Indian Cyber Crime Coordination Centre (I4C)

January 24, 2020
***Source**: The Hindu*

Manifest pedagogy: Indian cyber crime coordination centre was a long carved out plan since the formulation of National Cyber Security Policy in 2013. Since cyber security is an exclusive topic in mains syllabus, it becomes very important. Even in prelims the factual questions on I4C might be asked.

In news: Union Minister for Home Affairs recently inaugurated the Indian Cyber Crime Coordination Centre (I4C) and also dedicated National Cyber Crime Reporting Portal.

Placing it in syllabus: Internal security

Static dimensions: National cyber security policy, 2013

Current dimensions:

- I4C
- Its components
- National Cyber Crime Reporting Portal

Content: I4C is meant to combat cyber crime in the country, in a coordinated and effective manner. **India is ranked a high 23rd** out of 165 nations in a **Global Cybersecurity Index (GCI), 2017** released by the International Telecommunication Union (ITU).

Cyber Crimes in India almost doubled in 2017 than in 2015, according to statistics released by the National Crime Records Bureau (NCRB). Hence I4C is a first step in the right direction to deal with cybercrimes. The scheme was approved in October 2018 with an **outlay of Rs. 415.86 Crore and for two years (2018-2020).**

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.

National Cybersecurity policy, 2013:

The policy **aims at** facilitating the creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders actions for the protection of cyberspace.

Vision: To build a secure and resilient cyberspace for citizens, businesses and Government.

Objectives:

- To **create a secure cyber ecosystem in the country**, generate adequate trust & confidence in IT systems and transactions in cyberspace.
- To **create an assurance framework for the design of security policies** and for promotion and enabling actions for compliance to global security standards.
- To **strengthen the Regulatory framework** for ensuring a Secure Cyberspace ecosystem.
- To **enhance and create National and Sectoral level 24 x 7 mechanisms** for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management.
- To operate a 24×7 **National Critical Information Infrastructure Protection Centre (NCIIPC).**
- To **develop suitable indigenous security technologies** leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.
- To **create a workforce of 500,000 professionals skilled in cyber security** in the next 5 years through capacity building, skill development and training.

- To **provide fiscal benefits to businesses** for adoption of standard security practices and processes.
- To **enable protection of information** while in process, handling, storage & transit so as to safeguard the privacy of citizen’s data and for reducing economic losses due to cyber crime or data theft.
- To **enable effective prevention, investigation and prosecution of cyber crime** and enhancement of law enforcement capabilities through appropriate legislative intervention.
- To **develop effective public private partnerships** and collaborative engagements for enhancing the security of cyberspace.

I4C scheme:

- 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 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 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 cybercrime centric discussions.

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.
- Will have the capability to respond in real time to rapidly changing cybercrime threat.

3) Platform For Joint Cybercrime Investigation Team

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

4) National Cybercrime Forensic Laboratory (NCFL) Ecosystem

- Forensic analysis and investigation of cybercrime as a result of new digital technology and techniques.
- Develop a centre to support investigation process.

5) National Cybercrime Training Centre (NCTC)

- It 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.

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**

- 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 cyber crimes online.**
- This portal was launched on pilot basis on 30th August, 2019.
- It enables filing of all cyber crimes with specific focus on crimes against women, children, particularly child pornography, child sex abuse material, online content pertaining to rapes/gang rapes, etc.
- This portal also focuses on specific crimes like financial crime and social media related crimes like stalking, cyber bullying, etc..
- So far, **more than 700 police districts and more than 3,900 police stations have been connected** with this Portal.
- After successful completion, this portal will **improve coordination amongst the law enforcement agencies of different States, districts and police stations** for dealing with cyber crimes.