drishti

Rising Cybercrimes

drishtiias.com/printpdf/rising-cybercrimes

Why in News

The **Ministry of Home Affairs (MHA)** has written to all States to examine and register First Information Reports (FIRs) based on the complaints received on **National Cybercrime Reporting Portal (www.cybercrime.gov.in).**

Key Points

- **Low Conversion Rates:** As per Ministry of Home Affairs, only 2.5% of total complaints registered on the portal are converted into FIRs.
- **Cyber Crime Volunteers:** Through the portal, the Government seeks to promote Cyber Crime Volunteers for identifying, reporting and removal of illegal/unlawful online content.
- **Increase in Cases:** According to the **National Crime Records Bureau (NCRB)**, the number of registered cyber crimes increased by 63.5% in the year 2019 compared to 2018.
- **Benefits:**
  - Help in curbing rising cyber frauds ,cyber bullying,child pornography etc.
  - In consonance with the Digital India drive of the government as with rising digital footprint cyber crimes are bound to rise.
  - Massive Digitalisation in the post-covid world in the sectors of education , health etc highlights the importance of cyber governance initiatives such as this.

National Cyber Crime Reporting Portal

- Launched in 2019, it is a citizen-centric initiative enabling citizens to report cybercrimes online.
- The portal specifically focuses on crimes against women, children, particularly child pornography, child sex abuse material, online content pertaining to rapes/gang rapes, etc.

- It also focuses on crimes like financial crime and social media related crimes like stalking, cyberbullying, etc.
- It will improve the capacity of law enforcement agencies to investigate the cases after successful completion by improving coordination amongst the law enforcement agencies of different States, districts and police stations.

Budapest Convention

- The **Council of Europe's (CoE) Cybercrime Convention, also known as the Budapest Convention** is the **sole legally binding international multilateral treaty** on cybercrime. It coordinates cybercrime investigations between nation-states and criminalizes certain cybercrime conduct.
- It was open for signature in 2001 and **came into force in 2004.**
- The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.
- India is **not a party** to it. India recently **voted in favour of a Russian-led UN resolution** to set up a separate convention. The resolution seeks to set up new cyber norms considered as a **counter alternative to the US backed Budapest Accord.**

Recent Initiatives to Tackle Cybercrime

- **Indian Cyber Crime Coordination Centre (I4C):** The **I4C will assist in centralising cyber security investigations**, prioritise the development of response tools and bring together private companies to contain the menace.
- **Draft Personal Data Protection Bill, 2018** (based on the recommendation of Justice BN Srikrishna Committee) to secure citizens data.
- **Cyber Swachhta Kendra:** The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's **Digital India initiative** under the Ministry of Electronics and Information Technology (MeitY).
- **Indian Computer Emergency Response Team (CERT-IN):** It is an organisation of the Ministry of Electronics and Information Technology, Government of India, with the objective of securing Indian cyberspace. It is the nodal agency which deals with cybersecurity threats like hacking and phishing.

Source :TH