus attacks can be used to damage the system to make the system unavailable
- Computer virus is a program that can "infect" legitimate (valid) programs by modifying them to include a possibly "evolved" copy of itself.
- Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.

e. E-Mail bombing/mail bombs:

- E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim's E-Mail account (in the case of an individual) or to make victim's mail servers crash (in the case of a company or an E-Mail service provider).

f. Salami attack/Salami technique:

- These attacks are used for committing financial crimes.
- The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed;
- for example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say ` 2/- or a few cents in a month) from the account of every customer.
- No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.

g. Logic bomb:

- Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs.
- Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date

h. Trojan Horse:

- Trojan Horses: A **Trojan Horse**, Trojan for short, **is a** term used to describe **malware** that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system

i. Data diddling:

- A data diddling (data cheating) attack involves **altering raw data just before it is processed by a computer** and then changing it back after the processing is completed.

- Electricity Boards in India have been victims to data diddling programs inserted when private parties computerize their systems.

j. Industrial spying/industrial espionage:

- Spying is not limited to governments. Corporations, like governments, often spy on the enemy.The Internet and privately networked systems provide new and better opportunities forespionage.
- "Spies" can get information about product finances, research and development and marketing strategies, an activity known as "industrial spying."
- However, cyberspies rarely leave behind a trail.

k. Computer network intrusions:

- "Crackers" who are often misnamed "Hackers can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses or change user names and passwords.

l. Software piracy :

- Cybercrime investigation cell of India defines "software piracy" as *theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.*
- There are many examples of software piracy:
    - *end-user copying* – friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses;
    - *hard disk loading with illicit means* – hard disk vendors load pirated software;
    - *counterfeiting* – large-scale duplication and distribution of illegally copied software;
    - *illegal downloads from the Internet* – by intrusion, by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose:

Cybercrime against Society

a. Forgery

- Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners.
- Outside many colleges there are miscreants soliciting the sale of fake mark-sheets or even degree certificates.
- These are made using computers and high quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

b. Cyberterrorism:

Cyberterrorism is defined as "*any person, group or organization who, with* ***terrorist intent****, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism*."

c. Web jacking:

- Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it).
- Thus, the first stage of this crime involves "password sniffing."
- The actual owner of the website does not have any more control over what appears on that website.

6. Cybercrime: The Legal Perspectives

- Cybercrime poses a biggest challenge.
- *Computer Crime: As per "Criminal Justice Resource Manual* (1979)", computer-related crime was defined in the broader meaning as:"*any illegal act for which knowledge of computer technology is essential for a successfulprosecution".*
- International legal aspects of computer crimes were studied in 1983.In that study, computer crime was consequently defined as:"*encompasses any illegal act for which knowledge of computer technology is essentialfor its commit*".
- Cybercrime, in a way, is the outcome of "globalization." However, globalization does not mean globalized welfare at all. Globalized information systems accommodate an increasing number of transnationaloffenses.

Some key aspects of cyber security from a legal perspective:

1. **Data Protection and Privacy Laws**: Many countries have enacted data protection and privacy laws that regulate the collection, storage, processing, and transfer of personal data. These laws typically require organizations to implement security measures to safeguard personal information and provide individuals with certain rights regarding their data.
2. **Cybersecurity Regulations and Standards:** Governments may establish cybersecurity regulations and standards to protect critical infrastructure, sensitive information, and public systems. These regulations may require organizations to implement specific security controls, conduct risk assessments, or report data breaches.
3. **Intellectual Property Protection:** Intellectual property laws protect copyrights, patents, trademarks, and trade secrets. In the context of cybersecurity, these laws can be relevant in cases involving the theft, misuse, or unauthorized disclosure of proprietary information or software.
4. **Cybercrime Laws:** Governments enact laws to address cybercrimes and provide legal frameworks for prosecuting offenders. These laws may cover offenses such as hacking, identity theft, fraud, unauthorized access, and distribution of malware. They also establish penalties for cybercriminal activities.
5. **Incident Response and Breach Notification:** Some jurisdictions have laws that require organizations to have incident response plans in place to effectively respond to cybersecurity incidents. They may also mandate the notification of affected individuals, regulators, or authorities in the event of a data breach.
6. **International Cooperation and Treaties:** Cybersecurity often involves cross-border issues, and international cooperation is crucial. Countries may enter into bilateral or multilateral agreements, treaties, or conventions to enhance collaboration in combating cyber threats, sharing information, and extraditing cybercriminals.
7. **Law Enforcement and Investigation:** Cybersecurity laws empower law enforcement agencies to investigate and prosecute cybercrimes. These agencies may engage in activities such as digital forensics, monitoring online activities, and coordinating international efforts to combat cyber threats.

