Introduction to Cybercrime

Outline

- Introduction
- Role of Electronic Communication Devices and Information and Communication Technologies in Cybercrime
- Mens rea and Actusreus in Cybercrime
- Types of Cybercrime
- Cybercrime against Individuals, Property Nation
- Crimes Associated with Mobile Electronic Communication Device
- Classification of Cybercriminals
- Execution of Cybercrime
- Tools used in Cybercrime
- Factors influencing Cybercrime
- Challenges to Cybercrime
- Strategies to prevent Cybercrime
- Extent of Cybercrime
- Terms and Terminologies Associated with Cybercrime

Introduction

- ‘Cybercrime’ encompasses acts committed in cyberspace.
- Cybercrime includes:

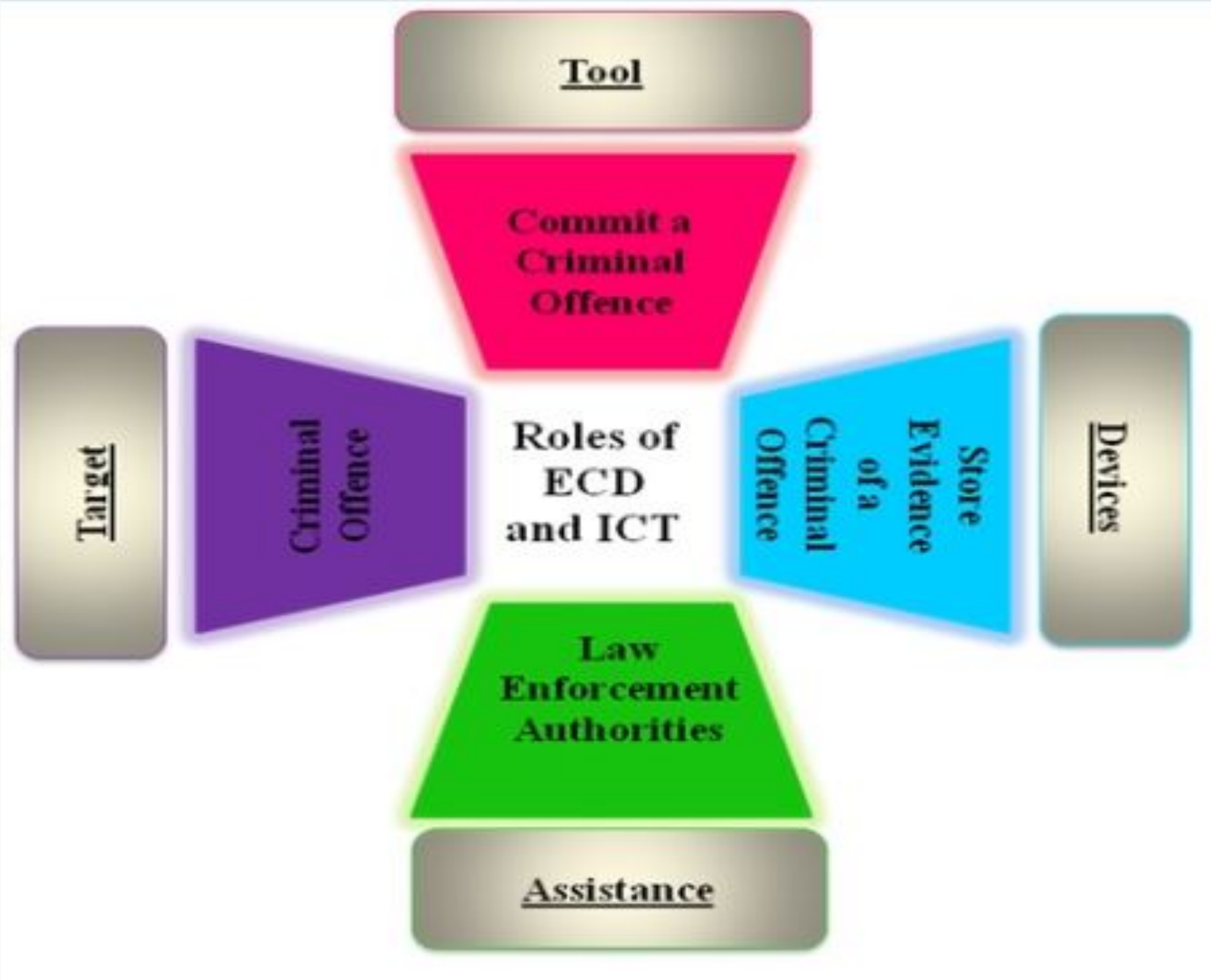
1. Crimes against confidentiality.
2. Integrity and availability of data and computer system.
3. Computer related traditional crimes.
4. Content related offences.
5. Offences related to infringement of copyright and privacy.

