GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:4212
ANSWERED ON:02.05.2012
SETTING UP INTERNET AUTHORITY
Pandey Saroj;Punia Shri P.L.

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

(a) whether it is true that the (dot in) domain is not protected well and is open to security threats as reported in the media;

(b) if so, the details thereof and the action taken in this regard;

(c) whether the Government proposes to set up an Internet Authority to check cyber crimes;

(d) if so, the details thereof; and

(e) if not, the reasons therefor and the steps being taken by the Government in this regard?

Answer

MINISTER OF THE STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI SACHIN PILOT)

(a) and (b): Worldwide around 64.4 crore websites are registered under `.com`, `.org`, `.net`, `.info`, `.biz` etc. domains and approximately 14.3 lakhs websites are under `.in` domain. Out of the total registered websites, hacking under `.in` domain is around 0.7% and other domains are around 0.3%. Large number of websites hacked under `.in` domain are hosted on the infrastructure installed outside the country. Hacking of websites under `.in` domain is therefore a result of combination of poor design of websites as well as poor security of the infrastructure hosting such websites. The allocation of `.in` country code top level domain (ccTLD) is carried out by .IN Registry. It is one of the best protected registry in the world , as access to `.in` domains is performed via a highly redundant, global Anycast Server network, which protects against massive distributed denial of service (DDOS) attacks.

(c), (d) and (e): There is no proposal in the Department to set up an Internet Authority to check cyber crime.In order to address the growing threat of cyber crimes in the country, Government has evolved an integrated approach with a series of legal, technical and administrative steps to ensure that necessary systems are in place to address the threat effectively. They are:

(i) The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced with effect from 27.10.2009. The Act provides legal framework to address various types of cyber crimes and prescribes punishment also for such crimes.

(ii) A major programme has been initiated on development of cyber forensics specifically 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.

(iii) Indian Computer Emergency Response Team (CERT-In) and Centre for Deveload Advanced Computing (CDAC) are involved in providing basic and advanced training. Enforcement Agencies, Forensic labs and Judiciary on the procedures and methoded collecting, analysing and presenting digital evidence.

(iv) Cyber forensic training lab has been set up at the Training Academy of Central Bureau of Investigation (CBI) 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.

(v) In collaboration with Data Security Council of India (DSCI), NASSCOM Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata. DSCI has organized 112 training programmes on cyber crime investigation and awareness and a total of 3680 Police officials, Judicial officials and Public Prosecutors have been trained through these programmes. National Law School of India University, Bengaluru has also been conducting training on Cyber Law and Cyber Forensics through Judicial officers.

(vi) 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 of all States. Indian Computer Emergency Response Team (CERT-In) 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.