EXPANDING HORIZON OF SURVEILLANCE

(GS-3: Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges.)

Context:

- The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs (MHA), launched the Cyber Crime Volunteers Programme.
- Aim is to allow citizens to register themselves as "Cyber Crime Volunteers" in the role of "Unlawful Content Flaggers".
- As per the **National Cyber Crime Reporting Portal**, the programme will help law enforcement agencies in identifying, reporting and in the removal of illegal/unlawful online content.

AbouttheCyber Crime Volunteers Programme:

- The volunteer programme is supposed to act as a facilitativetool between ordinary citizens and the government for the prevention of cybercrime.
- Any citizen can register himself/herself under one of three categories: 'Cyber Volunteer Unlawful Content Flagger', 'Cyber Awareness Promoter', and 'Cyber Expert'.
- Post-registration, the individual can directly report "unlawful content" being circulated over the Internet, which presumably includes social media platforms like Facebook, Instagram and Twitter, among others.

What is 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

Overview about the I4C (Indian Cyber Crime Coordination Centre) scheme:

- Act as a nodal point in the fight against cybercrime
- Identify the research problems/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 cyber space 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 implementation of Mutual Legal Assistance Treaties (MLAT) with other countries related to cybercrimes in consultation with the concerned nodal authority in MHA
- I4Chas seven components viz., 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.

Lateral vs. vertical surveillance:

- Lateral or social or peer-to-peer surveillance differs from typical surveillance.
- Surveillance, which enables citizens to “watch over” one another is called lateral surveillance.
- The conventional understanding of the term, surveillance, is its use in the hierarchical sense, i.e. the vertical relationship between the person watching and the person being watched, which is usually the state and its citizenry.
- While surveillance of any kind shows an imbalance of power between the person who surveils, and the one under surveillance, lateral surveillance specifically ensures that the imbalance of power no longer exists.
- Informal watching of communities by their members has been an age-old part of society, and its members view it as a harmless activity.
- The problem arises when it is organised and state-sponsored.

Examples of lateral surveillance:

- In the 1970s, the United States had the neighborhood watch schemes which increased community policing.

- With the introduction of technology and development of applications such as Citizen and Next door, monitoring of people and their behaviour has become easier.
- Further, government and private sector institutions alike collect swathes of data for supposedly 'public functions'.
- Specifically in the sphere of crime prevention, much like the cyber crime prevention programme, there has been a transition in the outlook from a 'punishing state' to a 'preventive state'.
- **Extent of surveillance in India:**

- This is not the first time state-sponsored lateral surveillance has been implemented in India.
- For example, the C-Plan App in Uttar Pradesh launched for keeping a tab on anti-social elements, is designed to receive inputs from certain identified individuals in villages across the State.
- These individuals have been given the responsibility to solve local problems such as providing information about simmering communal tensions or land disputes taking place in their respective villages through the mobile application.
- The scope of lateral surveillance was greatly expanded during the pandemic lockdown, both with and without the introduction of technology.
- The Karnataka government released a PDF with the names and addresses of around 19,000 international passengers who were quarantined in Bengaluru.
- While in the North, a woman was harassed and boycotted by her neighbours after the Delhi government marked her house with a quarantine sticker.

Lateral surveillance as a tool for social exclusion and suspicion:

- lateral surveillance is used to further emotional objectives such as community building and strengthening relationships with neighbours where emotional and social factors act as a driving force
- Thus it creates a situation where privacy may be undermined for the betterment of the community.
- However, surveillance technologies not only act as a tool for social control but also as a tool for social exclusion.
- Lateral surveillance thus makes it easier to discriminate between those who conform to the social norms of the majority.
- For example, the LGBT community in South Korea came under the scanner after a cluster of novel coronavirus cases were reported from a particular area which had resulted in large-scale circulation of homophobic content and comments against the patients who tested positive from the community.
- This not only made it difficult for authorities to collect information but also increased troubles for the people belonging to the sexual minority in getting themselves tested.

- State-sponsored lateral surveillance is harmful as it creates a culture of 'hate', 'fear' and 'constant suspicion' against an 'enemy'.
- Wherever the state identifies that it "cannot be everywhere", it deploys this mechanism.
- This culture places a duty on people to 'keep an eye out' for 'their own safety' and this heightens the fear of crime in society.
- Such perceived threats have a tendency to increase intolerance, prejudice, xenophobia and casteism in our society
- It also violates the fundamental right to privacy, and, consequently, the unfettered expression of free speech and behavior

Surveillance as apolicy:

- Despite the controversy, the government recently notified the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.**
- New Rules intended to expand "due diligence" obligations by intermediaries.
- This not only substantially increases surveillance but also promotes lateral surveillance.
- For example provisions pertaining to user directed take downs of non-consensual sexually explicit content or 'any other matters' and even the harsh content take down/data sharing timelines will enable intermediaries to remove or disable access to information within a short period of time of being notified by users, circumventing the "actual knowledge" doctrine given in *ShreyaSinghalvs Union of India*.
- This will further create an incentive to take down content and share user data without sufficient due process safeguards, violating the fundamental right to privacy and freedom of expression.

Conclusion:

- The right to Internet access, which has been declared as a fundamental right by the apex court, often gets infringed as a result of internet shutdowns across various corners of the country.
- Social media platforms which become an effective forum for mobilisation, dissemination of views, asserting individual autonomy and freedom of speech and expression enabled by the access to the internet
- Thus Volunteer Programmeand recently notified the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,**needs to be evaluated in the larger socio-political context of the day.