

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**LOK SABHA
UNSTARRED QUESTION NO. 1560**

**TO BE ANSWERED ON THE 9TH DECEMBER, 2025/ AGRAHAYANA 18, 1947
(SAKA)**

STRATEGY TO CURB CYBER CRIMES

†1560. SMT. DELKAR KALABEN MOHANBHAI:

Will the Minister of HOME AFFAIRS be pleased to state:

- (a) whether the Government has formulated any strategy to curb cyber crimes;**
- (b) if so, the details thereof in respect of the Union Territory of Dadra & Nagar Haveli;**
- (c) whether any policy has been formulated for quick action in case of cyber crime;**
- (d) the steps taken by the Government to enhance the capacity building of police/investigation agencies across the country to deal with the increasing cyber crimes; and**
- (e) if so, the details thereof?**

ANSWER

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

(a) to (e): ‘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 in the country including Union Territory of Dadra & Nagar Haveli 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. So far, financial amount of more than Rs. 7,130 Crore has been saved in more than 23.02 lakh complaints. 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. I4C, MHA is regularly organising 'State Connect', 'Thana Connect' and Peer learning session to share best practices, enhance capacity building, etc.**
- vi. The state of the art 'National Cyber Forensic Laboratory (Investigation)' has been established, as a part of the I4C, at New Delhi (on 18.02.2019) and at Assam (on 29.08.2025) to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation), New Delhi has provided its services to State/UT LEAs in around 12,952 cases pertaining to cyber crimes.**

- vii. 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 1,44,895 police officers/judicial officers from States/UTs are registered and more than 1,19,628 Certificates issued through the portal.**
- viii. Cyber Commando programme was launched by the Hon'ble Home Minister on 10.09.2024 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. So far, 281 cyber commandos successfully completed their training at premier institutions including IITs, IIITs, Rashtriya Raksha University (RRU), National Forensic Sciences University (NFSU) Gandhinagar & New Delhi, etc.**
- ix. 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.

- x. '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.**
- xi. 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 18.43 lakh suspect identifier data received from Banks and 24.67 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 8031.56 crores.**
- xii. 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 16,840 accused and 1,05,129 Cyber Investigation assistance request.

xiii. 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 Aakashvani, 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, special programme on Aakashvani.**
- 5) In partnership with DD News, I4C conducted a cybercrime awareness campaign running through Weekly Show Cyber-Alert starting from 19th July 2025 for 52 Weeks.**
- 6) 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& Suraj Kund 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 across, etc.

*** * * * ***