New Cybersecurity Initiatives

September 11, 2024 • vajiramandravi.com

New Cybersecurity Initiatives:

- **Cyber Fraud Mitigation Centre (CFMC):**
  - CFMC has been established **at the Indian cybercrime Coordination Centre (14C)** in **New Delhi** with **representatives of major banks**, Financial Intermediaries, **Payment Aggregators**, **Telecom Service Providers**, **IT Intermediaries,** and States/UTs **Law Enforcement Agencies** (LEAs).
  - They will work together for immediate action and seamless cooperation to **tackle online financial crimes.**
  - CFMC will serve as an example of "**Cooperative Federalism**" in law enforcement.
- **Samanvaya Platform (Joint Cybercrime Investigation Facilitation System**): It is a web-based module to act as a **One Stop Portal for data repository of cybercrime**, data sharing, crime mapping, data analytics, cooperation, and **coordination platform for LEAs** across the country.
- **'Cyber Commandos' Program:**
  - Under this program, a **special wing of trained 'Cyber Commandos' in States/UTs** and **Central Police Organizations (CPOs)** will be established to counter threats of cyber security landscape in the country.

    - Trained Cyber Commandos will **assist States/UTs and Central Agencies** in securing the digital space.
- **Suspect Registry**: It is a new initiative to **strengthen fraud risk management** by creating a **registry of identifiers based on** the **National Cybercrime Reporting Portal** in **collaboration with banks** and financial intermediaries.

Key Facts about Indian Cyber Crime Coordination Centre (I4C):

- I4C has been established **under the Ministry of Home Affairs (MHA)** to deal with cybercrime in the country in a coordinated and comprehensive manner.
- The I4C focuses on tackling issues related to cybercrime for citizens, including improving coordination between various LEAs and stakeholders.
- The centre is **located in New Delhi.**
- **Functions:**
    - To act as a **nodal point** in the **fight against cybercrime.**
    - Identify the research problems and needs of LEAs and **take up R&D activities** in developing new technologies and forensic tools in collaboration with academia / research institutes within India and abroad.
    - To **prevent misuse of cyberspace** for furthering the cause of extremist and terrorist groups.
    - **Suggest amendments**, if required, **in cyber laws** to keep pace with fast changing technologies and international cooperation.
    - To **coordinate all activities related** to the **implementation of Mutual Legal Assistance Treaties (MLAT)**with other countries related to cybercrimes in consultation with the concerned nodal authority in MHA.
- **Components of I4C:**
    - **National Cybercrime Threat Analytics Unit (TAU):** For reporting threats pertaining to cybercrimes at regular intervals.
    - **National Cybercrime Reporting Portal (NCRP):** To report various cybercrime complaints by citizens at all India level on a common platform on a 24×7 basis from “anywhere, anytime”.
    - **National Cybercrime Training Centre (NCTC):** To impart training to government officials, especially state law enforcement agencies.
    - **National Cybercrime Research and Innovation Centre:** To carry out research for the development of indigenous tools for the prevention of cybercrimes.
    - **Platform for Joint Cyber Crime Coordination Team:** For coordination, sharing of modus operandi of cybercrimes, data/information among states/UTs LEAs.
    - **Cybercrime Ecosystem Management Unit:** For creating mass awareness in cyber hygiene for prevention of cybercrimes.
    - **National Cybercrime Forensic Laboratory (Investigation) Ecosystem:** For helping LEAs in cyber forensics investigation.
- I4C **brings together academia, industry**, **public** and **government** in the prevention, detection, investigation, and prosecution of cybercrimes.

- I4C has **envisaged the Cyber Crime Volunteers Program** to bring together citizens with passion to serve the nation on a single platform and contribute in fight against cybercrime in the country.

Q1: What is the Indian Computer Emergency Response Team (CERT-In)?

It is the national nodal agency for responding to computer security incidents as and when they occur. It is a functional organisation of the Ministry of Information & Electronics Technology, Government of India, with the objective of securing Indian cyberspace. CERT-In has been operational since January 2004. The constituency of CERT-In is the Indian cyber community and Indian cyberspace.

Source: ‘National Security Not Possible without Cybersecurity’: Amit Shah Launches Four Key Initiatives