GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1586
TO BE ANSWERED ON: **27.12.2017**

INCREASE IN HACKING ATTEMPTS

1586. PROF. K.V. THOMAS:
DR. KAMBHAMPATI HARIBABU:

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

(a) whether foreign hackers, especially from China and Pakistan are secretly getting into our system and creating security threats and if so, the details thereof;

(b) whether there has been an increase in the number of hacking attempts of Indian companies;

(c) if so, the details thereof including number of hacking attempts identified/reported during the last three years; year-wise;

(d) whether the Government has estimated any loss to the companies due to hacking attempts and cyber attacks and if so, the details thereof; and

(e) the steps taken by the Government to end this menace?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ALPHONS KANNANTHANAM)

(a): There have been attempts from time to time to penetrate systems/devices of cyber networks operating in Government and its personnel. These attacks have been observed to be originating from the cyber space of a number of countries including China and Pakistan.

(b) and (c): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455, 50362 and 40054 cyber security incidents were observed during the year 2014, 2015, 2016 and 2017 (till November) respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, ransomware, denial-of-service attacks, etc. These incidents were reported to CERT-In by various organisations and individuals.

(d): No separate data with regard to the losses incurred by the Indian companies as a result of cyber attacks is maintained by Indian Computer Emergency Response Team (CERT-In).

(e): The Government has taken following measures in regard to preventing unauthorised access to data and enhancing the cyber security of information technology infrastructure in the country:

(i) Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks.

(ii) Government has published Guidelines for Chief Information Security Officers (CISOs) for Secure Applications and Infrastructure. Government has also specified key roles and responsibilities of CISOs in all Central Government Ministries/Department, State Governments/UTs and critical sector organisations managing ICT operations to strengthen IT Infrastructure. National Critical Information Infrastructure Protection Centre (NCIIPC) sends alerts and advisories for the protection of critical information infrastructure periodically.

(iii) Government (MeitY) has formulated Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments/UTs and their organizations and critical sectors.

(iv) CERT-In publishes guidelines regularly for securing the websites, computer systems and applications, which are available on its website (www.cert-in.org.in).

(v) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers on regular basis. Security tips have been published to enable users to secure their Desktops and mobile/smart phones. Tailored alerts are sent to key organisations to enable them to detect and prevent cyber attacks.

(vi) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. In addition 3 drills were conducted in coordination with The Reserve Bank of India and The Institute for Development and Research in Banking Technology.

(vii) CERT-In regularly conducts 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. 14 training programs covering 431 participants and 22 training programs covering 610 participants were conducted during 2016 and 2017 (till November) respectively.

(viii) National Informatics Centre (NIC), which provides Information Technology / E-Governance related services to Government Ministries/Departments, protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place.

(ix) NIC protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place. NIC has deployed state-of-the-art security solutions including firewalls,

intrusion prevention systems, anti-virus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardenings. These are complemented by round-the-clock monitoring of security events and remedial measures are carried out for solving the problems subsequently. A 24x7 security monitoring centre including NIC-CERT is in place at NIC for detecting and responding to security incidents.

****