GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:5347
ANSWERED ON:09.05.2012
MISUSE OF ICT
Rao Shri Sambasiva Rayapati

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

(a) whether the incidences of misuse of Information and Communication Technologies has been reported during the last three years and the current year;

(b) if so, the details thereof, State-wise;

(c) the action taken by the Government against the persons/companies involved therein; and

(d) the steps taken/being taken in coordination with the States and IT professionals to avoid such incidents in future?

Answer

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI MILIND DEORA)

(a) and (b): With the increase in the proliferation of Information Technology and related services there is a rise in number of incidences of misuse of information and communication technologies. The trend in increase in cyber incidents is similar to that worldwide. As per the crime data maintained by National Crime Records Bureau, a total of 288, 420 and 966 Cyber Crime cases were registered under Information Technology Act, 2000 during 2008, 2009 and 2010 respectively. A total of 176, 276 and 356 cyber crime cases were reported under Sections of Indian Penal Code (IPC) relating to Cyber Crime cases during 2008, 2009, 2010 respectively.

State-wise details of cyber crime cases registered under Information Technology Act 2000 and Indian Penal Code are enclosed at Annexure.

(c): 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.

Indian Computer Response Team (CERT-In) has the mandate to analyze and respond to Cyber Incidents in the country. The organization scan the malicious information in the Cyber space and detect the misuse of Information and Communication Technologies. CERT-In collects details of the incident from persons/organisations about information and communication assets which are misused. Based on their analysis of such Incidents of misuse, CERT-In issues advisories to the persons/organizations/service providers about such misuse. CERT-In advises them appropriate preventive steps. Further, the Government under Section 69A of Information Technology Act, 2000 is also empowered to block the website only under specific conditions.

(d): 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) 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.

iv) 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,

v) Cyber forensic training lab has been set up at 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.

vi) 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.

vii) 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 Unkm 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.