GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *299
TO BE ANSWERED ON:23.03.2022

CYBER ATTACK ON CRITICAL INFRASTRUCTURE

***299. MS. S. JOTHIMANI:**
SHRI KUMBAKUDI SUDHAKARAN:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) the year-wise number of cyber attacks on India's critical infrastructure from 2014 till date;

(b) whether the Government deems the current legal framework adequate to address the increase in the number of cyber attacks, especially in the light of recent security breaches;

(c) if so, the details thereof;

(d) whether the Government is planning to introduce a new, targeted legislation to address the increase in cyber attacks and if so, the details thereof; and

(e) the details of the measures taken by the Government to set up requisite infrastructure and schemes to provide a greater security against cyber attacks in the country?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (e): A Statement is laid on the Table of the House

STATEMENT REFERRED TO IN REPLY TO LOK SABHA
STARRED QUESTION NO. *299 FOR 23.03.2022REGARDING
CYBER ATTACK ON CRITICAL INFRASTRUCTURE
……..

(a):The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. As per information provided by National Critical Information Infrastructure Protection Centre (NCIIPC), no cyber attack was reported to NCIIPC in the declared Critical Information Infrastructures (CIIS)/Protected Systems (PS).

(b) and (c):Legal provisions exist in the Information Technology Act, 2000 to deal with cyber attacks. Sections 43 and 66 of the Act provides for penalty and punishment for cyber attacks. Section 70(3) of the Information Technology Act 2000 provides for penalty and punishment for unauthorized access of Critical Information Infrastructure/Protected Systems.

(d):There is no such new legislation under active consideration of this Ministry.

(e): Government is fully cognizant and aware of various cyber security threats including cyber terrorism; and has taken following measures to set up requisite infrastructure and scheme to provide greater security against cyber-attacks in the country:

(i) National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for cyber security matters.

(ii) Under the provisions of section 70A of the Information Technology (IT) Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. NCIIPC provides near real-time threatintelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

(iii) Under the provisions of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents.

(iv) National Cyber Coordination Centre (NCCC) is a multi-stakeholder project and is implemented by the CERT-In under the Ministry of Electronics and Information Technology (MeitY). NCCC scans the cyberspace in the country at meta-data level to generate near real-time macroscopic views of the cyber security threats. NCCC provides a structured system and facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate the cyber security threats.

(v) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre provides detection of malicious programs and free tools to remove the same.

(vi) CERT-In operates 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.

(vii) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.

(viii) CERT-In has empanelled 96 security auditing organisations to support and audit implementation of Information Security Best Practices.

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

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

(xi) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 64 such drills have so far been conducted by CERT-In where 820 organizations from different States and sectors participated.

(xii) CERT-In regularly conducts workshops for Ministries, Departments, States & UTs and organizations to sensitise them about the cyber security threat landscape and enable them to prepare and implement the CCMP. 128 CCMP workshops have been conducted till February 2022 by CERT-In. Out of these, 31 CCMP workshops conducted during the year 2021.

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

(xiv) 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. 15 and 19 training programs were conducted covering 708 and 5169 participants during the year 2020 and 2021 respectively.

(xv) CERT-In co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

****