GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:637
ANSWERED ON:07.08.2013
CYBER CRIME AND HACKING OF WEBSITES
Dhanaplan Shri K. P.;Hazari Shri Maheshwar ;Jardosh Smt. Darshana Vikram;Mohan Shri P. C.;Ray Shri Saugata;Saroj Smt. Sushila;Shivanagouda Shri Shivaramagouda;Singh Shri Uday Pratap;Sivasami Shri C.;Tanwar Shri Ashok;Upadhyay Seema;Vardhan Shri Harsh;Verma Smt. Usha;Vijayan Shri A.K.S.;Viswanathan Shri P.

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

(a) whether the cases of cyber attacks and hacking of Government websites including that of Defence and Public Sector Undertakings by foreign nationals have been reported and if so, the details thereof;

(b) the details of the security measures taken / proposed to be taken by the Government to protect cyber networks and also the action taken against the culprits;

(c) whether the Government proposes to create the National Critical Information Infrastructure Protection Centre (NCIIPC) and if so, the details thereof and the present status of the NCIEPC;

(d) whether there is acute shortage of cyber professionals / experts in the country to deal with Cyber attacks; and

(e) if so, the details thereof and the action taken by the Government for training and recruitment of cyber professionals?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRIMILINDDEORA)

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team

(CERT-In), a total number of 308, 371 and 78 Government websites were hacked during the years 2011, 2012 and 2013 (up to June) respectively. A total no. of 13301, 22060 and 16035 security incidents related to scanning/probing, spam, malware infection, Denial of Service and system break-in including that of Govt, Defence and Public sector undertakings were reported to CERT-In during the year 2011, 2012 and 2013 (upto June) respectively. 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 system from which the attacks are being launched. It is difficult to attribute the origin of cyber attacks.

(b): Various measures have been taken by the Government to detect and prevent cyber attacks on web sites. These are:

i) National Cyber Security Policy 2013 approved by the Government on May 8, 2013 and released on July 2, 2013 addresses protection of information and information infrastructure in Cyber Space, building capabilities to prevent and respond to Cyber threats, reducing vulnerabilities and minimizing damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

ii) 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,

iii) It has been mandated that all government websites to be hosted on infrastructure of NIC, ERNET or any other secure infrastructure service provider in the country.

iv) National Informatics Centre (NIC) which hosts the government websites is continuously engaged in upgrading and improving the security posture of its hosting infrastructure,

v) Legal Framework in the form of Information Technology Act, 2000. The Act provides legal framework to address the issues connected with cyber attacks and security breaches of information technology infrastructure, vi) All the Ministries / Departments of Central Government and State Governments have been asked to implement the Crisis Management Plan to counter cyber attacks and cyber terrorism.

vii) The Government has circulated Computer Security Policy and Guidelines to all the Ministries /Departments on taking steps to prevent, detect and mitigate cyber attacks. In addition, all state governments and UTs have been advised to implement appropriate security measures to prevent hacking of websites.

viii) 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 the websites, which are available in its website (www.cert-in.org.in). CERT-In also conducts regular training programme to make the system administrators aware about secure hosting of the websites.

ix) The organizations operating critical information infrastructure are regularly advised to implement information security management practices based on International Standard ISO 27001. Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems.

x) Cyber Security Mock Drills to assess preparedness of organizations to withstand cyber attacks are being conducted by the Government. Seven such drills have been conducted since November 2009. The Government is developing indigenous technology by carrying out Research and Development (R&D) in the area of cyber security,

xi) CERT-In has empanelled a total of 22 IT Security Auditors, who may be engaged by any Government or private Organization to conduct security audit of their IT infrastructure.

xii) The Government is developing indigenous technology by carrying out research and development in the area of Cyber Security.

(c): Section 70A of the Information Technology Act 2000 provides for designating a National Nodal Agency for protection of National Critical Information Infrastructure. Government has identified National Information Infrastructure Protection Centre (NC1IPC) as the Agency for protection of Critical Information Infrastructure and appropriate steps in this regard have been initiated.

(d) and (e); A recent study conducted by International Information Systems Security Certification Consortium, Inc. reveal that globally there has been steady rise in the demand of Information Security professionals which would continue to increase by 13.2% CAGR in the coming years. The demand forecast for Information security professionals is of 4.2 lakhs by 2016. Further, due to the recent amendments in IT Act and the changing threat pattern it is expected that more than 1 lakh resources would be additionally required in the field of information security.

National Cyber Security Policy 2013 approved by the Government on May 8, 2013 and released on July 2, 2013 has included as an objective creation of a workforce of 500,000 professionals skilled in Cyber Security in the next 5 years through capacity building, skill development and training. The strategy for Human Resource Development comprises of:

Fostering education and training programs both in formal and informal sectors to support the Nation`s cyber security needs and build capacity.

Establishing cyber security training infrastructure across the country by way of public private partnership arrangements.

Establishing cyber security concept labs for awareness and skill development in key areas.

Establishing institutional mechanisms for capacity building for Law Enforcement Agencies.

The Government has taken the initiative to engage with the private sector on cyber security including capacity building in various fields of Cyber security. In this regard, a Joint Working Group (JWG) with representatives of both public and private sector was set up to work out the details in July 2012 and the Joint Working Group (JWG) has submitted its report on engagement with Private Sector on Cyber Security in Oct. 15, 2012. Action has been initiated for implementation of the recommendations in key priority areas and it is an on-going process.

Indian Computer Emergency Resoonse Team (CERT-In) is involved in providing basic and advanced training in Cyber Security to professionals in Government involved in operation of Information Infrastructure. Further. CERT-In and Centre for Development of Advanced Computing (CDAC) provide training in Cyber Forensics to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.