GOVERNMENT OF INDIA
HOME AFFAIRS
LOK SABHA

STARRED QUESTION NO:336
ANSWERED ON:17.08.2010
CYBER CRIMES
Meghwal Shri Arjun Ram ;Shetkar Shri Suresh Kumar

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether cases of cyber crimes have been reported in the recent past;

(b) if so, the details of the crimes reported during each of the last three years and the current year, State-wise and crime-wise;

(c) whether the Government has taken any steps to augment the cyber security infrastructure of the States and amendments to the relevant laws; and

(d) if so, the details thereof?

Answer

MINISTER OF THE STATE IN THE MINISTRY OF HOME AFFAIRS (SHRI AJAY MAKEN)

(a) to (d): A Statement is laid on the Table of the House.

STATEMENT IN REPLY TO PARTS (a) TO (d) OF THE LOK SABHA STARRED QUESTION NO.336 FOR 17.08.2010.

(a) to (d): According to the information reported to the National Crime Records Bureau (NCRB) by the State Governments/UT Administrations, a total of 142, 217 and 288 cases under the Information Technology (IT) Act and 311, 339 and 176 cases under various sections of the Indian Penal Code (IPC) related to cyber crimes were reported in the country during the years 2006 to 2008 respectively. The State/UT-wise details of the aforesaid cases of cyber crimes, as compiled by the NCRB, are at the Annexure. The latest information is available for the year 2008.

'Police' and 'Public Order' are State subjects under the Seventh Schedule to the Constitution of India and, therefore, the State Governments are primarily responsible for prevention, detection, registration and investigation of crime, including cyber crimes, and also for prosecuting the accused criminals through the law enforcement machinery within their jurisdiction. 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:Â¬-

(i) The State Governments and UT Administrations must 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.

(ii) The States/UTs must establish anti-cyber-crime missions to stop those behind computer intrusions, frauds, the spread of malicious code etc.; to identify and thwart online sexual predators who use the Internet to exploit children and produce, possess 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. The comprehensive advisory on Prevention of Crime dated 16th July, 2010 is available on the website of the Ministry of Home Affairs (http://mha.nic.in).

The fight against cyber crime involves a coordinated effort on the part of several agencies in the Govt. on an on going basis. Government is following an Integrated approach with a series of legal, technical and administrative steps to ensure that necessary structures and mechanisms are in place to address the growing threat of Cyber Crimes in the country. Some of the specific steps taken by the Government are:

1. The Information Technology Act 2000 together with the Indian Penal Code, 1860 provides legal framework for countering cyber crimes.

2. The Information Technology Act, 2000 has been amended by the Information Technology (Amendment) Act, 2008 w.e.f. 27-10-2009. The amended act is a comprehensive Act and addresses all prevailing forms of cyber crimes. It has provisions to deal with cyber crimes such as: - tampering with computer source documents, computer related offences, sending offensive messages through communication services, dishonestly receiving stolen computer resource or communication device, identity theft, cheating by

personation by using computer resource, violation of privacy, cyber terrorism, publishing or transmitting obscene material in electronic form, publishing or transmitting of material containing sexually explicit act in electronic form, publishing or transmitting of material depicting children in sexually explicit act, in electronic form. The Act also provides for penalty and compensation to the affected victims for damage to computer, computer system & network and loss of data.

3. Indian Computer Emergency Response Team (CERT-In) has been set up to act as a national nodal agency to deal with and coordinate all matters concerning cyber security emergency response in the country. CERT -In develops appropriate Security Guidelines and other best practices for securing the Information Technology infrastructure. CERT-In publishes security alerts and advisories to prevent occurrence of cyber incidents and also conducts security workshops and training programs on regular basis to enhance user awareness for safeguarding computer systems. CERT-In is collaborating with computer hardware, software, and security product vendors, international Computer Emergency Response Teams (CERTs) and forums to share information on vulnerabilities, latest computer security threats and devise suitable countermeasures. CERT-In is also collaborating with sectoral CERTs in critical sectors such as Defence and Finance to address computer security incidents and promote security best practices in these sectors.

4. A major programme on cyber forensics, especially development of cyber forensic tools, setting up of infrastructure for investigations and training of the users has been initiated.

5. Basic and advanced training in the area of computer and cyber security & forensics is being provided to the Law Enforcement Agencies, Forensics Labs and Judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence in a court of Law.

6. Department of Information Technology (DIT) is implementing an Information Security Education and Awareness (ISEA) programme with the objectives of introducing Information Security Curriculum at M.Tech & B.Tech level and Research Activity/PhD, training System Administrators by offering Diploma/Certificate Course and training programmes for Government Officers on Information Security issues and General Awareness Programme.

7. DIT is facilitating research & development in security technology. These efforts cover basic research, technology demonstration, proofÂ¬-of-concept and R&D test bed projects in advanced and front line technology areas such as encryption, steganography, digital marking etc.

8. Cyber Forensic Training Labs have been set up at CBI - Academy and Kerala Police Head quarters for investigation of cyber crimes as well as training of police officials in the area of Seizure, analysis and presenting digital evidence in a court of Law.

9. For training police, judicial officers and others in cyber security, cyber crimes and forensics, training and lab facilities are being set up at the North-Eastern states namely, Assam, Tripura, Meghalaya, Sikkim, Manipur, Mizoram and Nagaland.

10. Department has formulated collaborative arrangements with industry associations such as NASSCOM and CII to enhance information security awareness among consumers and users.

11. Cyber crime cells have been set up by the State Police and Central Bureau of Investigation (CBI). These cells investigate cyber crime cases and help respective police organisations in implementation of Laws addressing cyber crime.