Introduction (Cont…)

Definition

- *An unlawful act wherein the electronic communication device is either a tool, target, or both.*

Role of Electronic Communication Devices and Information and Communication Technologies in Cybercrime

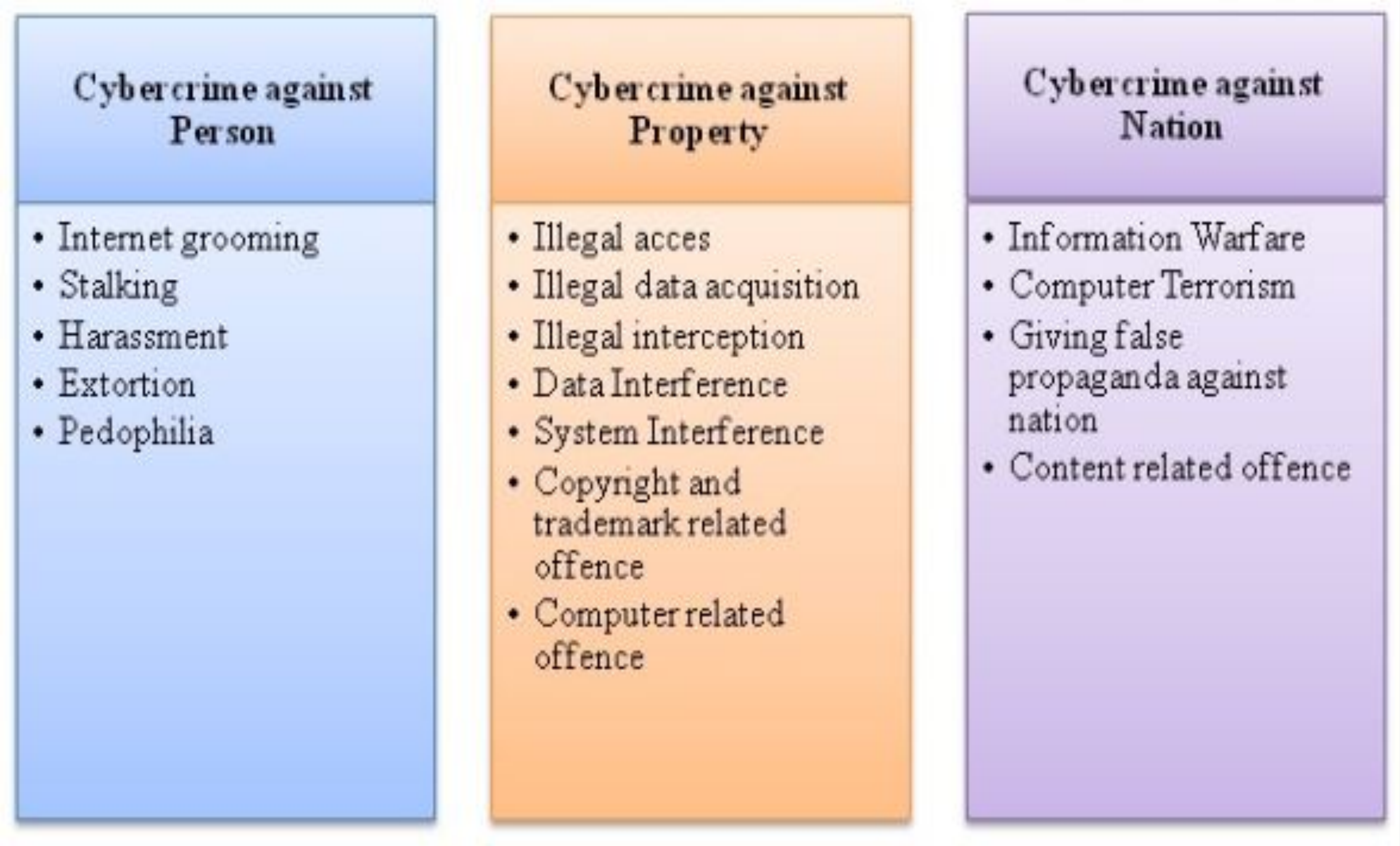

Tool
Commit a Criminal Offence
Target
Criminal Offence
Roles of ECD and ICT
Store Evidence of a Criminal Offence
Devices
Law Enforcement Authorities
Assistance

Mens rea and Actusreus in Cybercrime

- A fundamental principle of criminal law: Crime consists of both mental and physical elements.
- Mens rea (Mental element): A person’s awareness of the fact that his or her conduct is criminal.
- Actusreus (Physical element): The act itself.