7. Cybercrimes: An Indian Perspective

- India has the fourth highest number of Internet users in the world. The population of educated youth is high in India. A point to note is that the majority of off enders were under 30 years.
- The maximum cybercrime cases, about 46%, were related to incidents of cyberpornography, followed by hacking. In over 60% of these cases, offenders were between 18 and 30 years.
- The Indian Government is doing its best to control cybercrimes.

Some key aspects of cybercrime in the Indian legal perspective:

1 **Information Technology Act, 2000:** The Information Technology Act (IT Act) is the primary legislation governing cybercrime in India. It provides legal recognition for electronic transactions, digital signatures, and data protection. The IT Act was amended in 2008 to incorporate provisions related to cybercrime offenses and their penalties.

2 **Cybercrime Offenses:** The IT Act defines several cybercrime offenses which include unauthorized access and hacking, data theft and misuse, identity theft and impersonation, cyberstalking and harassment, online fraud and forgery etc.

3 **Data Protection and Privacy:** India has recently enacted the Personal Data Protection Bill, 2019 (yet to become law as of my knowledge cutoff in September 2021), which aims to establish a comprehensive framework for protecting personal data. The bill outlines principles for data processing, consent requirements, and the establishment of a Data Protection Authority.

4 **Aadhaar Act:** The Aadhaar Act, 2016 governs the unique identification system in India, known as Aadhaar. It addresses privacy concerns related to the collection, storage, and use of Aadhaar data and imposes penalties for unauthorized access or misuse of Aadhaar information.

5 **Cyber Reporting and Investigation:** The IT Act mandates the reporting of cyber incidents to the Indian Computer Emergency Response Team (CERT-In) or the appropriate authorities.

6 **Cyber Appellate Tribunal:** The Cyber Appellate Tribunal (CAT) was established under the IT Act to hear appeals against adjudicating officers' decisions and provide a forum for resolving disputes related to cybercrime offenses.

7 **International Cooperation:** India participates in international efforts to combat cybercrime and cooperates with other countries through mutual legal assistance treaties (MLATs) and other mechanisms. It collaborates with international organizations such as Interpol and conducts joint operations to address transnational cyber threats.

8 Cybercrime and the Indian ITA 2000

- In India, the ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 in January 30, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.

8.1 Hacking and the Indian Law(s)

- Cybercrimes are punishable under two categories: the ITA 2000 and the IPC.
- The number of Offenses to be monitored has increased. Cases of Spam, hacking, cyberstalking and E-Mail fraud are rampant and, although cybercrimes cells have been set up in major cities, the problem is that most cases remain unreported due to a lack of awareness.
- In an environment like this, there are a number of questions in the minds of a commoner:
    - When can consumers approach a cybercrime cell?
    - What should the victims do?

- How does one maintain security online?
- Any and every incident of cybercrime involving a computer or electronic network can be reported to a police station, irrespective of whether it maintains a separate cell or not.

 CHAPTER XI of the original ITA 2000 lists a number of activities that may be taken to constitute cybercrimes which includes tampering with computer source code, hacking, publishing or transmitting any information in electronic form

- In the amendment to the IT Act 2000, now known as the ITA 2008, several offenses have been added to the Act. Existing Sections 66 and 67 (in the original ITA 2000) on hacking and obscene material have been updated by dividing them into more crime-specific subsections, thereby making cybercrimes punishable.
- In Section 66, hacking as a term has been removed. This section has now been expanded to include Sections
  - 66A (offensive messages),
  - 66B (receiving stolen computer),
  - 66C (identity theft),
  - 66D (impersonation),
  - 66E (voyeurism) and
  - 66F (cyberterrorism).,

Some key aspects of the ITA 2000 in relation to cybercrime:

