Challenges in Cyber Security

Why in news?

India's rapid adoption of digital technology over the past decade has introduced new challenges, particularly for policymakers and the security apparatus.

What are the challenges posed by cybercrime?

- **Deep fake videos**- These are manipulated videos that could cause havoc during elections and other sensitive events.
- **Privacy violation-** Cybercriminals can impersonate individuals and engage in identity theft.
- **Financial scams-** The Cambridge Analytica data scandal involved harvested social media data for election advertising.
- **Financial fraud**- It is originated from 3 contiguous Southeast Asian countries: Myanmar, Laos, and Cambodia.

Categories of cyber fraud

- **I4C-** Indian Cyber Crime Coordination Centre has identified four main categories of cyber frauds.
- **Trading scam**- Fraudsters post advertisements on social media offering free trading tips, often using images of well-known stock market experts and fake news articles.
- **Digital arrest-** Victims receive calls informing them that they are implicated in crimes involving illegal goods or contraband.
- **Investment scam-** Victims receive WhatsApp messages from overseas numbers offering work-from-home opportunities to earn money by boosting social media ratings.
- After completing initial tasks and receiving small payments, they are asked to participate in pre-paid tasks requiring larger deposits.
- **Dating scam**- Male victims are targeted by fraudsters posing as foreign women interested in relationships or marriage

What are the steps taken by India to prevent cyber-attack?

- **Indian Computer Emergency Team (CERT-In)** - It 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.
- **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.
- **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.,

Institutional framework
• **MeitY-** The Ministry for Electronics and Information Technology handles policies related to IT, electronics, and the Internet, including cyber laws. • **Internal security**- The Ministry of Home Affairs (MHA) is responsible for internal security, • **Cybersecurity wing-** MHA has created the Cyber and Information Security Division, which includes the cybercrime and cybersecurity wings.
Legislative framework for cybersecurity

• The Bharatiya Nagarik Suraksha Sanhita (BNSSS), Bharatiya Nyaya Sanhita, and Bharatiya Sakshya Adhiniyam (BSS) were enacted to update India's legal system.
• **Electronic FIRs**- The BNSSS allows for the registration of electronic First Information Reports (FIRs) and recognizes electronic evidence as primary proof.
• **Data collection**- The BNSSS permits data collection for criminal identification, enhancing the ability to track and prosecute cybercriminals.
• **Digital trials-** All trials, inquiries, and proceedings can be conducted electronically, streamlining legal processes and reducing delays.
• **Classification of electronic records-** The BSS classifies electronic records as primary evidence, expanding the definition to include information stored in various digital devices.

What lies ahead?

- The surge in financial frauds over the Internet underscores the need for heightened cybersecurity measures and public awareness.
- The government and cybersecurity agencies must continue to strengthen their efforts to combat these sophisticated scams and protect citizens from falling prey to cybercriminals.

References

1. Indian Express- Challenges in cyber crime
2. Indian Express- Criminals in South Asia trap Indians online