Mens rea
+
Actus reus
=
Crime

Types of Cybercrime



Cybercrime against Person

- Internet grooming
- Stalking
- Harassment
- Extortion
- Pedophilia

Cybercrime against Property

- Illegal acces
- Illegal data acquisition
- Illegal interception
- Data Interference
- System Interference
- Copyright and trademark related offence
- Computer related offence

Cybercrime against Nation

- Information Warfare
- Computer Terrorism
- Giving false propaganda against nation
- Content related offence

Cybercrime against Individuals

- **Internet Grooming:** Befriending children to perpetrate sexual crimes, abuse, or exploitation over the Internet.
- **Stalking:** Sending threatening emails or messages to follow and harass the victim persistently.
  - *Cyber stalking:* Harassing, embarrassing, humiliating, isolating or frightening the victim by following him/her online.
  - *Internet stalking:* Sending obscene content or a virus repeatedly through email.
  - *Computer stalking:* Gain unauthorized access to a victim’s computer.
- **Harassment:** Uses online communication facilities to cause emotional distress.
- **Facebook stalking:** Using a Facebook account to follow the actions of the targeted Facebook user.

Cybercrime against Individuals (Cont…)

- **Extortion / Digital blackmail:** Damaging the reputation of an individual or an organization for exploiting money or any other benefit unlawfully.
- **Pedophilia:** Sexual predators approach children.
  - Online pedophiles exploit children through email, chat, and instant messages.
- **Internet troll:** A person who uses the Internet to post unwanted, provocative messages to an online community with the intention to provoke a person.
- **Pyramid scheme fraud:** Rewards people for enrolling others into an unsustainable business.
- **Credit card fraud:** Fraudster steals the card’s number, pin, and security code so as to make purchases on behalf of the victim without his/her authorization

Cybercrime against Property

1. Illegal Access – Hacking and Cracking

- Cracking of the passwords.
- Illegally gaining access to systems
- Spoofing systems and websites,
- Employ keyloggers to capture sensitive information.

– *SQL Injection:* Destroys the SQL database if it is unprotected.

– *Theft of FTP passwords:* Acquiring the website login information.

Cybercrime against Property (Cont…)

- *Cross-site scripting or XSS attack:* Compromise the users (victims) of a website to gain access to the user’s cookies, session IDs, and passwords.
- *Web jacking:* Alters the content or posts obscene content.
- *Exploit kits:* Exploiting the vulnerabilities in the software.

Cybercrime against Property (Cont…)

2. Illegal Data Acquisition – Data Espionage: Gaining access to sensitive information from any computer system.

3. Illegal Interception: Targets the communication medium to gain access to the sensitive information being exchanged.

- *Spoofing*
- *Skimming*
- *ATM hacking*

Cybercrime against Property (Cont…)

4. Data Interference:

- Gain access to the data may either delete it or alter it.
- Loss of access to data.
  - *Viruses*
  - *Trojan horse*
  - *Logic bombs*
  - *Ransomware*

5. System Interference: Results in huge financial loss to the victims.

- *DoS Attack*
- *Email bombing*
- *Email spamming*
- *Malvertising*
- *Publicly unwanted program*

Cybercrime against Property (Cont…)

6. Copyright and Trademark-related Offences

- *Copyright infringing software or software piracy*
- *Trademark-related offences*
- *Clone*
- *Software crack*

7. Computer-related Offences: Computer-related fraud, computer-related forgery, phishing, identity theft, and misuse of devices.

- *Impersonation*
- *Data diddling*
- *Salami slicing attack*
- *Remote commands*
- *Pharming*

Cybercrime against Property (Cont…)

8. Network attacks against mission-critical infrastructure.

- *Cyber terrorism*
- *Cyber warfare*
- *Cyber laundering*

Content-related Offences: Dissemination of content that is illegal.

