GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:5445
ANSWERED ON:09.05.2012
CYBER SECURITY
Bapurao Shri Khatgaonkar Patil Bhaskarrao;Bhoi Shri Sanjay;Chavan Shri Harischandra Deoram;Gaikwad Shri Eknath Mahadeo;Paranjpe Shri Anand Prakash;Punia Shri P.L. ;Venugopal Shri P.

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

(a) whether the Government has requested its embassies abroad to search for cyber security entities that can be acquired by Indian firms to secure the nation`s computer networks and websites against hacking attacks;

(b) if so, the details thereof and the outcome thereof;

(c) whether Indian cyber security agencies are not well equipped to deal and investigate with cyber crimes/threats as compared to other countries including China;

(d) if so, the details thereof; and

(e) the action taken by the Government to evolve a fool proof cyber prevention mechanism in the country?

Answer

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

(a): No, Sir.

(b): Does not arise.

(c) and (d): Police and Public Order are State subjects under the Constitution and as such the State Governments and Union Territory Administrations are primarily responsible for prevention, detection, registration and investigation of crime including Cyber Crime and for prosecuting the criminals through Law Enforcement machinery within their jurisdictions. The Government of India is, however, deeply concerned about crime, including the Cyber Crimes and therefore, has been advising the State Governments from time to time to give more focused attention to improving the administration of criminal justice system and take such measures as are necessary for the prevention of crime. The Government has issued a comprehensive advisory on prevention of crime on 16th July 2010 to all the State Governments and UT Administrations advising inter-alia, as under:

# To build adequate technical capacity in handling cyber crime (wherein a computer is either a tool or a target or both). They must create necessary technical infrastructure, including establishment of adequate number of cyber police stations, and post technically trained manpower for detection, registration, investigation and prosecution of cyber crimes.

# To establish anti-cyber-crime missions to stop those behind computer intrusions., the spread of malicious code etc; to identify and thwart online sexual predators -wife use the Internet to exploit children and produce, posses or share child pornography; to counteract operations that target intellectual property, endangering national security and competitiveness; and to dismantle national and transnational organized criminal enterprises engaging in crimes / frauds on the Internet.

(e): In order to address the growing threat of Cyber incidents in the country, Government has taken a series of measures covering aspects like 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 various types of cyber crimes and prescribes punishment also for such crimes.

(ii) 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.

(iii) Cyber Crime Cells have been set up by the State Police. These Cells investigate cyber crime cases and help respective police organizations in implementation of Laws addressing cyber crime.

(iv) Cyber forensic training lab has been set up at Traimng 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) 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.

(vi) Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are 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.

(vii) In collaboration with Data Security Council of India (DSCI), NASSCOM. Cyber Forensic Labs have been set up at Mumbai, Bangluru, Pune and Kolkata. DSCI has organized 112 training programmes on Cyber Crime Investigation and awareness and a total of 3680 Police officials, judiciary and Public prosecutors have been trained through these programmes. 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.

(viii) 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. 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.