Cyber Security: Cybercrime Volunteers Programme

March 4, 2021

'Cyber Crime Volunteers Programme' is an initiative aimed at inviting ordinary citizens to sign up as volunteers who would help identify the circulation of digital "unlawful content". While cybercrime experts have highlighted potential problems with such a move, it is also important to assess the cybercrime scenario in detail.

In news: Cyber crime volunteers plan fraught with dangers: Internet Freedom Foundation
Placing it in syllabus: Internal Security
Dimensions

- Cyber crimes and Types
- Objectives of the Programme: Advantage and Problems
- Policy Framework – Cyber Security Policy 2013
- Legislative Framework
- Recent Initiatives
- International Measures: Budapest Convention

Content:

Cyber crimes and Types:

- When any crime is committed over the Internet it is referred to as a cyber crime.
- In general cybercrime may be defined as "Any **unlawful act** where **computer** or communication device or computer network **is used to commit or facilitate the commission of crime**"
- These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium.

- Because of the **anonymous nature of the Internet**, it is possible to engage into a variety of criminal activities with impunity.

There are many types of cyber crimes and the most common ones are explained below:

Hacking:

- This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.
- In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Cyber Theft:

- This crime occurs when a person violates copyrights and downloads music, movies, games and software.
- There are even peer sharing websites which encourage software piracy.
- Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

Cyber Stalking:

- This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.
- offline stalking along with cyber stalking to make the victims' lives more miserable.

Identity Theft:

- This has become a major problem with people using the Internet for cash transactions and banking services.
- In this cyber crime, a criminal accesses data about a

person’s bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim’s name.
- It can result in major financial losses for the victim and even spoil the victim’s credit history.

Malicious Software:

- These are Internet-based software or programs that are used to disrupt a network.
- The software is used to gain access to a system to steal sensitive information or data or cause damage to software present in the system.

Child soliciting and Abuse:

- This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

Cyber Terrorism

- It enables terrorists to co-operate with each other via the internet to plan a terrorist attack.
- The other form of cyber terrorism is when a hacker attacks the website of any government agency.

Spam

- In this crime, some companies send unwanted Emails to advertise their products or services.
- Normally, companies abuse the privacy of the victim by sending emails without their permission.

Cyber Bullying

- It is a type of harassment through internet mostly to the teenagers which sometimes results in suicide.

Objectives of the Programme: Advantage and Problems

- **The Ministry of Home Affairs' (MHA)** controversial cyber crime volunteers programme targets to rope in around 500 persons to flag unlawful content on the Internet for "improvement in the cybercrime ecosystem of India".
- The programme will include 200 "cyber awareness promoters" and 50 "cyber experts", according to the output outcome monitoring framework of the MHA's budget 2021-22.
- **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.
- Good Samaritans have 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.
- Individuals who are willing to volunteer in any other area that can help in fighting cybercrime.

The programmes states that the following types of content would be considered as unlawful content:

- 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

Advantages

- According to the government, the general public's aid will help law enforcement agencies spot, report, and remove illegal/unlawful content from online platforms effectively.

Problems

The Internet Freedom Foundation has raised several concerns about the initiative:

- ***Lack of underlying legal framework***
- The Program has been launched without establishing any underlying legal framework or Standard Operating Procedure (SOP) to regulate its functioning or the action of volunteers involved in it.
- Without clear guidelines and defining parameters, there is always a possibility of misuse of this platform.
- ***Vague Definitions***
- The official website provides little insight into what constitutes unlawful content.
- There are no fixed criteria as to what counts or doesn't count as hurting the sovereignty and integrity of India.
- This creates chances of overzealous and overbroad restrictions being put onto the freedom of speech online.
- ***Chances for lateral surveillance and cyber vigilantism***
- Without an underlying legal framework or rules, this experiment could promote a culture of surveillance and constant suspicion in society, further leading to social distrust.
- Also cyber-vigilantism creates chaos and life-threatening situations for victims instead of solving the issue.
- ***Authenticity of complaints***
- There is no clarity on how the authenticity of the complaints filed by volunteers will be ensured.
- I4C has not provided any information on how MHA will make sure that people do not misuse this platform to exact their misguided personal/political vendettas.
- Moreover, there is no process in place for the withdrawal of complaints once submitted.
- ***No prior KYC required to flag any content***

- Anyone can become a “Cyber Volunteer Unlawful Content Flagger” without prior verification (KYC).
- Since no verification is required and the nature of the position is voluntary, it exempts the I4C and the MHA of any liability or guilt in cases of misuse.

