GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

STARRED QUESTION NO:137
ANSWERED ON:14.08.2013
NATIONAL CYBER SECURITY POLICY
Adsul Shri Anandrao Vithoba;Anandan Shri K.Murugeshan

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

(a) whether the cyber security threats and cases of hacking have risen from 23 in 2004 to 22,060 in 2012 according to the report of the Indian Computer Emergency Response Team; ^

(b) if so, the details thereof;

(c) whether certain cases of cyber attacks affecting various Ministries/Departments have been reported and if so, the details thereof;

(d) whether attention of the Government has been drawn to the reported surveillance of Indian web users by US agencies; and

(e) if so, the reaction of the Government thereto along with the measures being taken thereon to protect the public and private infrastructure from cyber attacks?

Answer

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI KAPIL SIBAL)

(a) to (e); A Statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. 137 FOR 14.08.2013 REGARDING NATIONAL CYBER SECURITY POLICY

(a) and (b): As per the data tracked and reported to the Indian Computer Emergency Response Team (CERT-In), the number of incidents pertaining to cyber security threats and hacking have risen from 23 in 2004 to 22060 in 2012. These security incidents are related to scanning/probing, spam, malware infection, denial of service, website hacking and email & system hacking. These attacks have been observed to be directed from cyber space of different countries. Over a period, the nature and pattern of incidents have become more sophisticated and complex.

(c): There have been attempts from time to time to launch cyber attacks on the Information Technology (IT) infrastructure of Government organizations. These attacks are of the nature of web site hacking, injecting malware, targeted denial of service and hacking of emails. The number of cases of hacking of web sites of Central Ministries/Departments and State Governments increased to 371 in the year 2012 from 308 in the year 2011.

(d) and (e): In June 2013, foreign media reports disclosed extensive electronic surveillance programmes deployed by the U.S. agencies to collect internet and telephony data.

Government has expressed concerns over reported U.S. monitoring of internet traffic from India. Concerns with regard to violation of any of Indian laws relating to privacy of information of ordinary Indian citizens as well as intrusive data capture deployed against Indian citizens or Government infrastructure have been conveyed to the U.S. Government. In addition, the issue of U.S. cyber surveillance activities was discussed during the India-US Strategic Dialogue meeting held in New Delhi on 24 June 2013.

Government is taking appropriate protective measures by way of an integrated approach with a series of legal, technical and administrative steps to ensure that necessary systems are in place to address the growing threat of cyber attacks. In this direction,

Government has approved a framework for cyber security, including protection of critical sectors in country that envisages a multi-layered approach for ensuring defence-in-depth with clear demarcation of responsibilities among various agencies and departments. Government is also working towards promoting the evolution of better international internet governance-norms, through ongoing discussions at international fora.

Besides this, in order to address the issues of cyber security in a holistic manner, the Government has released the `National Cyber Security Policy - 2013` for public use and implementation with all relevant stakeholders. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.