Indian Cyber Crime Coordination Centre

July 1, 2020

Union Minister for Home Affairs inaugurated the Indian Cyber Crime Coordination Centre (I4C) and Also dedicated the National Cyber Crime Reporting Portal to the Nation recently. This state-of-the-art center is **located in New Delhi.**

About Indian Cyber Crime Coordination Centre (I4C)

- I4C is meant to **combat cybercrime in the country, in a coordinated and effective manner.**
- **The scheme was approved in October 2018**
- At the initiative of the Union Ministry for Home Affairs (MHA), 15 States and UTs have given their consent to set up **Regional Cyber Crime Coordination Centres** at respective States/UTs.
- The scheme is proposed to **act as a nodal point in the fight against cybercrime.**
- It envisages to **identify the research problems and take up R&D activities** in developing new technologies and forensic tools in collaboration with academia/ research institutes within India and abroad.
- It is meant to **prevent misuse of cyberspace** for furthering the cause of extremist and terrorist groups.
- It would suggest amendments, if required, in cyber laws to keep pace with fast-changing technologies and international cooperation.
- **It coordinates 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 the MHA.

Components of I4C:

The scheme has the following seven components:

1) National Cybercrime Threat Analytics Unit (TAU)

- TAU shall provide a **platform for law enforcement personnel, persons from the private sector,** academia, research organizations and law enforcement specialists to work collaboratively.
- It shall **produce cybercrime threat intelligence reports** and organize periodic interaction on specific cyber crime centric discussions.

2)National Cyber crime Reporting

- This unit will **work in tandem with already established investigation units at state and central** levels as well as experts from different spheres to create expert investigation teams.
- Will have the **capability to respond in real-time to rapidly changing cyber crime threat.**

3)Platform for Joint Cyber crime Investigation Team

- Its objective is to **drive intelligence-led, coordinated action against key cyber crime threats** and targets.

4)National Cyber crime Forensic Laboratory (NCFL) Ecosystem

- **Forensic analysis and investigation of cyber crime** as a result of new digital technology and techniques.
- Develop a centre to support the investigation process.

5)National Cyber crime Training Centre (NCTC)

- It will be set up to **focus on standardization of course curriculum focused on cybercrimes**, impact containment and investigations, **imparting practical cybercrime detection, containment and reporting training on simulated cyber environments.**
- Development of **Massive Open Online Course** to be

delivered on a cloud-based training platform.

6)Cybercrime Ecosystem Management Unit

- **Develop ecosystems that bring together academia, industry and government to operate**, investigate a cybercrime basis established standard operating procedures, contain the impact of cybercrimes and respond to cybercrimes.
- Provide **incubation support** for the development of all components of the cybercrime combatting ecosystem.

7)National Cyber Research and Innovation Centre

- **Track emerging technological developments; proactively predict potential vulnerabilities,** which can be exploited by cybercriminals.
- **Create strategic partnerships** with all entities in the area of research and innovation focused on cybercrimes, cybercrime impact containment and investigations.
- **National Cyber Crime Reporting Portal**
- It is a **citizen-centric initiative that will enable citizens to report cybercrimes online through the portal**.
- **All the cybercrime-related complaints will be accessed by the concerned law enforcement** agencies in the States and Union Territories for taking action as per law.
- This **portal was launched on a pilot basis on 30th August 2019** and it enables filing of all cybercrimes with a specific focus on crimes against women, children, particularly child pornography, child sex abuse material, online content pertaining to rapes/gang rapes, etc.