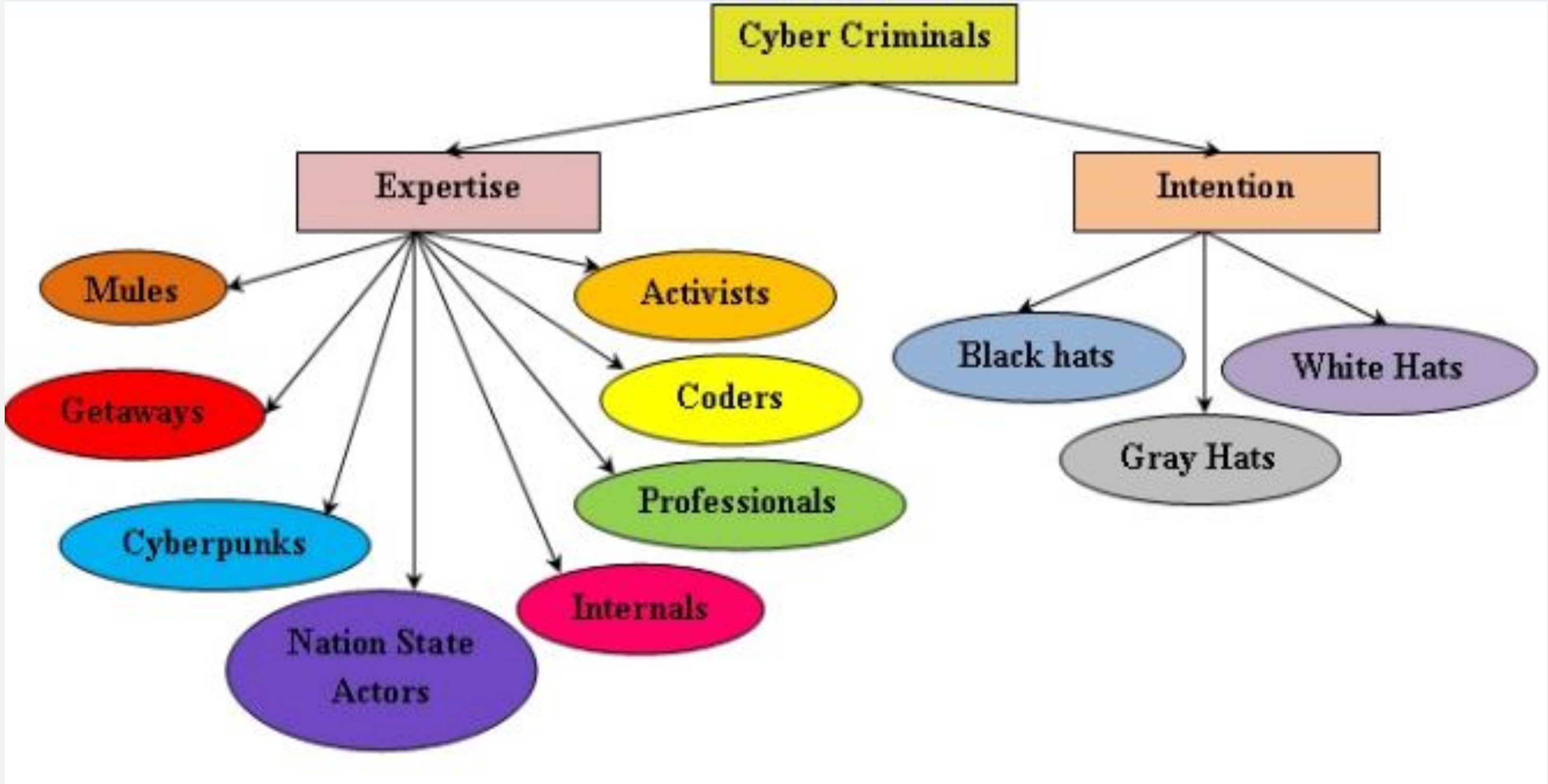
- *Pornography*
- *Racist and xenophobic material*
- *Religious offences*
- *Spread of false and defamatory information*
- *Email spam*

