GOVERNMENT OF INDIA

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

LOK SABHA

UNSTARRED QUESTION NO. 2719

TO BE ANSWERED ON: 04.08.2021

CYBER ATTACKS

2719. DR. NISHIKANT DUBEY:

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

(a) whether the Government has taken adequate steps to counter both the cyber-attacks and cyber terrorism and if so, the details thereof;

(a) whether the incidents of cyber-attacks and hacking of Indian websites from hackers of foreign countries are on the rise; and

(b) if so, the details thereof; and

(c) the required steps taken by the Government in this regard?

ANSWER

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

(a) and (d): Government has taken the following measures to enhance the cyber security posture and prevent cyber attacks:

i. Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India.

ii. 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 Governments and their organizations and critical sectors.

iii. CERT-Inissues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.

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

v. 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.

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

vii. Cyber security mock drills and exercises are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 59 such drills have so far been conducted by CERT-In where 565 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

viii. 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.

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

x. Government 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 cooperates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

xii. National Critical Information Infrastructure Protection Centre (NCIIPC) provides near real time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

(b) and (c): 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 of 2,08,456, 3,94,499, 11,58,208 and 6,07,220 cyber security incidents have been observed during the year 2018, 2019, 2020 and 2021 (upto June) respectively. Out of this, a total number of 17,560, 24,768, 26,121 and 15,651Indian websites were hacked during the year 2018, 2019, 2020 and 2021 (upto June)respectively.

There have been attempts from time to time to launch cyber attacks on Indian cyber space. It has been observed that attackers are compromising computer systems located in different parts of the world and use masquerading techniques and hidden servers to hide the identity of actual systems from which the attacks are being launched.

According to the logs analyzed and made available to CERT-In, the Internet Protocol (IP) addresses of the computers from where the attacks appear to be originated belong to various countries including Algeria, Brazil, Canada, China, France, Germany, Hong Kong, Indonesia, Netherlands, North Korea, Pakistan, Russia, Serbia, Singapore, South Korea, Sri Lanka, Taiwan, Thailand, Tunisia, Turkey, USA, Vietnam etc.

****