GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 350

TO BE ANSWERED ON THE 22ND JULY, 2025/ ASHADHA 31, 1947 (SAKA)

INDIAN CYBER CRIME COORDINATION CENTRE

†350. SHRI SATISH KUMAR GAUTAM:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether Indian Cyber Crime Coordination Centre was setup to coordinate cyber crimes;

(b) the objectives and functions of the Indian Cyber Crime Coordination Centre and whether it is effective in tackling cyber crimes; and

(c) the other measures taken by the Government to deal with all types of cyber crimes in a comprehensive and coordinated manner?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI BANDI SANJAY KUMAR)

(a) to (c): 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber crime through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

To strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, 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. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.

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, financial amount of more than Rs. 5,489Crore has been saved in more than 17.82lakh complaints

so far. A toll-free Helpline number ‘1930’ has been operationalized to get assistance in lodging online cyber complaints.

iv. **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.**

v. **So far, more than 9.42 lakhs SIM cards and 2,63,348 IMEIs as reported by Police authorities have been blocked by Government of India.**

vi. **‘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.**

vii. **A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. So far, more than 11 lakh suspect identifier data received from Banks and 24 lakh Layer 1 mule accounts have been shared with**

the participating entities of Suspect Registry and saved more than Rs. 4631 crores.

viii. 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 10,599accused, 26,096 linkages and 63,019 Cyber Investigation assistance request.

ix. To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; 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, campaign during Kumbh Mela 2025, Mann Ki Baat, caller tune, engaged MyGov for publicity in multiple mediums,

organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, newspaper advertisement on digital arrest scam, announcement in Delhi metros on digital arrest and other modus operandi of cyber criminals, use of social media influencers to create special posts on digital arrest, digital displays on railway stations and airports across, etc.

x. The Central Government and Telecom Service Providers (TSPs) have devised a system to identify and block incoming international spoofed calls displaying Indian mobile numbers appear to be originating within India.

xi. The Central Government has launched Sanchar Saathi portal (www.sancharsaathi.gov.in) to empower mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives of the Government. The portal provides, inter-alia, facilities to citizens to report suspected fraud communications, know the mobile connections issued in their name and report the mobile connections for disconnection which are either not required or not taken by them, report the stolen / lost mobile handset for blocking and tracing, check the genuineness of mobile handset, report the incoming international

calls received with Indian telephone number as calling line identification.

xii. The Central Government has launched an online Digital Intelligence Platform (DIP) for sharing of telecom misuse related information with the concerned stakeholders for prevention of cyber-crime and financial frauds.

*****