Crimes Associated with Mobile Electronic Communication Devices

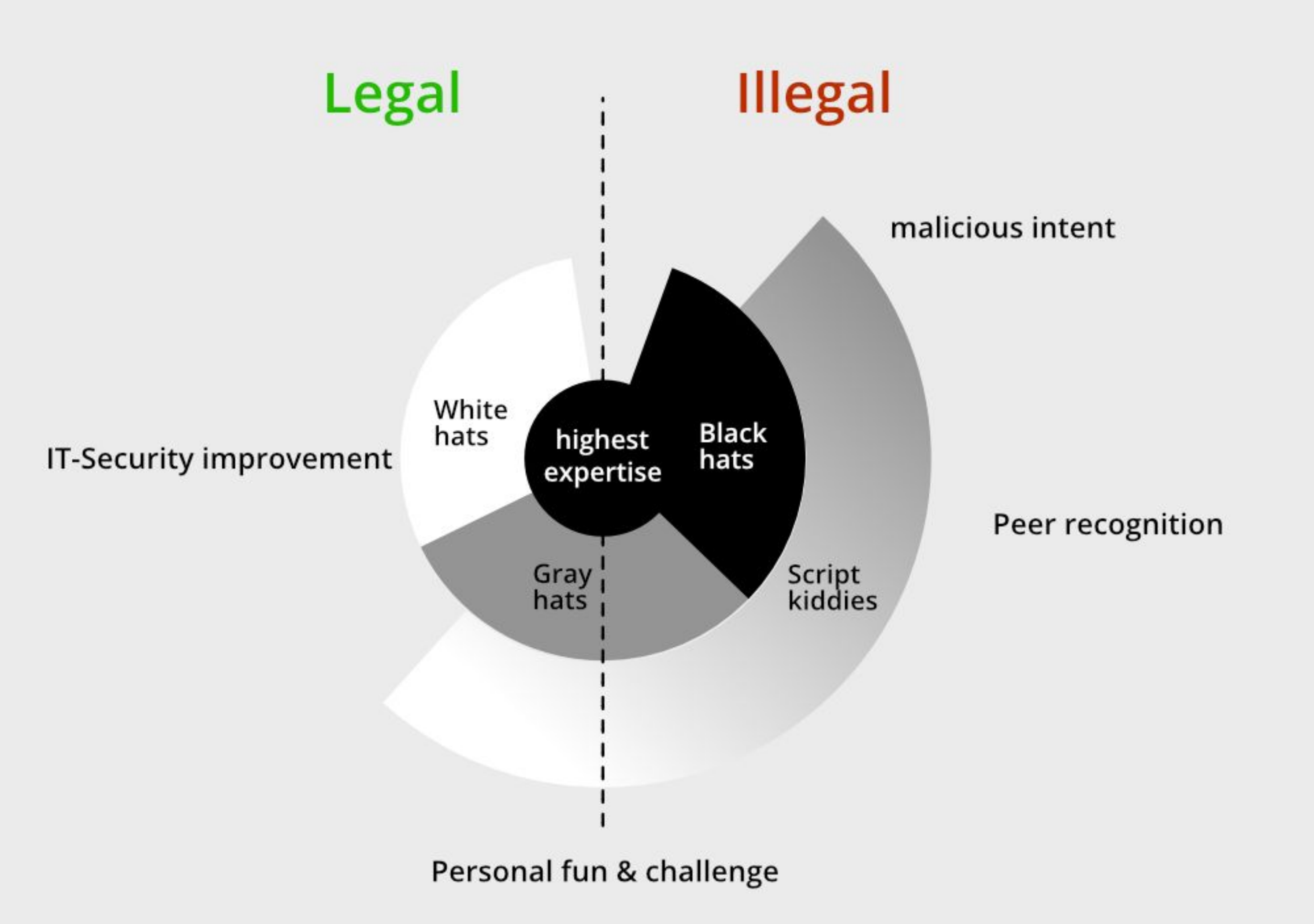
- Handset theft
- SMS-related crimes
  - *SMShing*
  - *Flashing SMS*
  - *Altering dates in SMS*
  - *SMS spoofing*
- Bluetooth mobile hacking
- Crimes with calls
- SIM card cloning
- MMS crime

