AI-ENABLED CYBER CRIME PREVENTION AND DIGITAL IDENTITY PROTECTION

प्रविष्टि तिथि: 12 AUG 2026 4:50PM by PIB Delhi

'Police' and 'Public Order' are State subjects under the Seventh Schedule to the Constitution of India. Accordingly, the States and Union Territories (UTs) are primarily responsible for the prevention, detection, investigation, and prosecution of cybercrime. The Central Government, through the Ministry of Home Affairs (MHA), supplements the efforts of States and UTs by providing policy guidance, technological support, capacity-building assistance, and financial resources to strengthen cybercrime management and enforcement capabilities.

To strengthen the mechanism to deal with cyber crimes including AI-enabled cyber crimes in a comprehensive and coordinated manner and to strengthen cyber resilience, the Central Government has taken steps which, inter-alia, include the following:

i. **The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.**
ii. **The 'National Cyber Crime Reporting Portal' (NCRP) (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children.**
iii. **The 'Citizen Financial Cyber Fraud Reporting and Management System' (CFCFRMS), under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. As per CFCFRMS operated by I4C, till 30.06.2026, financial amount of more than Rs. 11,158 Crore has been saved in more than 32.80 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.**
iv. **The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. Till 30.06.2026, more than 1,63,344 police officers/judicial officers from States/UTs are registered and more than 1,61,957 Certificates issued through the portal.**
v. **Cyber Commando programme was launched by the Hon'ble Home Minister to establish a Special Wing of Cyber Commandos equipped with specialized training to counter cybersecurity threats in the country. The programme envisions the creation of a dedicated, skilled workforce capable of securing critical information infrastructure and supporting national cybersecurity efforts. 281 cyber commandos successfully completed training.**

vi. **I4C, MHA is regularly organising 'State Connect', 'Thana Connect' 'Bank Connect' and Peer learning session to share best practices, enhance capacity building, etc.**

vii. **A State of the Art, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.**

viii. **Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by onboarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs.**

ix. **A Suspect Registry of identifiers of cyber criminals has been launched by I4C in collaboration with Banks/Financial Institutions. Till 30.06.2026, more than 30.48 lakh suspect identifier data received from Banks and 32.08 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 25,698 crores.**

x. **Samanvaya Platform has been made operational to serve as an Management Information System (MIS) platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics based interstate linkages of crimes and criminals, involved in cybercrime complaints in various States/UTs. The module 'Pratibimb' maps locations of criminals and crime infrastructure on a map to give visibility to jurisdictional officers. The module also facilitates seeking and receiving of techno-legal assistance by Law Enforcement Agencies from I4C and other SMEs. It has lead to arrest of more than 29,837 accused and more than 2,33,593 Cyber Investigation assistance request.**

xi. **'Sahyog' Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act.**

xii. **The Ministry of Home Affairs has established CyMAC (Cyber Multi Agency Centre) under the MAC (Multi Agency Centre) platform on 22.01.2025 with the objective to effectively address cybersecurity**

threats, cyber espionage, misuse of emerging technologies and similar concerns against national security.

xiii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis.

xiv. National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned State Governments, organisations across sectors, and stakeholder agencies for taking action.

xv. AI driven situational awareness systems are deployed by CERT-In to detect malicious domains and phishing activities for necessary mitigation.

xvi. CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with State Governments and organisations across sectors for proactive threat mitigation actions by them.

xvii. Cyber Swachhta Kendra (CSK) is a service provided by CERT-In, which extends the vision of Swachh Bharat to the cyber space. Cyber Swachhta Kendra helps to detect malicious

programs and vulnerable

services and provide remedial measures to organisations across States and sectors.

xviii. CERT-In has empanelled 237 security auditing organizations to support and audit implementation of information security best practices.

xix. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government (Central & States) and critical sectors. Workshops along with these drills are conducted in States for facilitating coordination and information sharing in the area of cyber security.

xx. To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; caller tune campaign, dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (CyberDostI4C), Telegram(cyberdosti4c), SMS campaign, TV campaign, Radio campaign, School Campaign, advertisement in cinema halls, celebrity endorsement, IPL campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, digital displays on metro stations, railway stations and airports across, etc.

This was stated by the Minister of State in the Ministry of Home Affairs Shri Bandi Sanjay Kumar in a written reply to a question in the the Rajya Sabha.

*****

RK/RR/PR/PS/SKS

(रिलीज़ आईडी: 2298336) आगंतुक पटल : 800