GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2348

TO BE ANSWERED ON THE 03RD AUGUST, 2021/ SRAVANA 12, 1943 (SAKA)

CYBER CRIMES

2348. SADHVI PRAGYA SINGH THAKUR:
SHRI RAMESH BIDHURI:
SHRI B.B. PATIL:
SHRI SUNIL BABURAO MENDHE:
DR. NISHIKANT DUBEY:
SHRI BALUBHAU *ALIAS* SURESH NARAYAN DHANORKAR:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the cases of cyber frauds/crimes have increased during the recent period and if so, the details thereof including the number of such cases reported during each of the last three years and the reaction of the Government thereto;

(b) whether there are reports of cyber attack into systems of the companies which manage power supply and also into the system of a company which is supplying COVID-19 Vaccine across the country, if so, the details thereof along with the action taken thereon;

(c) whether the Government proposes to strengthen cyber security in tandem with Digital India, if so, the details thereof; and

(d) the challenges faced by the law enforcement agencies in investigating and apprehending the criminals in cyber frauds accross the country and the steps taken to address these challenges?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS

(SHRI AJAY KUMAR MISHRA)

(a) & (d): With the enhanced use of cyber space, the number of cyber crimes including financial frauds, is also increasing. National Crime Records Bureau (NCRB) compiles and publishes statistical data on crimes in its publication 'Crime in India'. The latest published report is for the year 2019.

As per the data published by the NCRB, the details of cases registered under cyber crimes, during 2017,2018 & 2019 are 21796, 27248 and 44546 respectively.

'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of cyber crime through their Law Enforcement Agencies (LEAs) as per provisions of law. Further, States/UTs are responsible for strengthening their cyber security apparatus/ infrastructure, and build capacity of their Law Enforcement Agencies, by imparting training to police personnel to meet the challenges in the field of cyber crime, forensics etc. The Central Government supplements the initiatives of the State Governments through advisories and financial assistance under various schemes for their capacity building.

The Central Government has taken steps for spreading awareness about cybercrimes, issuance of alerts/ advisories, capacity building of law enforcement personnel/prosecutors/judicial officers, improving cyber forensic facilities etc. The Government has established Indian Cyber Crime Coordination Centre (I4C) to provide a framework and eco-system for LEAs to deal with the cyber crimes in a comprehensive and coordinated manner. The Government has launched the National Cyber Crime Reporting Portal (www.cybercrime.gov.in), to enable public to report incidents

pertaining to all types of cyber crimes, with a special focus on cyber crimes against women and children. A toll-free number 155260 has been operationalized to get assistance in lodging online cyber complaints. Citizen Financial Cyber Fraud Reporting and Management System module has been launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters.

(b) & (c): The Indian Computer Emergency Response Team (CERT-In) is serving as national agency for responding to cyber security incidents as per provisions of Section 70B of Information Technology Act, 2000. CERT-In receives inputs from its situational awareness systems and threat intelligence sources about malware infections in networks of entities across sectors. Whenever any incident comes to the notice of CERT-In, it issues alerts and advisories to the entities concerned and sectoral Computer Emergency Response Teams (CERTs) for remedial measures.

Government has taken measures to strengthen the cyber security set-up in the country which, inter-alia, include the following:

i. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and counter measures to protect computers and networks on regular basis.

ii. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications/ infrastructure and compliance.

iii. All the government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications are conducted on a regular basis after hosting also.

iv. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.

v. Government has formulated Cyber Crisis Management Plan (CCMP) for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

vi. Government is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

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

*****