GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 2322
TO BE ANSWERED ON: 17.12.2021

INCIDENCE OF CYBER ATTACKS

2322. SHRI PARIMAL NATHWANI:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) how many incidents of cyber attacks have taken place in the country in the last three years;
(b) whether Government has taken adequate steps to counter both cyber attacks and cyber terrorism and if so, the details thereof; and
(c) the relevant laws in place to handle these kind of threats created by cyber terrorism and whether they are adequate to tackle the same?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The Government is well aware of cyber security threats as the Internet expands and more & more Indians get connected and use Internet. Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. CERT-In has reported that a total number of 208456, 394499, 1158208 and 1213784 cyber security incidents are observed during the year 2018, 2019, 2020 and 2021 (upto October) respectively.

(b): Government is fully cognizant and aware of various cyber security threats; and has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures 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 is conducted on a regular basis after hosting also.
iv. CERT-In has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.
v. The Government has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments

of Central Government, State/UT Governments and their organizations and critical sectors.

vi. Cyber security mock drills are conducted regularly in Government and critical sectors. 61 such drills have so far been conducted by CERT-In where 600 organisations from different States and sectors participated.

vii. 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 17 training programs were conducted covering 708 and 4801 participants during the year 2020 and 2021 (till October) respectively.

viii. CERT-In 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.

ix. CERT-In is providing the requisite leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to, containment and mitigation of cyber security incidents reported from the financial sector.

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

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

(c): The current law provides certain legal provisions to deal with cyber-attacks and cyber terrorism. Section 66F of the Information Technology (IT) Act, 2000 has prescribed stringent punishment for cyber terrorism. Also sections 43 and 66 of the Act provides for penalty and punishment for cyber-attacks.

Further, section 69A of the Information Technology Act 2000 empowers Government to block any information generated, transmitted, received, stored or hosted in any computer resource in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above.

****