Classification of Cybercriminals

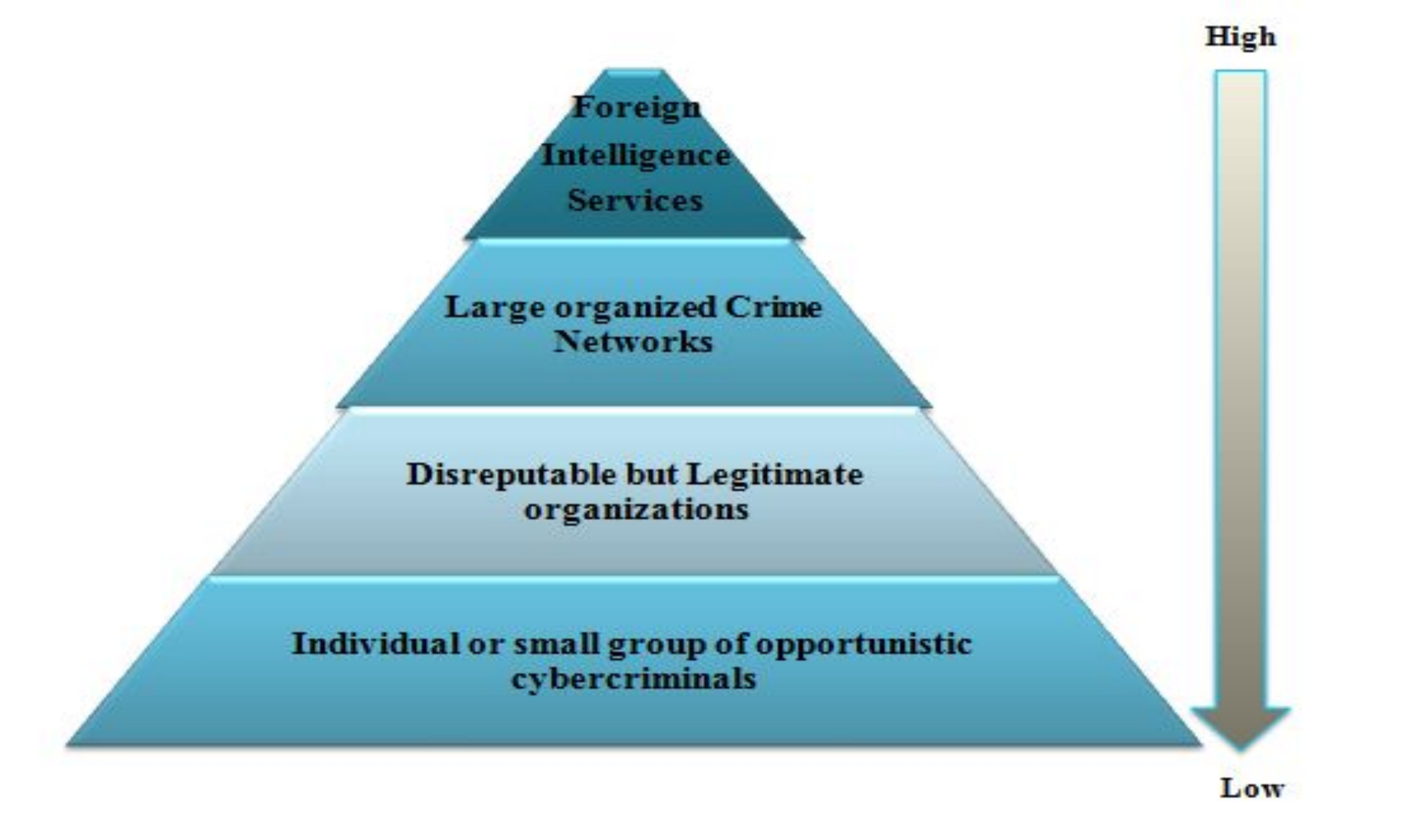
- Cybercriminals / Offenders: Hackers, crackers and network attackers.



Classification of Cybercriminals



Execution of Cybercrime



High

Foreign Intelligence Services

Large organized Crime Networks

Disreputable but Legitimate organizations

Individual or small group of opportunistic cybercriminals

Low

Tools used in Cybercrime

- Proxy servers and anonymizers
- Phishing
- Malware
- Keyloggers, password stealers and spyware
- Virus and worm
- Trojan and backdoors
- Steganography
- DoS and DDoS attacks
- SQL injection
- Buffer overflow

Tools used in Cybercrime (Cont…)

- Cracking
- Data diddling
- Rootkit
- Salami attack
- Sniffer
- Social engineering
- Spoofing
- Rogue security software
- Pharming
- Hijackware

Tools used in Cybercrime (Cont…)

- Man-in-the middle or MITM attack
- Watering hole

Factors influencing Cybercrime

- Availability of tools to commit crime.
- No necessity of physical presence to commit crime.
- Less investment to commit crime.
- Availability of forensic tools to mask crime.
- Jurisdictional concern of cybercrime.
- Lack of awareness regarding usage of ECDs.
- Impact of social media.

Strategies to prevent Cybercrimes

- Turn off the systems when not in use.
- Use of antivirus software and periodic updating of the same is essential.
- Always turn on the firewall.
- Update all software in the system.
- Lock social media accounts while not in use.
- Use of more than one email account (banking, shopping) is desirable.
- Avoid clicking on pop-ups.

