Unit – 2

Cyber–crime and Cyber law

Cyber Crime

Cyber crime is related to the criminal activities that are carried out over the internet or through computer networks. This can include hacking, online fraud, identity theft, spreading malware, cyberbullying, and various other forms of criminal behaviour committed through digital means.

Cyber Law

Cyber law, also known as internet law or digital law, signifies the legal regulations and frameworks governing digital activities. It covers a large range of issues, including online communication, e-commerce, digital privacy, and the prevention and prosecution of cybercrimes.

Classification of Cyber Crimes

Cybercrimes can be classified into various categories based on the nature of the offense. Here are some common classifications:

1) **Financial Fraud:**
   - Scams like fake emails or websites to steal money or sensitive information.
   - Unauthorized transactions or hacking into bank accounts.
2) **Online Harassment and Bullying:**
   - Sending mean messages, threats, or spreading rumors online.
   - Persistently following or monitoring someone online without their consent.
3) **Cyber Surveillance:**
   - Stealing secrets, intellectual property, or sensitive information for spying or competitive advantage.
   - Hacking into government or corporate networks for classified data.
4) **Cyber Terrorism:**
   - Using computers to create fear or chaos by disrupting critical systems..
   - Sharing scary ideas or planning bad things using the internet to scare people.

5) **Ransomware Attacks:**
    - Malicious software encrypts data and demands payment for decryption.
    - Holding data or systems hostage until a ransom is paid.
6) **Intellectual Property Theft:**
    - Illegally sharing or distributing copyrighted material like movies or software.
    - Using trademarks or brand names without permission for profit.
7) **Cyber Vandalism:**
    - Breaking or messing up websites, emails, or computer systems on purpose.
    - Creating trouble or spreading viruses online just to cause problems or annoy people.
8) **Identity Theft:**
    - Phishing emails or fake websites tricking people into revealing personal information.
    - Creating fake identities or accounts using stolen information for fraudulent activities.

Common Cyber Crimes

1) **Phishing:** Deceiving people into sharing personal information via fake emails or websites.
2) **Malware Attacks:** Harmful software infecting computers to steal data or damage systems.
3) **Identity Theft:** Stealing personal information to impersonate someone for financial gain.
4) **Online Fraud:** Tricking individuals into giving money or sensitive information through fake websites or ads.
5) **Cyberbullying:** Harassing or threatening others online through messages or social media.
6) **Data Breaches:** Unauthorized access to sensitive information stored in databases.
7) **Ransomware:** Holding data or systems hostage until a ransom is paid to unlock them.

Cyber Crime Targeting Computers and Mobiles

Cybercrime targeting computers and mobile devices involves illegal activities done using technology like computers, smartphones, and the internet.

1) **Malware Attacks:** Harmful software sneaks into computers and mobiles to steal data or cause damage. It can come from suspicious downloads, emails, or websites.
2) **Phishing:** Tricky emails or messages pretend to be from trustworthy sources to trick users into revealing personal information like passwords or credit card numbers.
3) **Identity Theft:** Personal information is stolen to pretend to be someone else and commit fraud or other crimes. This can lead to financial loss and damage to reputation.

4) **Online Fraud:** Deceptive tactics are used to trick people into giving away money or sensitive information, often through fake websites, ads, or online marketplaces.
5) **Cyberbullying:** Harassment or threats are sent to others online, causing emotional distress or harm. It can happen through social media, messaging apps, or online forums.
6) **Data Breaches:** Hackers gain unauthorized access to databases, stealing personal information like usernames, passwords, or credit card details. This information can be sold on the dark web or used for identity theft.
7) **Ransomware:** Malicious software locks up devices or files until a ransom is paid. It can encrypt data or make devices unusable, causing disruption and financial loss.
8) **Social Engineering:** Tricking people into revealing sensitive information or performing actions that compromise security. This can happen through manipulation, persuasion, or impersonation.
9) **Mobile App Fraud:** Fraudulent apps on mobile devices deceive users into downloading them, stealing personal information, or displaying ads without permission.
10) **Unauthorized Access:** Intruders gain entry to computers or mobile devices without permission, accessing sensitive data or using the device for malicious activities such as spying or spreading malware.

