GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 4588
TO BE ANSWERED ON: 06.04.2018

MENACE OF CYBER ATTACK

4588 SHRI LAL SINH VADODIA:

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

(a) whether it is a fact that there is an apprehension of cyber attacks in the country;

(b) if so, whether Government is considering to safeguard the country from the cyber attacks; and

(c) if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI K. J. ALPHONS)

(a): With the proliferation of Information Technology and related services, there is a rise in cyber attacks in the country like elsewhere in the world. Cyberspace is virtual and borderless, thus cyber attacks can come from anywhere, anytime and by anyone.

(b) and (c) : Government has taken the following steps to enhance cyber security in the country:

(i) 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).

(ii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of section 70A of the Information Technology (IT) Act, 2000 for protection of critical information infrastructure in the country. NCIIPC has been regularly advising the critical information infrastructure (CII) sector organisation to reduce vulnerabilities to all kinds of threats and attacks, by sharing threat intelligence, guidelines, best practices and frameworks for protection and guiding them with policies and protection strategies. In addition, training and awareness programs are regularly conducted to improve the cyber hygiene in CII organisations

(iii) 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.

(iv) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 25 such exercises have so far been conducted by CERT-In wherein organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc participated.

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

(vi) Government has empaneled 67 security auditing organisations to support and audit implementation of Information Security Best Practices.

(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. 22 training programs covering 610 participants were conducted during the year 2017.

(viii) 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.

(ix) 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 already been made operational.

****