Strategies to prevent Cybercrimes (Cont…)

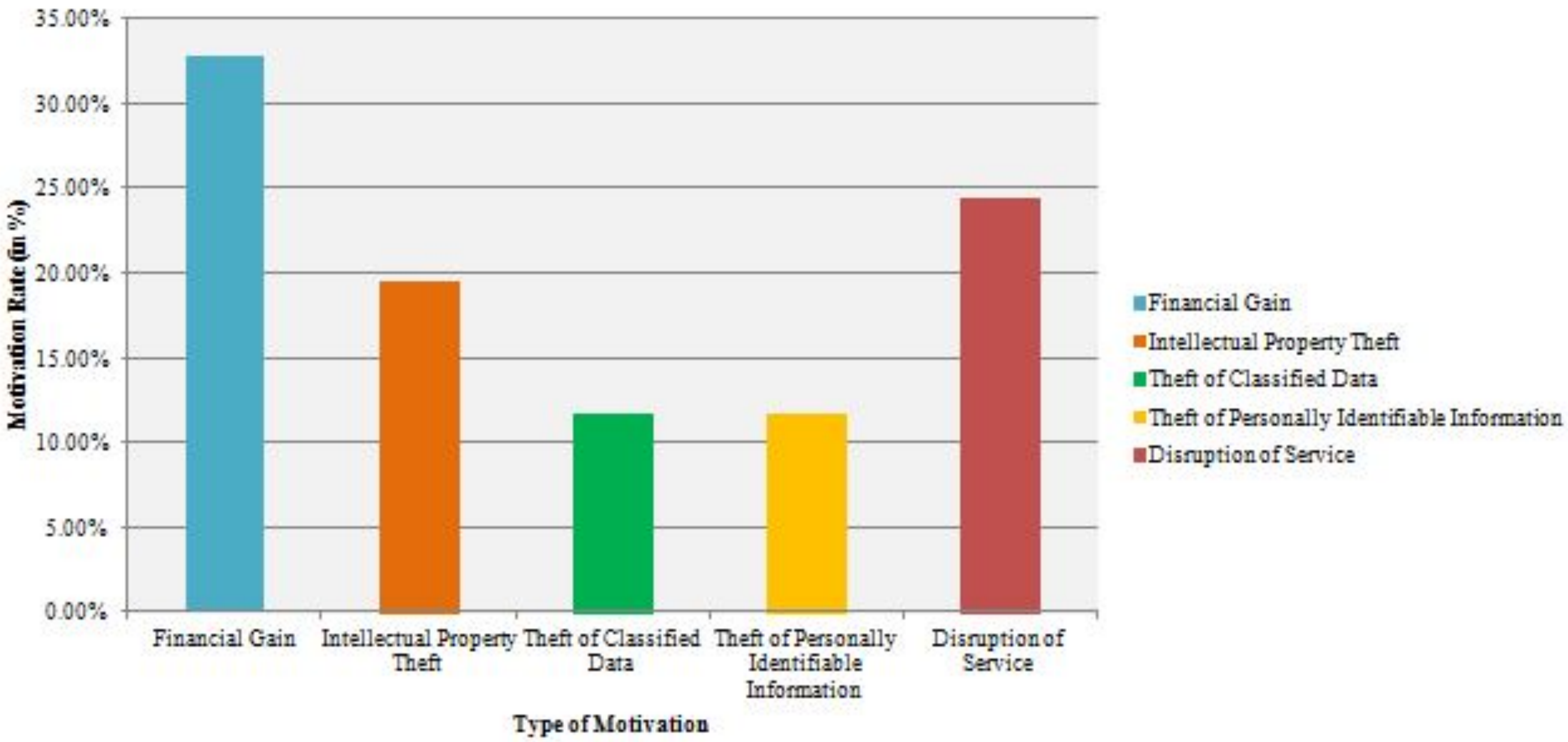
- Enable two-step verification for email and social media accounts.
- Avoid opening unknown attachments in emails.
- Avoid shopping online and if necessary proceed only on secure sites.
- Be aware of the privacy policies of social media and websites.
- Use strong passwords.
- Avoid maintaining credit card details and disclosing other valuable information on websites.
- Keep updated of major security breaches.