Cyber Crime Against Women and Children

Cybercrime against women and children, often referred to as **"online gender-based violence"** or **"cyber harassment"**, is a serious and concerning issue. These crimes can encompass various forms of online harassment, exploitation, and abuse that target women and children.

1) **Online Harassment:** Women and children face bullying, threats, or stalking online, causing emotional distress and sometimes leading to offline harm.
2) **Cyberstalking:** Persistent monitoring or tracking of women and children's online activities, often leading to fear for safety and invasion of privacy.
3) **Revenge Porn:** Intimate images or videos are shared without consent, causing humiliation, harassment, and potential harm to reputation.
4) **Online Grooming:** Predators befriend children online to manipulate, exploit, or sexually abuse them, often by gaining their trust and gradually escalating contact.

5) **Sextortion:** Threats or blackmail are used to force women and children into providing sexual images or engaging in sexual acts online.
6) **Cyberbullying:** Children are subjected to bullying, harassment, or exclusion online, leading to low self-esteem, depression, and social isolation.
7) **Child Exploitation:** Children are trafficked, sexually abused, or exploited through online platforms, often disguised as modeling opportunities or relationships.
8) **Identity Theft:** Personal information of women and children is stolen and misused for fraudulent activities, leading to financial loss and reputational damage.
9) **Unauthorized Sharing of Personal Information:** Private details of women and children are shared without consent, leading to risks of stalking, harassment, or identity theft.
10) **False Representation:** Fake profiles or personas are created to deceive women and children online, leading to trust violations and potential exploitation or fraud.

Financial Frauds

1) **Phishing**: Phishing attacks often involve creating fake links that appear to be from a legitimate organization.[40] These links may use misspelled URLs or subdomains to deceive the user.
2) **Identity theft**: Identity theft is the crime of using the personal or financial information of another person to commit fraud, such as making unauthorized transactions or purchases.
3) **Ransomware**: Malicious software encrypts a victim's files, and the attacker demands payment (usually in cryptocurrency) for the decryption key.
4) **Credit Card Fraud**: Unauthorized use of credit card information, either through physical theft or online hacking, for making purchases or withdrawals.
5) **Investment Scams**: Cybercriminals may create fake investment opportunities, promising high returns to lure victims into investing money, which is then stolen.
6) **Online Banking Fraud**: Criminals use various methods like keyloggers or phishing to gain access to online banking credentials and conduct unauthorized transactions.
7) **Cryptocurrency Scams**: Fraudulent schemes related to cryptocurrencies, including fake initial coin offerings (ICOs), Ponzi schemes, or fake exchanges
8) **Business email compromise (BEC)** is a type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential company info. The culprit poses

as a trusted figure, then asks for a fake bill to be paid or for sensitive data they can use in another scam.

9) **ATM Skimming**: Criminals install devices on ATMs to capture card information, enabling them to create counterfeit cards or make unauthorized transactions.

Social Engineering attacks

Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information

- It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Types of social engineering attacks

1) Phishing

Phishing scams are the most common type of social engineering attack. They typically take the form of an email that looks as if it is from a legitimate source.

2) Watering hole attacks

An attacker will set a trap by compromising a website that is likely to be visited by a particular group of people, rather than targeting that group directly. An example is industry websites that are frequently visited by employees of a certain sector, such as energy or a public service.

3) Business email compromise attacks

Business email compromise (BEC) attacks are a form of email fraud where the attacker masquerades as a C-level executive and attempts to trick the recipient into performing their business function, for an illegitimate purpose, such as wiring them money.

4) USB baiting

USB baiting sounds a bit unrealistic, but it happens more often than you might think. Essentially what happens is that cybercriminals install malware onto USB sticks and leave them in strategic places, hoping that someone will pick the USB up and plug it into a corporate environment, thereby unwittingly unleashing malicious code into their organization.

