SHANKAR
IAS PARLIAMENT
Information is Empowering

Prevention of Cyber Crimes

Why in news?

The States and Union Territories are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cybercrime through their Law Enforcement Agencies (LEAs).

Status of Cybercrime in India
• 'Police' and 'Public Order' are State subjects as per the 7th Schedule of the Constitution of India. • Hence States and UTs are responsible for cybercrime prevention, detection etc., • The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes. • As per Crime in India 2022 report majority of the cybercrime cases are fraud, extortion and sexual exploitation • The states most affected with the cybercrimes are Maharashtra, Karnataka, Uttar Pradesh, Telangana and Kerala. • As per a research, online abuse disproportionately affected *young women*. • Out of 400 students surveyed from 111 Indian higher education institutions (HEIs), it is found around 60% of women experienced some form of Technology Facilitated Sexual Violence compared to only 8% of men. • A global study by Economist Intelligence Unit found that 38% of women have had personal experiences of online violence, and 85% of women who spend time online have witnessed digital violence against other women.

What is a cyber-crime?

- It is a *criminal activity* that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money.
- Cybercrime can be carried out by individuals or organizations, some are organized, use advanced techniques and are highly technically skilled.
- **Types-**
    - Email and internet fraud.
    - **Identity fraud-** Personal information is stolen and used.
    - **Cyberextortion-** Demanding money to prevent a threatened attack.
    - **Cryptojacking-** Hackers mine cryptocurrency using resources they do not own.
    - **Cyberespionage-** Hackers access government or company data.
    - Infringing copyright, illegal gambling etc.,

To know about cyber threats click here

What are the steps taken to prevent cyber-attack?

- **Indian Computer Emergency Team (CERT-In)** - CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.
- **Indian Cyber Crime Coordination Centre (I4C) -** It is launched to deal with all types of cybercrime in the country, in a coordinated and comprehensive manner.
  - National Cyber Forensic Laboratory
  - National Cyber Crime Reporting Portal
  - Citizen Financial Cyber Fraud Reporting and Management System
- **National Cyber Forensic Laboratory (Investigation) -** It has been established at ***New Delhi*** to provide early stage cyber forensic assistance to Investigating Officers.
- **National Cyber Crime Reporting Portal-** It has been launched to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cybercrimes against *women* and *children*.
- **Citizen Financial Cyber Fraud Reporting and Management System-** It has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters.
- **National Cyber Forensic Laboratory (Evidence)** - It has been set up at ***Hyderabad*** to provide the necessary forensic support in cases of evidence related to cybercrime, preserving the evidence and its analysis in line with the provisions of Information Technology Act and Evidence Act.
- **National Cyber Security Coordinator** - It is under the National Security Council Secretariat, coordinates with different agencies at the national level on cybersecurity issues.
- **The National Critical Information Infrastructure Protection Centre** - It has been set up for the protection of national critical information infrastructure.
- **Cyber Swachhta Kendra** - It is a *Botnet Cleaning and Malware Analysis Centre* that has been launched for detection of malicious software programmes and to provide free tools to remove them.
- **National Cyber Coordination Centre** - It works on creating awareness about existing and potential threats.
- **Cyber Crisis Management Plan** - It has been formulated for countering cyber-attacks.
- **Centre for Financial Literacy Project**- It was launched by Reserve Bank of India in 2017 as a pilot project on financial literacy with an objective to adopt community led innovative and participatory approaches.
- **Massive Open Online Courses (MOOC) platform**- 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc., along with certification.
- **Awareness generation**- Dissemination of messages through SMS, I4C social media account.
  - Example- CyberDostI4C in Facebook, Radio campaign, Cyber Safety and Security Awareness weeks etc.,
- **Cyber Surakshit Bharat programme-** It is a public-private partnership to educate and enable the Chief Information Security Officers & broader IT community in

Central/State Governments, Banks, PSUs and Government organizations to address the challenges of cyber security.

To know about cybersecurity click here

References

1. PIB- Cybercrime awareness
2. PIB- Cybercrime awareness in rural areas