GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:580
ANSWERED ON:27.02.2013
HACKING OF WEBSIES
Jakhar Shri Badri Ram ;Kanubhai Patel Jayshreeben;Krishnaswamy Shri M.;Meghe Shri Datta Raghobaji;Shetkar Shri Suresh Kumar;Venugopal Shri P.

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

(a) whether the incidents of cyber crimes and hacking of websites are on the rise;

(b) if so, the names and number of websites hacked separately by the national and international hackers;

(c) whether some websites have been hacked as a protest against Section 66A of Information Technology Act;

(d) if so, the details thereof and the action taken by the Government to check the misuse of the said section of the Act; and

(e) the corrective measures taken by the Government to check recurrence of such hackings of websites and the training imparted/proposed to be imparted to Security Agency/Police Personnels in this regard?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRJM1LINDDEORA)

(a) and (b): With the increase in the proliferation of Information Technology and related services there is a rise in number of cyber crimes and hacking of websites. As per the cyber crime data maintained by National Crime Records Bureau (NCRB), a total of 420, 966 and 1791 Cyber Crime cases were registered under Information Technology Ac! during 2009, 2010, 2011 respectively, thereby showing an increasing trend. A total of 276, 356 and 422 cases were registered under Cyber Crime related Sections of Indian Penal Court (IPC) during 2009, 2010, 2011 respectively. In addition, 6, 5. 6 Cyber Crime cases were registered by Central Bureau of Investigation (CBI) during the years 2010. 2011 & 2012 under provisions of Information Technology Act 2000 along with other acts. As per the information tracked and reported to Indian Computer Emergency Response Team (CERT-In) a total number of 9180, 16126, 14232 and 15895 and 1210 websites were hacked in the year 2009, 2010, 2011, 2012 and 2013 (January) respectively. The hackers operate with various fictitious and virtual names in the cyberspace and hack the websites. The hackers connect themselves nationally and internationally. It is therefore difficult to identify them with respect to any geographical boundaries.

(c) and (d): The website of Bharat Sanchar Nigam Limited (BSNL), `www.bsnl.co.in1 was reported to be hacked as a protest against section 66A of Information Technology Act on 13.12.2012 by ` Anonymous India hacker group.

Government has issued an Advisory to all the State Governments and Union Territories to ensure citizen`s right to freedom of speech and expression and proper implementation of provisions of section 66A of the Information Technology Act. 2000.

(e): The various corrective measures taken by the Government to check recurrence of such hackings of websites, cyber attacks and the training imparted/proposed to be imparted to Security Agencies /Police Personnals arc: 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 various types of cyber crimes and prescribes punishment also for such crimes.

ii. All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The existing Government websites are periodically audited from security perspective and vulnerabilities found are plugged.

iii. 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.

iv. Indian Computer Emergency Response Team (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.

v. 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.

vi. 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. Next cyber security mock drill is scheduled in July, 2013.
vii. The Government is developing indigenous technology by carrying out Research and Development (R&D) in the area of cyber security.

viii. Ministry of Home Affairs has issued an Advisory to the State Governments and Union Territory Administrations on Cyber Crime. State Governments have been advised to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes. Also, under the Cyber Crime Investigation programme, Ministry of Home Affairs is supporting the establishment of Cyber Crime Police Station (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each State / Union Territory of India under Police Modernization Scheme. Action also has been taken to set up a National Centre of Excellence exclusively devoted to render Cyber Forensic services and to act as National Research and Training Centre on Cyber Forensics.

ix. Government 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.

x. A major programme has been initiated on development of cyber forensics 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 Courts.

xi. Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence. Â«

xii. Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CB1) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura. Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.

In collaboration with Data Security Council of India (DSCI), NASSCOM. Cyber Forensic Labs have been set up at Mumbai, Bangluru. Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.