5) Physical social engineering

Certain people in your organization--such as help desk staff, receptionists, and frequent travelers--are more at risk from physical social engineering attacks, which happen in person.

Malware and Ransomware attacks

Ransomware is a specific type of malware that encrypts a user's files or locks them out of their system, rendering the data inaccessible.

1) **Evolution and Sophistication**: Ransomware and malware attacks continually evolve, with cybercriminals developing more sophisticated techniques and methods to bypass security measures.
2) **Ransomware-as-a-Service (RaaS)**: Criminals often utilize RaaS platforms, enabling even non-technical individuals to launch ransomware attacks. This commodification increases the prevalence of such attacks.
3) **Double Extortion:** In addition to encrypting files, modern ransomware often involves double extortion, where attackers threaten to leak sensitive data unless a ransom is paid. This adds a layer of complexity and urgency for victims.
4) **Targeted Attacks:** Some ransomware attacks are highly targeted, focusing on specific organizations or industries. Cybercriminals may conduct extensive reconnaissance to maximize the impact of their attacks
5) **Supply Chain** Attacks: Ransomware and malware can infiltrate organizations through supply chain weaknesses. This includes compromising software vendors, third-party services, or even trusted partners in the supply chain.

Malware

Malware is a broader term encompassing various types of malicious software. This includes viruses, worms, trojans, spyware, and other harmful programs.

Objectives: Malware can have different objectives, such as stealing sensitive information, disrupting system operations, or providing unauthorized access to a computer system.

Types of Malware attacks:

1) **Viruses**: Malicious software that attaches itself to legitimate programs and spreads when the infected program is executed
2) **Worms**: Self-replicating malware that spreads across networks without human intervention.
3) **Trojans**: Disguised as legitimate software, trojans trick users into installing them, often leading to unauthorized access or data theft.
4) **Spyware**: Secretly monitors user activity, capturing sensitive information without the user's knowledge.

5) **Rootkits**: Conceals the existence of malicious software, often granting unauthorized access.
6) **Botnets**: Networks of compromised computers controlled by a central server.
7) **Keyloggers**: Records keystrokes to capture sensitive information like passwords.

Zero Day and Zero Click attacks

Zero-day attacks target vulnerabilities in software or hardware that are unknown to the vendor or the public.

1) **Exploitation Period**: Attackers exploit these vulnerabilities before the software vendor releases a patch or fix, leaving no time for defenders to prepare.
2) **Stealthy Nature**: Zero-day attacks are often stealthy and can go undetected for extended periods, making them particularly dangerous.
3) **Targeted Exploitation**: Zero-day vulnerabilities are frequently used in targeted attacks against specific individuals, organizations, or even nations.
4) **High Market Value**: Information about zero-day vulnerabilities and their associated exploits can have a high value on the black market, motivating attackers to discover and use them.
5) **Challenges in Detection**: Traditional security measures may not detect zero-day attacks since there are no known signatures or patterns to identify these exploits.

Zero-click attack

A zero-click attack is a type of cyber attack that requires no user interaction to exploit a vulnerability in a device or application. In other words, the attacker can gain access to a device or network without the user clicking on a link or downloading a file.

1) **No User Interaction**: Zero-click attacks do not rely on user actions such as clicking on links or opening attachments. The exploitation occurs automatically without any explicit involvement from the user.
2) **Advanced Persistence**: Zero-click attacks often involve advanced and persistent threats that can remain undetected for extended periods, increasing the potential damage.
3) **Malware Delivery**: Zero-click attacks may deliver malware silently, allowing it to operate in the background without the user's knowledge, leading to data theft, surveillance, or other malicious activities.

4) **Supply Chain Exploitation**: Zero-click attacks can exploit weaknesses in the software supply chain, compromising software before it even reaches the end user. This highlights the importance of secure development practices and supply chain integrity.
5) **Cyber Espionage**: Zero-click attacks are frequently associated with cyber espionage activities, allowing attackers to gain persistent access to sensitive information without raising suspicion.

