GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.1879
TO BE ANSWERED ON: 03.07.2019

CYBER ATTACKS AND CYBER TERRORISM

1879. SHRI RAHUL RAMESH SHEWALE:
SHRI BHARTRUHARI MAHTAB:

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

(a) whether the Department of Telecom (DoT) has issued guidelines to counter cyber-attacks and cyber terrorism for Indian carrier and if so, the details of such guidelines;
(b) whether the Government has reviewed such guidelines during each of the last three years and the current year and if so, the details and the outcome thereof;
(c) whether the incidents of cyber-attacks and hacking of Indian websites from foreign countries particularly China and Pakistan are on the rise during the said period and if so, the details thereof, country-wise; and
(d) the corrective steps taken by the Government in this regard?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a) and (b): Department of Telecommunications has issued comprehensive security conditions to the Telecom Service Providers through amendment in the of terms and conditions of license agreement in May/June 2011. Subsequently these have been suitably made as an integral part of Unified License. The salient features are as follows:

(i) The LICENSEE shall be completely and totally responsible for security of their networks.
(ii) The LICENSEE shall have organizational policy on security and security management of their networks including Network forensics, Network Hardening, Network penetration test, Risk assessment.
(iii) The LICENSEE shall audit their network or get the network audited from security point of view once a year from a network audit and certification agency.
(iv) The LICENSEE shall induct only those network elements into its telecom network, which have been got tested as per relevant contemporary Indian or International Security Standards.
(v) The certification shall be got done only from authorized and certified agencies/ labs.
(vi) The LICENSEE shall keep record of all command logs.

(vii) The LICENSEE shall create facilities for the monitoring of all intrusions, attacks and frauds on his technical facilities and provide reports on the same to the Licensor/CERT-IN.

(c) : In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners to protect networks by way of hardening and deploying appropriate security controls. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 33147, 30067, 17560 and 10930 Indian websites were hacked during the year 2016 , 2017, 2018 and 2019 (till May) respectively.

There have been attempts from time to time to launch cyber attacks on Indian cyber space. These attacks have been observed to be originating from the cyber space of a number of countries including China and Pakistan.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.

(d): Government has taken several steps to prevent such cyber security incidents and enhancing cyber security posture in the country: These, *inter alia,* include :

(i) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology (IT) Act, 2000.

(ii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.cert-in.org.in).

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

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

(v) Government has empanelled 84 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vi) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

(vii) Government has formulated 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.

(viii) Cyber security mock drills and exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 43 such exercises have so far been conducted by CERT-In where organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS 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. 24 trainings covering 845 participants conducted in the year 2018.

(x) Government has launched 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.

(xi) Government has set up National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.

****