GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3887
TO BE ANSWERED ON: 11.12.2019

HACKING OF INDIAN WEBSITES

3887. SHRI BHARTRUHARI MAHTAB:
SHRI RAHUL RAMESH SHEWALE:

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

(a) whether the instances of cyber crimes and hacking of Indian websites from foreign countries have increased in recent years;

(b) if so, the details thereof including the number of such instances reported during each of the last three years and the current year, country-wise and the reasons therefor;

(c) whether the Indian Delegations have visited the said countries for dialogue under bilateral cooperation in the field of communications and IT during the said period;

(d) if so, the details and the outcome thereof, country-wise along with the issues discussed in such dialogue; and

(e) the safeguards in place to prevent cyber crimes and hacking of Indian websites by foreign countries and monitoring the activities of foreign countries along with achievements thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a) and (b): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 33147, 30067, 17560 and 21467Indian websites were hacked during the year 2016, 2017, 2018 and 2019 (till October) 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 China, Pakistan, Netherlands, France, Taiwan, Tunisia, Russia, Algeria and Serbia.

(c), (d) and (e): For resolution of incidents involving systems outside the country, CERT-In devises response measures in coordination with its counterpart agencies in foreign countries.

Government has taken several steps to prevent cyber security incidents and enhancing cyber security 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/vulnerabilities and countermeasures to protect computers and networks on regular basis
(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 90 security auditing organisations to support and audit implementation of Information Security Best Practices.
(vi) 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.
(vii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 44 such drills have so far been conducted by CERT-In where 265 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. 19 trainings covering 515 participants conducted in the year 2019 till October.
(ix) 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.
(x) 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.

****