GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2610

TO BE ANSWERED ON THE 5TH AUGUST, 2025/ SARVANA 14, 1947 (SAKA)

MODERNISE CYBER CRIME INFRASTRUCTURE IN CAPF

†2610. SHRI DAMODAR AGRAWAL:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the details of initiatives taken to modernise forensic and Cyber Crime Infrastructure of Central Armed Police Forces (CAPF);

(b) the details of the infrastructure set up under Indian Cyber Crime Coordination Centre and its associated cyber fraud prevention centres;

(c) the number of districts in the country where mobile forensic labs have been deployed so far and the manner by which these labs are helping in crime investigations; and

(d) the current status of integration of police, judiciary, prison, forensic and prosecution systems under the criminal justice system and the major achievements in the field of digitisation of criminal justice processes?

ANSWER

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

(a) and (b): '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. Strengthening of forensic and cybercrime investigation capabilities is an ongoing process, undertaken as per requirements, for various law enforcement agencies, including CAPFs.

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.

xii. The Central Government has taken various initiatives to create cyber crime awareness which, inter-alia, include:-

1) The Hon'ble Prime Minister spoke about digital arrests during the episode "Mann Ki Baat" on 27.10.2024 and apprised the citizens of India.

2) A special programme was organized by Akashvani, New Delhi on Digital Arrest on 28.10.2024.

3) Caller Tune Campaign: I4C in collaboration with the Department of Telecommunications (DoT) has launched a caller tune campaign

with effect from 19.12.2024 for raising awareness about cybercrime and promoting the Cybercrime Helpline Number 1930 & NCRP portal. The caller tunes were also being broadcast in English, Hindi and 10 regional languages by Telecom Service Providers (TSPs). Six versions of caller tunes were played which cover various modus-operandi, namely, Digital Arrest, Investment Scam, Malware, Fake Loan App, Fake Social Media Advertisements.

4) The Central Government has launched a comprehensive awareness programme on digital arrest scams which, inter-alia, include; newspaper advertisement, announcement in Delhi Metros, use of social media influencers to create special posts, campaign through Prasar Bharti and electronic media and participated in Raahgiri Function at Connaught Place, New Delhi on 27.10.2024.

5) To further 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, 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, digital displays on railway stations and airports etc.

(c): As per the available information, there are 605 District Mobile Units/labs in the country, these labs facilitates on-site examination and preservation of evidence, which aid the investigation process.

(d): ICJS is facilitating the integration of the stand-alone IT systems (Crime and Criminal Tracking Network and Systems, eForensics, eProsecution, eCourts and ePrisons) towards seamless transfer of information between the pillars, to enhance data quality by reducing errors in data entry, increase effectiveness and timeliness in investigations, enable effective use of data analytics.

As on June 2025, CCTNS has been implemented in 17,712 police stations, eForensics in 117 forensic science laboratories, eProsecution in 751 prosecution districts, eCourts in 3,637 court complexes, and ePrisons in 1,373 prisons across all the States/UTs.

As per the Pragati Dashboard Report of 01.06.2025, the forward integration of CCTNS pillar with e-Prison, e-Prosecution, e-Forensics and e-Courts are completed in 32, 28, 32 and 35 States/UTs respectively, and vice-versa, backward integration from pillar applications viz., e-Prison, e-Prosecution, e-Forensics and e-Courts to CCTNS is completed in 30, 26, 30 and 31 States/UTs respectively.

****