Policy Framework – National Cyber Security Policy 2013:

- National Cyber Security Policy is a policy framework by **Department of Electronics and Information Technology (DeitY)**
- It aims at protecting the public and private infrastructure from cyber attacks.
- The policy also intends to safeguard “information, such as personal information (of web users), financial and banking information and sovereign data”.
- Its vision is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

Legislative Framework:

IT Act 2000

- The Information Technology Act, 2000 provides a **legal framework for electronic governance** by giving recognition to electronic records and digital signatures.
- It also defines cyber crimes and prescribes penalties for them.
- The Act directed the **formation of a Controller of Certifying Authorities** to regulate the issuance of digital signatures.
- It also established a **Cyber Appellate Tribunal** to

resolve disputes rising from this new law.
- The Act also amended various sections of the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies.

Personal Data Protection Bill, 2019

The Personal Data Protection Bill 2019 (PDP Bill 2019) is being analyzed by a **Joint Parliamentary Committee (JPC)** in consultation with experts and stakeholders.

The Bill aims to:

- to **provide for protection of the privacy of individuals** relating to their personal data,
- specify the flow and usage of personal data,
- create a relationship of trust between persons and entities processing the personal data,
- protect the fundamental rights of individuals whose personal data are processed,
- to create a framework for organisational and technical measures in processing of data,
- laying down norms for social media intermediary,
- cross-border transfer, accountability of entities processing personal data,
- remedies for unauthorised and harmful processing, and
- to establish a **Data Protection Authority of India** for the said purposes and for matters connected therewith or incidental thereto.

Recent Initiatives:

Indian Cyber Crime Coordination Centre (I4C)

- 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.

The scheme has the following seven components:

- National Cybercrime Threat Analytics Unit (TAU)
- National Cyber crime Reporting
- Platform for Joint Cyber crime Investigation Team
- National Cyber crime Forensic Laboratory (NCFL) Ecosystem
- National Cyber crime Training Centre (NCTC)
- Cybercrime Ecosystem Management Unit
- National Cyber Research and Innovation Centre

Cyber Swachta Kendra:

- It is a **Botnet Cleaning and Malware Analysis Centre (BCMAC)**, operated by the **Indian Computer Emergency Response Team (CERT-In)** as part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY).
- Its goal is to **create a secure cyberspace by detecting botnet infections in India** and to notify, enable cleaning and securing systems of end users so as to prevent further infections.
- It is **set up in accordance with the objectives of the National Cyber Security Policy 2013**
- This centre operates in close coordination and

collaboration with Internet Service Providers and Product/Antivirus companies.

CERT-In

- The Indian Computer Emergency Response Team (CERT-In) is a **functional organisation within the Ministry of Electronics and Information Technology.**
- It is the **nodal agency to deal with cyber security threats** like hacking and phishing. It strengthens security-related defence of the Indian Internet domain.

National Cyber Crime Reporting Portal

- This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online.
- This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children.
- Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints.

International Measures: Budapest Convention:

- The Convention on Cybercrime is also known as the Budapest Convention on Cybercrime or the Budapest Convention.
- It is the **first international treaty seeking to address Internet and computer crime** (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations
- It is the **first multilateral legally binding instrument** to regulate cybercrime, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security.
- It also **contains a series of powers and procedures** such

as the search of computer networks and lawful interception.

- Since it entered into force, important countries like Brazil and India have declined to adopt the Convention on the grounds that they did not participate in its drafting.
- Russia opposes the Convention, stating that adoption would violate Russian sovereignty, and has usually refused to cooperate in law enforcement investigations relating to cybercrime.
- Since 2018, India has been reconsidering its stand on the Convention after a surge in cybercrime, though concerns about sharing data with foreign agencies remain

Mould your thought: What are cybercrimes? Discuss the recent initiatives of Indian government to tackle the issue.

Approach to the answer:

- Introduction
- Define Cybercrime
- Discuss the different types briefly
- Write about recent initiatives
- Conclusion