TO BE ANSWERED ON THE 7TH FEBRUARY 2024/ MAGHA 18, 1945 (SAKA)

INCREASE IN CYBER CRIMES

548. SHRI A. D. SINGH:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether cyber crimes have been increasing continuously in the country for the last few years;

(b) if so, the details of reported cyber crimes during the last three years;

(c) the reasons for continuous increase in the cyber crimes; and

(d) what efforts are being made to check these crimes and strengthen the cyber security?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI AJAY KUMAR MISHRA)

(a) to (d): 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. As per the data published by the NCRB, State/UT-wise details of cases registered under cyber crimes (involving communication devices as medium/target) for last three years are at the Annexure.

The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their Law Enforcement Agencies (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) 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. 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) have provided its services to State LEAs in around 9,000 cyber forensics like mobile forensics, memory forensics, Call Data Record (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, an amount of more than Rs. 1200 Crore have been saved in more than 4.7 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get 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 76,000 Police Officers from States/UTs are registered and more than 53,000 Certificates issued through the portal.

vii. Till date more than 3.2 lakhs SIM cards and 49,000 IMEIs as reported by Police authorities have been blocked by Government of India.

viii. I4C has imparted cyber hygiene training to 6,000 officials of various Ministries/ Departments of Government of India.

ix. I4C has imparted cyber hygiene training to more than 23,000 NCC cadets.

x. The Ministry of Home Affairs has provided financial assistance to the tune of Rs. 122.24 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. So far, cyber forensic-cum-training laboratories have been commissioned in 33

States/UTs. So far, 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.

xiii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.

xiv. **CERT-In, through RBI, has advised all authorised entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-empanelled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.**

xv. **CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.**

*****

State/UT-wise details of cases registered under cyber crimes (involving communication devices as medium/target) for last three years

Sl. no	State/UT	2020	2021	2022
1	Andhra Pradesh	1899	1875	2341
2	Arunachal Pradesh	30	47	14
3	Assam	3530	4846	1733
4	Bihar	1512	1413	1621
5	Chhattisgarh	297	352	439
6	Goa	40	36	90
7	Gujarat	1283	1536	1417
8	Haryana	656	622	681
9	Himachal Pradesh	98	70	77
10	Jharkhand	1204	953	967
11	Karnataka	10741	8136	12556
12	Kerala	426	626	773
13	Madhya Pradesh	699	589	826
14	Maharashtra	5496	5562	8249
15	Manipur	79	67	18
16	Meghalaya	142	107	75
17	Mizoram	13	30	1
18	Nagaland #	8	8	4
19	Odisha	1931	2037	1983
20	Punjab	378	551	697
21	Rajasthan	1354	1504	1833
22	Sikkim	0	0	26
23	Tamil Nadu	782	1076	2082
24	Telangana	5024	10303	15297
25	Tripura	34	24	30
26	Uttar Pradesh	11097	8829	10117
27	Uttarakhand	243	718	559
28	West Bengal	712	513	401
	TOTAL STATE(S)	**49708**	**52430**	**64907**
29	A&N Islands	5	8	28
30	Chandigarh	17	15	27
31	D&N Haveli and Daman & Diu	3	5	5
32	Delhi	168	356	685
33	Jammu & Kashmir	120	154	173
34	Ladakh	1	5	3
35	Lakshadweep	3	1	1
36	Puducherry	10	0	64
	TOTAL UT(S)	**327**	**544**	**986**
	TOTAL (ALL INDIA)	**50035**	**52974**	**65893**

Source: Crime in India published by NCRB.
Clarifications are pending from Nagaland for the year 2022