GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 399

TO BE ANSWERED ON THE 23RD JULY, 2025/ SRAVANA 1, 1947 (SAKA)

STRATEGY TO CONTROL CYBER CRIMES IN THE COUNTRY

399 # SHRI MADAN RATHORE:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether incidents of cyber crime are rapidly increasing in the country;

(b) whether Government has implemented any permanent system like Cyber Fraud Mitigation Centre (CFMC);

(c) whether guidelines have been issued to States for technical assistance and training; and

(d) whether Government is coordinating with social media platforms for this issue?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS

(SHRI BANDI SANJAY KUMAR)

(a) to (d): '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. 5,489 Crore has been saved in more than 17.82 lakh 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. The Ministry of Home Affairs has provided financial assistance under the 'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs' personnel, public prosecutors and judicial officers. Cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs and more than 24,600 LEA personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc.

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

viii. The state of the art 'National Cyber Forensic Laboratory (Investigation)' has been established, as a part of the I4C, at New Delhi to provide early

stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) has provided its services to State/UT LEAs in around 12,460 cases pertaining to cyber crimes.

ix. 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. More than 1,05,796 Police Officers from States/UTs are registered and more than 82,704 Certificates issued through the portal.

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 10,599 accused, 26,096 linkages and 63,019 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. So far, 9 Central and 34 State/UT Authorised Agencies, 72 IT Intermediaries and 35 Virtual Asset Service Providers (VASPs) have been onboarded on Sahyog Portal.

*****