GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
STARRED QUESTION NO. *204

TO BE ANSWERED ON THE 10TH DECEMBER, 2024/ AGRAHAYANA 19, 1946 (SAKA)

PREVENTION OF CYBER ATTACKS AND CYBER CRIMES

***204. SHRI ESWARASAMY K:**

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Union Government is considering to contain cyber attacks, hacking and many other computer based crimes with the help of other countries;

(b) if so, the details thereof along with the steps taken or proposed to be taken against cyber crime in the country; and

(c) whether the Government plans to train the police personnel in the country with the help of any security agencies and if so, the details thereof?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI NITYANAND RAI)

(a) to (c): A statement is laid on the Table of the House.

STATEMENT IN REPLY TO PARTS (a) to (c) OF THE LOK SABHA STARRED QUESTION NO. *204 TO BE ANSWERED ON 10.12.2024.

(a) to (c): '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).

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 Central Bureau of Investigation (CBI) participates in various regional and international cyber crime cooperation initiatives led by Interpol, fostering collaboration with global LEAs to address cross-border cyber crime challenges.**

iii. The CBI serves as the nodal point in India for data preservation requests, sending and receiving such requests through the G7 24/7 network to ensure the timely and secure exchange of cyber crime related data.

iv. The National Central Bureau (NCB) in CBI acts as a central coordination agency, facilitating the collection and dissemination of cyber crime information through Interpol channels.

v. The Indian Computer Emergency Response Team (CERT-In) is operating an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

vi. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.

vii. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

viii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 104 such drills have so far been conducted by CERT-In where around 1450 organizations from different States and sectors participated.

ix. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. A total of 32,075 officials have been trained in 103 training programs upto October 2024.

x. 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 and participated in Raahgiri Function at Connaught Place, New Delhi on 27.11.2024.

xi. I4C proactively identify and blocked more than 1700 Skype IDs and 59,000 Whatsapp accounts used for Digital Arrest.

xii. The Central Government has published a Press Release on Alert against incidents of 'Blackmail' and 'Digital Arrest' by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies.

xiii. A State of the Art Centre, 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 has led to debit freeze of 8.6 lakhs Mule accounts by various Banks and response time of banks has also decreased.

xiv. Till 15.11.2024, more than 6.69 lakhs SIM cards and 1,32,000 IMEIs as reported by Police authorities have been blocked by Government of India.

xv. 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.

xvi. The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints. So far, financial amount of more than Rs. 3431 Crore has been saved in more than 9.94 lakh complaints.

A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions which has led to declining of more than 5.6 lakhs fradulant transactions and saving more than Rs. 1400 Crore. These initiatives have saved more than 4800 Crores.

xvii. The Central Government has introduced a new feature titled as 'Report and Check Suspect' on https://cybercrime.gov.in. This facility provides citizens a search option to search I4C's repository of identifiers of cyber criminals through 'Suspect Search'.

xviii. 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.

xix. 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.

xx. 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 11,203 cases pertaining to cyber crimes.

xxi. 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 98,698 Police Officers from States/UTs are registered and more than 75,591 Certificates issued through the portal.

xxii. 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.

xxiii. 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.

xxiv. I4C has imparted cyber hygiene training to 7,330 officials of various Ministries/ Departments of Government of India.

xxv. I4C has imparted cyber hygiene training to more than 40,151 and 53,022 NCC cadets and NSS cadets respectively.

xxvi. 891 Judicial Officers, 395 Public Prosecutors, 12 Forensics Experts and 2180 LEAs have been trained by I4C in matters of cyber crime prevention, awareness, investigation forensics, etc.

xxvii. 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, digital displays on railway stations and airports across, etc.

******