Indian Cyber Crime Coordination Centre (I4C)

August 30, 2019
***Source**: PIB & Ministry of Home Affairs*

Ministry of Home Affairs(MHA) has rolled out a scheme 'Indian Cyber Crime Coordination Centre (I4C)' **for the period 2018-2020**, to combat cyber crime in the country, in a coordinated and effective manner.

Objectives

- To act as a **nodal point** in the fight against cybercrime
- To Identify the research problems/needs of Law Enforcement Agencies (LEAs) and take up **R&D** activities in developing new technologies and forensic tool
- To **prevent misuse of cyberspace** for furthering the cause of extremist and terrorist groups
- To **suggest amendments,** if required, in cyber laws to keep pace with fast changing technologies and International cooperation
- To coordinate all activities related to implementation of **Mutual Legal Assistance Treaties (**MLAT) **with other countries** related to cybercrimes in consultation with the concerned nodal authority in MHA

Components

The scheme has following **seven components:**

1.National Cybercrime Threat Analytics Unit:

- It shall provide a platform for law enforcement personnel, persons from the private sector, academia and research organizations to work collaboratively in order to analyse all pieces of puzzles of cybercrimes.
- Threat Analytics Unit shall also produce cybercrime

threat intelligence reports and organize periodic interaction on specific cybercrime centric discussions.
- Create multi-stakeholder environment for bringing together law enforcement specialists and industry experts.

2.National Cybercrime 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.
- It Will have the capability to respond in real time to rapidly changing cybercrime threat.
- It Will be able to collaborate with partners to investigate cyber and cyber-enabled crime.

3.Platform for Joint Cybercrime Investigation Team:

- Its objective is to drive intelligence-led, coordinated action against key cybercrime threats and targets.
- This will facilitate the joint identification, prioritization, preparation and initiation of multi-jurisdictional against cybercrimes.

4.National Cybercrime Forensic Laboratory Ecosystem:

- Forensic analysis and investigation of cybercrime as a result of new digital technology and techniques.
- Develop a centre to support investigation process. NCFL and associated Central Forensic Science Laboratory to be well-equipped and well-staffed in order to engage in analysis and investigation activities to keep-up with new technical developments, using which a completely new kind of cybercrime might have been committed.

5.National Cybercrime Training Centre(NCTC):

- NCTC will be setup to focus on standardization of course curriculum focused on cybercrimes, impact containment

and investigations, imparting practical cybercrime detection, containment and reporting trainings on simulated cyber environments.

- Development of Massive Open Online Course to be delivered on a cloud based training platform.
- It will also focus on establishing Cyber Range for advanced simulation and training on cyber-attack and investigation of such cybercrimes.

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 development of all components of cybercrime combatting ecosystem.

7.National Cyber Research and Innovation Centre:

- It tracks emerging technological developments, proactively predict potential vulnerabilities, which can be exploited by cybercriminals.
- To leverage the strength and expertise of all stakeholders, be it in academia, the private sector or inter-governmental organizations.
- It creates strategic partnerships with all such entities in the area of research and innovation focused on cybercrimes, cybercrime impact containment and investigations.