Cybercriminals modus - operandi

Modus operandi is the principle that a criminal is likely to use the same technique repeatedly, and analysis or record of that technique used in every serious crime will provide a means of identification in a particular crime."

Certainly, here's a more detailed breakdown of cybercriminal modus operandi in points:

1) **Phishing**: Creation of deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as usernames and passwords.
2) **Malware Attacks**: Deployment of malicious software, including viruses, trojans, and ransomware, to compromise systems, steal data, or disrupt operations.
3) **Social Engineering**: Manipulation of human psychology to deceive individuals or employees into disclosing confidential information or performing actions beneficial to the attacker.
4) **Ransomware Attacks**: Encryption of files or systems with a demand for payment in exchange for restoring access.
5) **Credential Stuffing**: Use of stolen login credentials from one service to gain unauthorized access to other accounts where users reuse passwords.
6) **Supply Chain Attacks:** Exploitation of vulnerabilities in third-party suppliers, software, or services to compromise the security of the target organization.
7) **Zero-Day Exploits**: Utilization of unknown vulnerabilities in software or hardware before vendors release patches.
8) **Distributed Denial of Service (DDoS)**: Overloading a target's network or website with traffic to disrupt normal operations and cause service outages.
9) **Crypto jacking**: Covert use of a victim's computing resources for cryptocurrency mining without their knowledge or consent.

10) **Man-in-the-Middle (MitM) Attacks:** Intercepting and potentially altering communication between two parties to eavesdrop or manipulate information.

Reporting of Cyber Crime

Reporting cybercrimes is essential to combat and prevent online criminal activities. Reporting these incidents can help law enforcement agencies and cybersecurity experts investigate and take action against cybercriminals.

Here are the steps you should take to report cybercrimes:

1)Contact Local Law Enforcement

If you are a victim of a cybercrime, such ae hacking, online harassment, identity theft, or fraud, you should contact your local police department or law enforcement agency. They can guide you on how to proceed and they may open an investigation if necessary ·

2)Contact National Authorities

In many countries there are national agencies or specialized cybercrime units responsible for investigating and handling cybercrimes. In the United States, for example, you can report cybercrimes to the Federal Bureau of Investigation (FBI) through its Inte et Crime Complaint Center (IC3).

3)Use Online Reporting Portals

Many countries have online reporting portals or websites where you can report cybercrimes. Check your local government websites for cybercrime reporting options. In the U.S., the IC3 website is a common platform for reporting various types of cybercrimes.

4)Contact Your Internet Service provider (ISP)

If you suspect that you are a victim of cyberattacks or online harassment, your ISP may be able to assist or guide you in reporting the issue.

5)Report to Financial Institutions

If you experience financial cybercrimes, such as credit card fraud or unauthorized bank transactions, contact your bank or credit card company immediately. They can help investigate and resolve these issues.

6)Cybersecurity Organizations

You can also report cybercrimes to cybersecurity organizations or Computer Emergency Response Teams (CERTs) in your country. These organizations are equipped to handle and investigate cyber incidents.

7)Online Platforms

If you encounter Cyberbullying, harassment, or other malicious activity on social media platforms or websites, report the incidents to those platforms. They often have mechanism in place for reporting abusive behavior.

Remedial and Mitigation Measures

Remedial and mitigation measures are essential steps to address and minimize the impact of cyber incidents and vulnerabilities. These actions aim to remediate the damage caused by a cyber incident and reduce the risk of future incidents. Here are some key remedial and mitigation measures:

Remedial Measures

1) **Containment**: Isolate affected systems or networks to prevent the spread of the incident. This may involve disconnecting compromised devices from the network.
2) **Data Recovery**: Restore lost or encrypted data from backups. Ensure that backups are secure and regularly tested for reliability.
3) **Malware Removal**: Use antivirus and anti-malware tools to detect and remove malicious software from infected systems.
4) **Patch and Update**: Apply patches and updates to affected software, systems, and devices to close vulnerabilities that were exploited in the incident.
5) **Password Reset**: Change passwords for compromised accounts or systems to prevent unauthorized access.
6) **Incident Documentation**: Thoroughly document the incident, including the timeline, actions taken, and evidence collected. This documentation is valuable for investigations and post-incident analysis
7) **Incident Documentation**: Thoroughly document the incident, including the timeline, actions taken, and evidence collected. This documentation is valuable for investigations and post-incident analysis.
8) **Communication**: Notify affected parties, including customers, partners, and • employees, about the incident and steps taken to remediate it. Transparent and timely communication is essential for maintaining trust.