1. **Cybercrime Offenses:** The ITA 2000 defines various offenses related to cybercrime and establishes penalties for committing them. Some notable offenses under the Act include:
   - **Unauthorized Access and Hacking**: The Act prohibits unauthorized access to computer systems, computer networks, or computer resources. It also criminalizes hacking activities, including introducing viruses, malware, or other malicious code into computer systems.
   - **Data Theft and Misuse:** The Act addresses the theft, destruction, alteration, or unauthorized copying of electronic information. It penalizes the unauthorized use, disclosure, or misuse of sensitive personal data or information.
   - **Identity Theft and Impersonation:** The Act makes it an offense to impersonate another person or entity online, including creating fake profiles or using others' personal information without consent.
   - **Cyberstalking and Harassment:** The Act criminalizes cyberstalking, cyberbullying, and online harassment, including sending threatening or offensive messages through electronic communication channels.
   - **Online Fraud and Forgery:** The Act addresses various forms of online fraud, such as phishing, credit card fraud, financial scams, and forgery of electronic records or digital signatures.
2. **Legal Recognition of Digital Signatures:** The ITA 2000 provides legal recognition for digital signatures, ensuring their validity and enforceability in electronic transactions. It establishes the Controller of Certifying Authorities (CCA) to regulate digital signatures and certification authorities in India.
3. **Cyber Offense Investigation and Prosecution:** The Act empowers law enforcement agencies, such as the police, to investigate and prosecute cybercrime offenses. It provides procedures for search and seizure of electronic evidence, preservation of digital records, and the admissibility of electronic evidence in court.

4. **Cyber Appellate Tribunal:** The ITA 2000 established the Cyber Appellate Tribunal (CAT) as an appellate body to hear appeals against orders passed by adjudicating officers under the Act.

Intermediary Liability Protection: The ITA 2000 includes provisions related to the liability of intermediaries, such as internet service providers (ISPs) and social media platforms. These provisions offer limited liability protection to intermediaries for third-party content hosted or transmitted through their platforms, subject to certain conditions

8. A Global Perspective on Cybercrimes

Cyber crime is a critical concern on a global scale as the world becomes increasingly interconnected. Some key aspects of cybersecurity from a global perspective:

1. **International Cooperation:** Recognizing the transnational nature of cyber threats, countries and international organizations collaborate to address cybersecurity challenges. Cooperation includes information sharing, joint investigations, capacity building, and the development of common cybersecurity frameworks and standards.
2. **International Cybersecurity Organizations:** Several international organizations play key roles in promoting global cybersecurity cooperation and coordination, such as:
   - **United Nations:** The UN promotes international norms and regulations for responsible state behavior in cyberspace.
   - **International Telecommunication Union (ITU)**: The ITU works on developing international cybersecurity standards and guidelines.
   - **Interpol:** Interpol facilitates cooperation among law enforcement agencies worldwide to combat cybercrime.
   - **Global Forum on Cyber Expertise (GFCE):** The GFCE fosters international collaboration and capacity building in cybersecurity.
3. **Cybersecurity Regulations and Legislation:** Governments around the world are enacting cybersecurity regulations and legislation to protect critical infrastructure, personal data, and digital services.
4. **Public-Private Partnerships:** Collaboration between governments, private sector organizations, and civil society is essential for effective cybersecurity. Public-private partnerships promote information sharing, joint initiatives, and the development of best practices to enhance cybersecurity resilience.
5. **Cybersecurity Skill Shortage:** The demand for skilled cybersecurity professionals exceeds the available talent globally. Bridging the skill gap requires concerted efforts in education, training, and workforce development to build a robust cybersecurity workforce.
6. **Emerging Technologies and Challenges:** Advancements in emerging technologies like artificial intelligence, Internet of Things (IoT), cloud computing, and 5G pose new cybersecurity challenges. Securing these technologies requires proactive measures, industry collaboration, and continuous innovation in cybersecurity solutions.
7. **Cyber-security Awareness and Education:** Raising public awareness about cyber-security risks and best practices is crucial. Efforts to educate individuals, businesses, and organizations about cyber threats, safe online practices, and the importance of strong cyber-security measures contribute to a more secure digital environment.

- The wide definition of cybercrime overlaps in part with general offense categories that need not be Information & Communication Technology (ICT)-dependent, such as white-collar crime and economic crime. Thus, one can see that there is a lot to do toward building

confidence and security in the use of ICTs and moving toward international cooperation agenda. This is because in the 21st century, there is a growing dependency on ICTs that span the globe.

- Some agencies have been advocating for the need to address protection of the Rights of Netizens.
- There are agencies that are trying to provide guidance to innocent victims of cybercrimes. However, these NGO like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police.
- There are also a few incidents where Police have pursued false cases on innocent IT professionals.
- The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time.