GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1522
TO BE ANSWERED ON: 27.11.2019

CYBER ATTACKS

1522. SHRI S. VENKATESAN:

Will the Minister of Electronics & Information Technology be pleased to state:-
(a)   whether incidents of cyber attacks have increased in recent times;
(b)   if so, the details thereof including the incidents of cyber attacks reported during each of the last three years and the steps taken by the Government in this regard; and
(c)   whether foreign companies are behind any such cyber attacks, if so, the details thereof and the effective steps and action taken by the Government in this regard?

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), 50362, 53117, 208456 and 313649 cyber security incidents including phishing, network scanning and probing, virus/malicious code and website hacking are reported during the year 2016, 2017, 2018 and 2019 (till October) respectively.

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.

Government 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) Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.
(iv)   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.
(v)   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.
(vi)   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.
(vii) 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.
(viii) Government has initiated setting up of 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.

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

****