GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

STARRED QUESTION NO:267
ANSWERED ON:12.12.2012
CYBER CRIMES
Dhanaplan Shri K. P.;Vinay Kumar Alias Vinnu Shri

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

(a) the details of the cases of cyber crimes and hacking of websites reported in the country during the last three years and the current year, State-wise;

(b) whether the Joint Working Group on cyber security has submitted its report;

(c) if so, the salient features of the recommendations along with the action taken/proposed to be taken by the Government thereon;

(d) whether the Government has any proposal to establish an autonomous institution on cyber security and if so, the details thereof; and

(e) the other security measures taken/being taken by the Government to check hacking and cyber crimes in the country?

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.267 FOR 12.12.2012 REGARDING CYBER CRIMES.

(a): According to National Crime Records Bureau (NCRB) a total number of 696, 1322 and 2213 cases of cyber crimes under IT Act and Cyber Crime related IPC Sections were registered in the year 2009, 2010 and 2011 respectively, State/UT wise list is at Annexure-I. State/UT wise and head wise (including hacking) number of cases reported and persons arrested under IT Act and Cyber Crime related IPC Sections reported during 2009-2011 are at Annexure II and III respectively. The latest available information pertains to the year 2011. Cyberspace is virtual and borderless. A website can be hosted on a server at any location in the country as well as worldwide. Similarly, the website could be accessed from anywhere in the world. It is difficult to categorise hacking of websites on Sate-wise basis. No such list is complied or available. As per the information tracked and reported to Indian Computer Emergency Response Team (CERT-In) a total number of 9180, 16126, 14232 and 14392 websites were hacked in the year 2009, 2010, 2011 and 2012 (till October) respectively.

(b): The report of the Joint Working Group (JWG) on "Engagement with Private Sector on Cyber Security" was released on 15 October, 2012.

(c): The salient features of the JWG inter alia include Guiding Principles and Objectives, "Roadmap" for Public-Private- Partnership (PPP) on cyber security and four pilot projects. The recommended "Roadmap" includes setting-up of an institutional framework for involvement of private sector, capacity-building in the area of cyber security, development of cyber security standards and assurance mechanisms and augmentation of testing & certification facilities for IT products.

(d): There is no such proposal to establish an autonomous institution on cyber security.

(e): The various measures taken by the Government to check hacking and cyber crimes in the country are:

i) Legal Framework in the form of Information Technology Act, 2000. The Act provides legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

ii) Setting up of Early Warning and Response to cyber security incidents through the Indian Computer Emergency Response Team (CERT-In) and collaboration at national and international level for information sharing and mitigation of cyber attacks. CERT-In regularly publishes Security Guidelines and advisories for safeguarding computer systems from hacking and these are widely circulated. CERT-In also conducts security workshops and training programs on regular basis to enhance user awareness.

iii) 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. The existing Government websites are periodically audited from security perspective and vulnerabilities found are plugged.

iv) 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.

v) The Government has circulated Computer Security Policies & Guidelines and 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.

vi) Cyber Security Mock Drills to assess preparedness of organizations to withstand cyber attacks are being conducted by the Government. Six such drills have been conducted since November 2009. Next cyber security mock drill is scheduled in December, 2012.

vii) The Government is developing indigenous technology by carrying out Research and Development (R&D) in the area of cyber security.

viii) Government is facilitating for skill & competence development in the area of cyber security by providing domain specific trainings on Cyber Forensics, Network & System Security Administration. Labs for training in collection and analysis of digital evidence for Law Enforcement & Judiciary have been setup.

ix) Government is working with the industry to create awareness in the area of cyber security. Brochures and pamphlets have been prepared providing information on do's and don'ts with respect to cyber security for the usage of electronic and Information Technology (IT) devices.