Cyber Crime Volunteers

Why in News

The Internet Freedom Foundation (IFF), a digital liberties organisation, has written to the **Ministry of Home Affairs (MHA)** that the **cyber crime volunteers concept** will lead to a "culture of surveillance and constant suspicion in society creating potential social distrust".

Key Points

- **About the Cyber Crime Volunteers Concept:**
  - **Indian Cyber Crime Coordination Centre (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 the fight against **cybercrime** in the country.
    - The programme **targets to rope in around 500 persons** to flag unlawful content on the Internet.
  - **Good Samaritans** are welcomed to register as Cyber Crime Volunteers in the role of unlawful content flaggers for facilitating law enforcement agencies in identifying, reporting and removal of illegal/unlawful online content.
  - Volunteers have been advised to study **Article 19** of the Indian Constitution, which deals with freedom of expression.
  - Further, the volunteer shall "maintain strict confidentiality of tasks assigned/carried out by him/her". The **State Nodal Officer of States/UTs** also reserves the **right to take legal action against the Volunteer,** in case of violation of terms and conditions of the Program.

- **Unlawful Content:** In general, content that violates any law in force in India. Such content may fall under following broad categories:
    - Against sovereignty and integrity of India.
    - Against defence of India.
    - Against Security of the State.
    - Against friendly relations with foreign States.
    - Content aimed at disturbing Public Order.
    - Disturbing communal harmony.
    - Child Sex Abuse material.
- **Concerns Raised:**
    - **Chances of Misuse:** There is no information available on how the Ministry will ensure that the program is not misused by certain elements to extract misguided personal or political vendettas.
        There is **no process in place for withdrawal of complaints** once submitted.
    - **Cyber-Vigilantism:** The programme will **essentially result in a similar situation to the one which East Germany was in the 1950s.**
        The state asking citizens to report their fellow citizens would lead to cyber-vigilantism, and would lead to peers turning against their peers to snitch on them.
    - **No Clear Definition:** The Ministry has failed to clearly define unlawful content and content which would relate to "anti-national" activities.
        - This could **allow the volunteers to exercise far more discretion than is necessary** and report on citizens who are well within their rights to post content which is critical of the State.
        - Such a program seems to be in direct violation of the decision of the Supreme Court in ***Shreya Singhal v Union of India*** (2013) which highlights the need to ensure that overbroad restrictions on online speech are not used as a tool by the State to criminalise free speech on the internet.

Indian Cyber Crime Coordination Centre

- It has been established under the **Ministry of Home affairs (MHA)** to act as a **nodal point at National level** in the fight against cybercrime.
    - The scheme to set up I4C was approved in October 2018, to deal with all types of cybercrimes in a comprehensive and coordinated manner.
    - This state-of-the-art Centre is located in **New Delhi.**
    - Various States and Union Territories have given their consent to set up Regional Cyber Crime Coordination Centres.

- **Seven Components of the Scheme:**
  - National Cyber Crime Threat Analytics Unit,
  - National Cyber Crime Reporting Portal,
  - National Cyber Crime Training Centre,
  - Cyber Crime Ecosystem Management Unit,
  - National Cyber Crime Research and Innovation Centre,
  - National Cyber Crime Forensic Laboratory Ecosystem and
  - Platform for Joint Cyber Crime Investigation Team.
- **Objectives:**
  - To provide a **platform to deal with cybercrimes** in a coordinated and comprehensive manner.
    - 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.
  - To **create an ecosystem** that brings together academia, industry, public and government in prevention, detection, investigation and prosecution of cybercrimes.
    - 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.
  - 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.

Source: TH