9) **Legal and Compliance Obligations**: Comply with legal requirements regarding data breach notifications, which may vary by jurisdiction
10) **Forensic Analysis**: Conduct a forensic analysis to understand the scopes and cause of the incident, which can help prevent future occurrence.

Mitigation Measures

1) **Risk Assessment**: Regularly assess and prioritize cyber risks to identify vulnerabilities and potential threats.
2) **Network Segmentation**: Isolate critical systems from less secure ones to limit the spread of an attack.
3) **Access Control**: Implement the principle or least privilege (PoLP) to restrict user and system access to only what is necessary.
4) **Data Encryption**: Encrypt sensitive data at rest and in transit to protect it from unauthorized access.
5) **Cybersecurity Training**: Educate employees and users on security best practices, including how to recognize phishing attempts and other threats.
6) **Intrusion Detection and Prevention**: Use intrusion detection and prevention systems (IDS/IPS) to identify and block suspicious network activity.
7) **Security Patch Management**: Establish a patch management process to keep software and systems up-to-date with the latest security updates.
8) **Incident Response Plan**: Develop and maintain an incident response plan to ensure a swift and organized response to future incidents.
9) **Backup and Recovery Strategy**: Regularly back up critical data and maintain an effective disaster recovery plan to minimize downtime in the event of an incident.

Legal Perspective of Cybercrimes

In India, cybercrimes have become a significant concern as the country continues to embrace digital technologies and the internet. The Information Technology Act, 2000 (amended in 2008) is the primary legislation governing cybercrimes in India. Here's an overview of cybercrimes from an Indian perspective:

1) **Legal Framework**: The Information Technology Act,2000 (IT Act) was enacted to address various cyber-related offenses and provide a legal framework to deal with cybercrimes. The

IT Act was subsequently amended in 2008 to expand its scope and strengthen provisions related to cybercrime.

2) **Punishments and Penalties**: The IT Act prescribes various penalties and imprisonment terms based on the severity of the cybercrime committed. The penalties • can range from fines t. imprisonment up to life, depending on the nature of e offense.
3) **Cyber Cell and Law Enforcement**: Many states in India have established specialized cyber cells or cybercrime units to investigate and tackle cybercrimes effectively. These units work closely with the Indian Computer Emergency Response Team (CERT-In) and other law enforcement agencies to address cyber threats.
4) **Cyber Appellate Tribunal**: The IT Act established the Cyber Appellate Tribunal to hear appeals against orders issued by the Controller of Certifying Authorities and adjudicate on certain cyber-related matters.
5) **Data Protection and Privacy**: India has been working on enacting comprehensive data protection legislation to protect individuals privacy and personal data. The Personal Data Protection Bill, 2019, aims to regulate the collection, storage, processing, and transfer of personal data and ensure data protection.
6) **Cyber Security Initiatives**: The Indian government has initiated several cybersecurity measures to enhance the country's resilience against cyber threats. Initiatives like Digital India and cyber Swachh Kendra (Botnet Cleaning and malware Analysis Center) aim to promote safe and secure digital practices.
7) **International Cooperation**: India actively participate in international efforts to combat cybercrime and cooperate with other countries in investigating cross-border cyber offenses. It is a signatory to the Budapest Convention on Cybercrime, a globally accepted treaty on combating cybercrime.

IT Act 2000 and its Amendments

The Indian Information Technology (IT) Act, 2000 is a significant piece of legislation that governs various aspects of electronic transactions, digital signatures, data protection, and cybercrimes in India. The act was enacted on October 17, 2000, and later amended in 2008 to address emerging challenges in the digital realm.

