GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

STARRED QUESTION NO:130
ANSWERED ON:30.11.2011
CYBER CRIMES
Raghavan Shri M. K.;Sayeed Muhammed Hamdulla A. B.

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

-

(a) whether there has been a spurt in cyber crimes / leaks in the country in the recent past;

(b) if so, the details thereof and the nature of cases reported during the last three years and the current year;

(c) whether the Universal Serial Bus (USB) memory sticks play a major role in Cyber leaks and if so, the details thereof;

(d) whether the Government has requested foreign countries including USA to share information on Cyber Crimes and if so, the details thereof and the reaction of these countries thereto;

(e) the percentage of Internet traffic monitored by the Government through monitoring equipment.; and

(f) the measures being taken to check cyber crimes?

Answer

MINISTER OF THE STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI KAPIL SIBAL)

(a)to(f): A Statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK S ABHA STARRRED QUESTION NO.M30 FOR 30-11-2011 REGARDING CYBER CRIMES.

(a)and(b): With the increase in the proliferation of Information Technology and related services there is a rise it number of cyber crimes and cyber security incidents. The trend in increase in cyber incidents is similar to that worldwide. As per the crime data maintained by National Crime Records Bureau, a total of 217,288,420 and 966 Cyber Crime cases were registered under Information Technology Act, 2000 during 2007, 2008, 2009, 2010 respectively, thereby showing an increasing trend. A total of 339, 176, 276 and 356 cyber crime cases were reported under Sections of Indian Penal Court (IPC) relating to Cyber cases during 2007, 2008, 2009, 2010 respectively.

The nature of cyber crimes as recorded by NCRB included tampering computer source documents, hacking, obscene publication / transmission in electronic media, un-authorized access / attempt to access to protected computer system, breach of confidentiality / privacy, digital signature related crimes.

(c): The Universal Serial Bus (USB) stick, also known as pen drive, is a removable storage media used by computer users. The USB sticks / pen drives are mostly used now due to operational convenience in data storage and mobility. Such USB sticks may a!so be used by miscreants to steal information from computers, which are not logically and physically protected. Malicious code and virus also propagates through such USB sticks.

(d): India has entered into cyber security incidents cooperation arrangements with United States of America, Japan and South Korea in the form of Memorandum of Understanding between Indian Computer Emergency Response Team (CERT-In) and the respective counterpart CERT agencies. These MoUs cover the aspect of exchange of information on cyber attacks and mutual response to cyber security incidents.

(e): Lawful monitoring of Internet traffic is carried out by Security Agencies as per the Laws of country. The installation and upgradation of Lawful Monitoring System at International Gateway and / or nodes of Service Providers is a continuous activity and is carried out as per the requirements of Security Agencies and terms & conditions of the respective License Agreement.

(f): In order to address the growing threat of Cyber Crimes in the country, Government has evolved an integrated approach with a series of the following legal, technical and administrative steps to ensure that necessary systems are in place to address the threat effectively.

i) The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address the issues connected with security breaches of information technology infrastructure,

ii) Department of Information Technology circulated Computer Security Guidelines and Cyber Security Policy to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks and leakage of information including security policy and procedures for handling portable storage media.

iii) National Informatics Centre (NIC) managing Govt. websites and providing e-mail services is implementing measures to secure the Govt. IT infrastructure from the cyber attacks,

iv) All the new 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. Out of approximately 7000 Government websites, more than 5500 websites have been audited. Steps are in progress for auditing of rest of the websites. Further, National Informatics Centre (NIC) has been directed not to host websites which are not audited with respect to cyber security.

v) Department of Information Technology along with Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) is involved in providing basic and advanced training of Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence,

vi) Department of Information Technology has initiated a major programme on cyber forensics specifically development of cyber forensic tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyse the digital evidence and present them in Court,

vii) Department of Information Technology has set up Cyber forensic training labs at Central Bureau of Investigation (CBI) and State of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir.

viii) Department of Information Technology has formulated a set of investigation manuals with procedures for Search, Seizure analysis and presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States,

ix) Indian Computer Emergency Response Team issues alerts, advisories and guidelines regarding cyber security threats and measures to be taken to prevent cyber incidents and enhance security of Information Technology systems.

x) The `Crisis Management Plan for countering cyber attacks and cyber terrorism` was prepared and circulated for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.