GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 1029

TO BE ANSWERED ON THE 31ST JULY, 2024/ SRAVANA 9, 1946 (SAKA)

PLANS TO CURTAIL CYBER CRIMES

1029. SHRI SHAKTISINH GOHIL:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the details of cities and places identified by police and agencies which are notorious for cyber crime;

(b) the number of criminals who are engaged in cyber crime, State-wise;

(c) the action taken against such cyber criminals; and

(d) the details of nation wide plan to curtail cyber crimes?

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 crimes through their Law Enforcement Agencies. The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

Cyber crime is a daunting challenge. Due to its vast and borderless nature, a cyber criminal can commit crime while sitting anywhere. On the basis of suspect mobile numbers reported by citizens on National Cyber Crime Reporting Portal, during the period 1st January 2024 to 22nd July 2024, the major cities and places of origination of cybercrime in the country are Deeg (Rajasthan), Deoghar (Jharkhand), Nuh (Haryana), Alwar (Rajasthan), Nawada (Bihar), West Delhi (Delhi), Nalanda (Bihar), Jamtara (Jharkhand), Mathura (Uttar Pradesh), Patna (Bihar), Bengaluru Urban (Karnataka), Dumka (Jharkhand), Gautam Budh Nagar (Uttar Pradesh) , Jaipur (Rajasthan), Khertal-Tijara (Rajasthan), North 24 Parganas (West Bengal), Kolkata (West Bengal), North West Delhi (Delhi), Sheikhpura (Bihar) and South West Delhi (Delhi).

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2022. Specific data regarding criminals engaged in cyber crime is not maintained separately by NCRB.

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 crime in the country, in a coordinated and comprehensive manner.

ii. 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 on boarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh in 2023.

iii. 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 LEAs in around 10,200 cyber forensics like mobile forensics, memory forensics, CDR Analysis, etc. to help them in investigation of cases pertaining to cyber crimes.

iv. The 'National Cyber Crime Reporting Portal' (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.

v. The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, financial amount of more than Rs. 2400 Crore has been saved in more than 7.6 lakh complaints. A toll-free Helpline number '1930' has been operationalized to provide assistance in lodging online cyber complaints.

vi. 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. along with certification. More than 96,288 Police Officers from States/UTs are registered and more than 70,992 Certificates issued through the portal.

vii. Till date more than 5.8 lakhs SIM cards and 1,08,000 IMEIs as reported by Police authorities have been blocked by Government of India.

viii. I4C has imparted cyber hygiene training to 6,800 officials of various Ministries/ Departments of Government of India.

ix. I4C has imparted cyber hygiene training to more than 35,000 NCC cadets.

x. The Ministry of Home Affairs has provided financial assistance to the tune of Rs. 131.60 crores 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.

xi. National Cyber Forensic Laboratory (Evidence) has been set up at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber crime,

preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and reduced turnaround time.

xii. 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), Radio campaign, 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, etc. The States/UTs have also been requested to carry out publicity to create mass awareness.

*****