Here are some key features and provisions of the Indian IT Act:

1) **Digital Signature**: The Act recognizes digital signatures as legally valid and equivalent to physical signatures. It provides a legal framework for the use of digital signatures in electronic transactions, contracts, and other digital documents.
2) **Electronic Records and Documents**: Act acknowledges the legal validity of electronic records and documents. It enables the use of electronic records as evidence in legal proceedings.
3) **Electronic Governance**: The act promotes electronic governance by mandating the use of electronic means for government communications, filings, and transactions. It aims to reduce paperwork and enhance the efficiency of government processes.
4) **Cybercrime Offenses**: The, IT Act addresses various cyber offenses and provides penalties for unauthorized access to computer systems, data theft, computer-related fraud, cyberterrorism, and other cybercrimes. It also criminalizes the publishing or transmitting of obscene material in electronic form.
5) **Penalties and Adjudication**: The act prescribes penalties for offenses, which may include imprisonment and fines. It also sets up Adjudicating Officers to adjudicate offenses under the act.

Cyber Crime and Offences

India Information Technology Act has been protecting citizens from white-collar crimes to attacks by terrorist

The laws for cyber-crime safeguard citizens from dispensing critical information to a stranger online. The rise of the 21st century marked the evolution of cyberlaw in India with the Information Technology Act, 2000.

Cyber Crimes Offenses & Penalties in India

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters any computer source code when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to **three years, or/and with fine up to ₹200,000**

66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public information residing in a computer resource by any means, commits hack.	Imprisonment up to **three years, or/and with fine up to ₹500,000**
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen.	Imprisonment up to **three years, or/and with fine up to ₹100,000**
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to **three years, or/and with fine up to ₹100,000**
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to **three years, or/and with fine up to ₹100,000**
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to **three years, or/and with fine up to ₹200,000**
66F	Acts of cyberterrorism	If a person denies access to authorised personnel to a computer resource, accesses a protected system or introduces contaminants into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to **life.**

67	Publishing information which is obscene in electronic form.	If a person publishes any material which appeals to the explicit interest or if its effect is such as to tend to corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to **five years, or/and with fine up to ₹1,000,000**
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexually explicit act or conduct.	Imprisonment up to **seven years, or/and with fine up to ₹1,000,000**
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to **five years, or/and with fine up to ₹1,000,000** on first conviction. Imprisonment up to **seven years, or/and with fine up to ₹1,000,000** on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatory (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to **three years, or/and with fine.**
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.	Imprisonment up to **2 years, or/and with fine up to ₹100,000**

70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to **ten years, or/and with fine.**
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to **2 years, or/and with fine up to ₹100,000**

Organizations dealing with Cyber-crime and cyber security in India

Indian Cybercrime Coordination Centre (I4C) was established by MHA (Ministry of Home Affairs), in New Delhi to provide a framework and eco-system for Law Enforcement Agencies (LEAs) for dealing with Cybercrime in a coordinated and comprehensive manner. I4C is envisaged to act as the nodal point to curb Cybercrime in the country.

- The Expert Group identified the gaps and challenges in tackling Cybercrime and made specific recommendations to combat Cybercrime in the country. The Expert Group recommended creation of **Indian Cybercrime Coordination Centre (I4C)** to strengthen the overall security apparatus to fight against Cybercrime.

Objectives of I4C

- To act as a nodal point to curb Cybercrime in the country.
- To strengthen the fight against Cybercrime committed against women and children.
- Facilitate easy filing Cybercrime related complaints and identifying Cybercrime trends and patterns.

- To act as an early warning system for Law Enforcement Agencies for proactive Cybercrime prevention and detection.
- Awareness creation among public about preventing Cybercrime.
- Assist States/Union Territories in capacity building of Police Officers, Public Prosecutors and Judicial Officers in the area of cyber forensic, investigation, cyber hygiene, cyber-criminology, etc.