36th CISO Deep-Dive Training Programme

Why in News?

The **National e-Governance Division (NeGD)**, under its **Capacity Building scheme**, organised 36th **CISO Deep-Dive training programme** with 24 participants from Central Line Ministries and States/UTs at **Indian Institute of Public Administration, New Delhi.**

- The training program is a part of a series of workshops organised under the **Cyber Surakshit Bharat initiative.**

What is Cyber Surakshit Bharat Initiative?

- The **Cyber Surakshit Bharat initiative** was conceptualised with the mission to spread awareness about cyber-crime and build capacities of Chief Information Security Officers (CISOs) and frontline IT officials, across all government departments.
- It was launched by the **Ministry of Electronics and Information Technology (MeitY) in 2018** in cooperation with **National e-Governance Division (NeGD)** and various industry partners in India.

What is CISOs Deep Dive Training?

- **About:**
  - It is the first-of-its-kind partnership between the Government and industry consortium under **Public Private Partnership (PPP) model.**
- **Objectives:**
  - Create awareness on the emerging landscape of cyber threats.
  - Provide in-depth understanding of related solutions.
  - Applicable frameworks, guidelines & policies related to cyber security.
  - Share best practices to learn from success & failures.
  - Provide key inputs to take informed decisions on Cyber Security related issues in their respective functional area.
- **Participants:**
  - The programme is organised for chief information security officers (CISOs) and frontline IT officials from various ministries and departments, government and semi-government organisations from central and state governments, PSUs, and banks among others.
- **Training:**
  - NeGD provides logistic support in arranging the training programmes, whereas the industry consortium provides technical support for the training.
  - The training partners from the industry are **Microsoft, IBM, Intel, Palo Alto Networks, E&Y, and Dell-EMC,** NIC**,** CERT-In**, and CDAC are knowledge partners from the Government side.**

What are the Other Initiatives Related to Enhancing Cyber Security?

- **Global:**
  - **Budapest Convention on Cybercrime**
  - Internet Governance Forum **(IGF)**

- **India-Specific:**
  - **National Cyber Security Strategy 2020**
  - **National Critical Information Infrastructure Protection Centre (NCIIPC)**
  - **Indian Cyber Crime Coordination Centre (I4C)**
  - **National Cyber Crime Reporting Portal**
  - **Computer Emergency Response Team - India (CERT-In)**
  - **Digital Personal Data Protection Bill 2022**
  - **Defence Cyber Agency (DCyA)**
  - **Digital India Bill, 2023**
  - **Cyber Swachhta Kendra:** In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.

UPSC Civil Services Examination Previous Year Question (PYQ)

Prelims

Q. The terms 'WannaCry, Petya and EternalBlue' sometimes mentioned in the news recently are related to (2018)

(a) Exoplanets
(b) Cryptocurrency
(c) Cyber-attacks
(d) Mini satellites

Ans: (c)

- **Ransomware is a form of malicious software (or malware). Once it takes over the computer, it threatens to harm the user, usually by denying access to data.** The attacker demands a ransom from the victim, promising to restore access to the data upon payment. WannaCry, Petya and EternalBlue are few of the ransom ware, which created havoc by demanding the victim ransom payment in bit coin (crypto currency).
- Cryptocurrency is a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. Therefore, option (c) is the correct answer.

Source: PIB