Strategies to prevent Cybercrimes (Cont…)

Global Best Practices

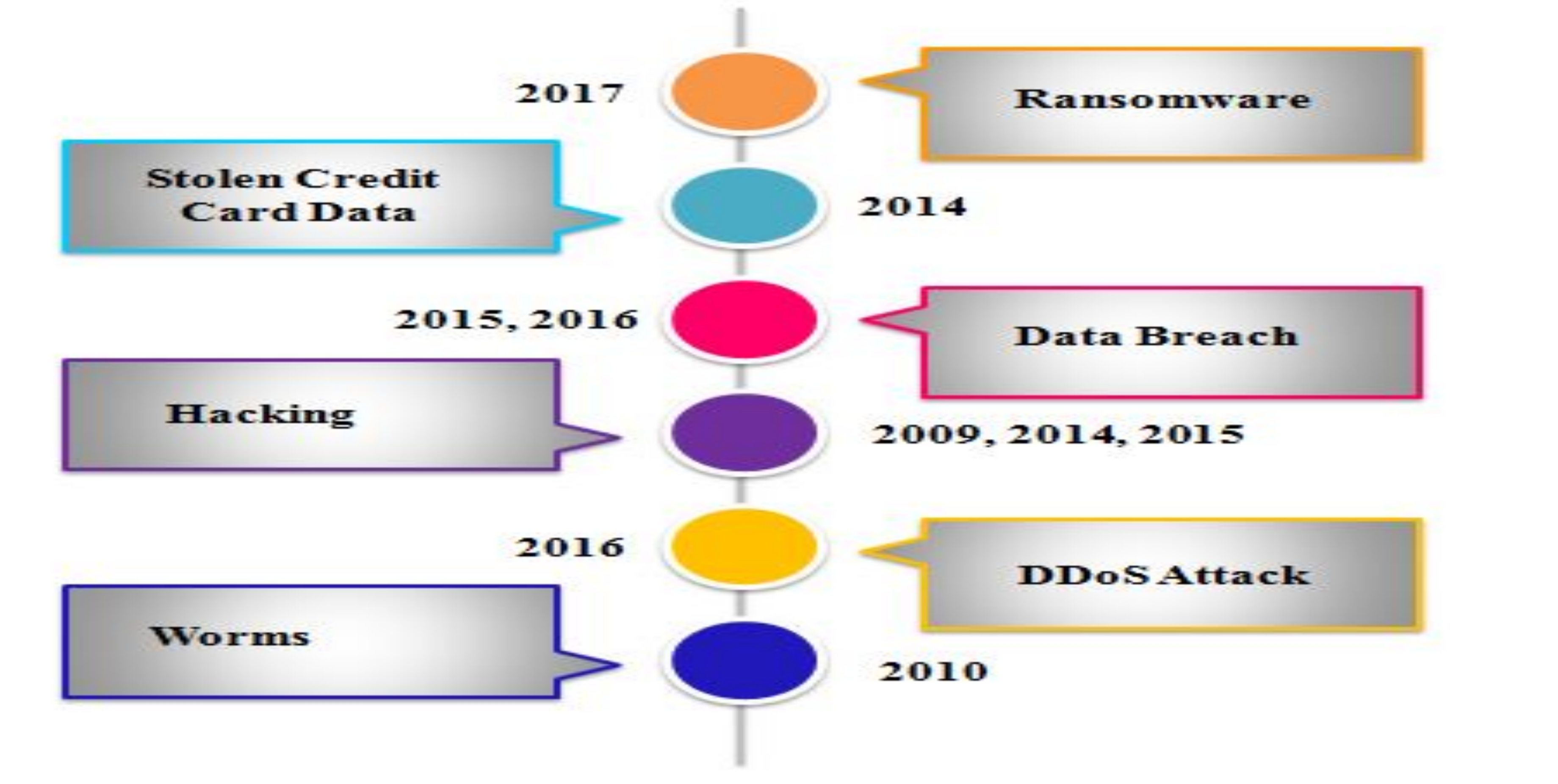
- Dedicated ministry: Responsible for cyber security.
- National cyber security coordinator: oversees cyber security activities across the country.
- National Cybersecurity Center Point: Deals with the protection of a nation's cyberspace.
- Legal measures are taken after review of cyber laws.
- National cyber security framework defines the minimum or mandatory security requirements.
- Cybercrime reporting and analysis is performed.
- National programme is convened to raise awareness about cyber threats.
- A programme is conducted to train cyber security professionals.
- International cooperation is extended.

Extent of Cybercrime (Cont…)



Extent of Cybercrime (Cont…)

Recent Sensitive Cybercrimes


2017
Ransomware
Stolen Credit Card Data
2014
2015, 2016
Data Breach
Hacking
2009, 2014, 2015
2016
DDoS Attack
Worms
2010