UNIT 1: CYBER SECURITY

1. Cyber Security

1.1 Definition

Cyber security encompasses a comprehensive framework of technologies, methodologies, and strategic policies designed to protect digital infrastructures, data systems, and networks from sophisticated cyber threats. It integrates cryptographic protocols, risk management strategies, and artificial intelligence-driven monitoring tools to ensure data confidentiality, integrity, and availability.

1.2 Importance of Cyber Security

- Establishes robust defensive mechanisms against unauthorized access and cyber intrusions.
- Ensures the confidentiality, availability, and integrity (CIA triad) of critical digital assets.
- Mitigates risks associated with advanced persistent threats (APTs) and zero-day exploits.
- Facilitates compliance with global cybersecurity regulations (e.g., GDPR, ISO 27001).
- Protects financial and intellectual assets from cybercriminal enterprises and state-sponsored actors.

2. Cybercrime and Information Security

2.1 Cybercrime: Definition

Cybercrime constitutes illicit digital activities executed with the intent of financial gain, data exfiltration, espionage, or critical infrastructure sabotage. It includes complex tactics such as polymorphic malware, ransomware-as-a-service (RaaS), and deepfake-enhanced fraud.

2.2 Information Security: Definition

Information security (InfoSec) involves systematic risk assessment, cryptographic encryption mechanisms, and multi-layered defense-in-depth strategies to counteract cyber threats and unauthorized data manipulation.

2.3 Distinctions Between Cybercrime and Information Security

Cybercrime	Information Security
Involves unlawful activities conducted in cyberspace.	Employs proactive strategies to protect digital assets.
Encompasses malware distribution, cyber fraud, and dark web operations.	Implements encryption, zero-trust architectures, and AI-driven intrusion detection.
Involves illegal activities using digital means.	Involves protection of information and data.
Includes hacking, fraud, and data breaches.	Includes encryption, access controls, and firewalls.
Targets individuals, organizations, or governments.	Aims to prevent unauthorized data access.

3. Cybercriminals

3.1 Definition

Cybercriminals operate as individuals, syndicates, or nation-state actors leveraging advanced digital methodologies for illicit gains, cyber espionage, or political subversion.

3.2 Categories of Cybercriminals

- **State-Sponsored Actors**: Government-affiliated groups executing cyber espionage and disruptive attacks.
- **Advanced Persistent Threat (APT) Groups**: Highly sophisticated entities engaging in prolonged cyberattacks.
- **Cyber Mercenaries**: Hackers-for-hire conducting cyber operations for financial incentives.
- **Insider Threats**: Employees or associates misusing privileged access to harm organizations.

4. Classification of Cybercrime

4.1 Based on Target

- **Against Individuals**: Identity fraud, cyberstalking, doxxing.
- **Against Organizations**: Corporate espionage, insider threats, intellectual property theft.

- **Against Nations**: Cyberterrorism, state-sponsored sabotage, critical infrastructure attacks.

4.2 Based on Modus Operandi

- **Advanced Persistent Threats (APTs)**: Long-term, covert cyber intrusion strategies.
- **Exploits and Zero-Day Attacks**: Exploitation of undisclosed software vulnerabilities.
- **Social Engineering Attacks**: Manipulating human psychology to gain unauthorized access.

5. Evolution of the Cybercrime Era

The cybercrime landscape has evolved in complexity:

- **Pre-2000s**: Simple malware, amateur hacking.
- **2000-2010**: Organized cybercrime, financial frauds, state-sponsored intrusions.
- **2010-Present**: AI-powered attacks, ransomware evolution, cyber warfare tactics.

6. Cyber Offences

6.1 Major Classifications

- **Economic Cybercrime**: Money laundering, crypto frauds, stock market manipulation.
- **Personal Data Exploitation**: Identity theft, privacy breaches, biometric data theft.
- **Political Cybercrime**: Election interference, information warfare, cyber espionage.

6.2 Cyberattack Lifecycle

- **Reconnaissance**: Intelligence gathering via OSINT and social engineering.
- **Weaponization**: Development of malware payloads, botnets, and automated exploits.
- **Delivery & Exploitation**: Deployment of cyberweapons via phishing, trojans, or exploits.
- **Command & Control (C2)**: Remote administration of compromised systems.
- **Execution & Exfiltration**: Data theft, system disruption, ransom demands.

7. Cyberstalking

7.1 Definition

Cyberstalking refers to persistent digital harassment, intimidation, or threats leveraging social media, geolocation tracking, and deepfake manipulation.

7.2 Techniques Utilized by Cyberstalkers

- **Malicious Surveillance**: Illicit tracking of an individual’s online presence.
- **Synthetic Identity Fraud**: Creation of fake profiles for manipulation and deception.
- **Persistent Harassment**: Psychological exploitation through digital communication.

8. Cybercafés as Cybercrime Hotspots

Public cybercafés often serve as hubs for anonymous cybercriminal operations.

8.1 Risks Associated with Public Networks

- **Unsecured Wi-Fi Threats**: Susceptibility to Man-in-the-Middle (MitM) attacks.
- **Keylogging & Credential Theft**: Malware-based interception of user inputs.
- **Data Residual Risks**: Inadvertent storage of personal credentials on shared systems.

9. Botnets and Cybercrime

9.1 Definition

Botnets are expansive networks of compromised devices under the remote command of cybercriminal entities.

9.2 Strategic Utilization of Botnets

- **DDoS-as-a-Service**: Large-scale disruption of online services.
- **Automated Cyber Fraud**: Credential stuffing, carding attacks, mass phishing.
- **Cryptojacking**: Unauthorized mining of cryptocurrency using hijacked computing power.

10. Cloud Computing and Its Cybersecurity Risks

10.1 Definition

Cloud computing facilitates on-demand computing resources but introduces unique security challenges.

10.2 Emerging Threats in Cloud Security

- **Data Integrity Attacks**: Manipulation of sensitive cloud-hosted records.

- **Hypervisor Exploits**: Attacks targeting virtualized environments.
- **Cloud Misconfiguration**: Poor access control leading to massive data leaks.