GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1665
ANSWERED ON:03.12.2014
CYBER CRIMES
Girri Shri Maheish;Kumar Dr. Virendra ;Patel Smt. Jayshreeben ;Rai Shri Prem Das

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

(a) the details of the instances of cyber crimes reported in the country during the last three years and the current year, year wise;

(b) whether the Government has undertaken any study to assess the threat of cyber crime, particularly those related to cyber terrorism and financial crimes and if so, the details thereof;

(c) the action plan formulated / proposed to be formulated for prevention of cyber crimes including the capacity building measures particularly related to cyber intelligence; and

(d) the details of other steps taken by the Government in this regard?

Answer

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI RAVI SHANKAR PRASAD)

(a): As per the cyber crime data maintained by National Crime Records Bureau, a total of 966, 1791, 2876 and 4356 Cyber Crime cases were registered under Information Technology Act during 2010, 2011, 2012 and 2013 respectively. A total of 356, 422, 601 and 1337 cases were registered under Cyber Crime related Sections of Indian Penal Court (IPC) during 2010, 2011, 2012 and 2013 respectively. As per the information provided by Reserve Bank of India (RBI), 14271, 10048, 8765 and 6034 cyber fraud cases have been reported to the RBI during 2010-11, 2011-12, 2012-13 and 2013-14 respectively.

(b): National Crime Records Bureau (NCRB) compiles and publishes Annual Report `Crime in India` on various types of crimes reported in India including cyber crimes reported under Information Technology (IT) Act and related sections of Indian Penal Code (IPC). The latest edition of publication pertains to the year 2013. The report provides pace of Cyber Crime rate in the country. As per the report of NCRB, incidence of cyber crimes under IT Act 2000 and related Sections of IPC has increased by 63.7% in 2013 as compared to 2012 (from 3,477 cases in 2012 to 5,693 cases in 2013). Major Cyber crimes reported include Loss/damage to computer resource and obscene publication/transmission in electronic form, cyber forgery and cyber frauds. Further, Reserve Bank of India compiles data on a quarterly basis relating to financial crimes committed through Credit cards, ATM / Debit Cards and Internet Banking.

(c) and (d): The Government has formulated action plan for prevention of Cyber Crimes which includes series of technical, administrative, legal and capacity building measures to address Cyber Crimes effectively. The steps include:

(i) The Information Technology Act, 2000 together with Indian Penal Code 1860 have adequate provisions to deal with prevailing Cyber Crimes. It provides punishment in the form of imprisonment ranging from two years to life imprisonment and fine / penalty depending on the type of Cyber Crime.

(ii) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.

(iii) 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.

(iv) In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bengaluru, 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.

(v) More than 26000 Police Officers and 600 judicial officers have so far been trained in the Training Labs established by the Government.

(vi) Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed and are being used by Law Enforcement Agencies.

(vii) Action has been initiated to set up two National Centres of Excellence in the area of Investigation of Cyber Crimes and Digital

Evidence.

(viii) The Government has initiated action to set up National Cyber Coordination Centre to coordinate with multiple agencies and stakeholders for preventing cyber attacks, reducing vulnerability to cyber attacks and minimizing damage & recovery time from such attacks when they occur.

(ix) 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.

(x) Indian Computer Emergency Response Team (CERT-In) also conducts training programmes regularly to Chief Information Security Officers, System Administrators, Network Administrators of different organizations in Public and Private Sector in relevant areas of Cyber security such as vulnerability assessment, advanced Cyber threat detection and mitigation, mobile security and latest cyber security technologies to build capacity at organization level leading to Cyber Intelligence skills.

(xi) Reserve Bank of India (RBI) has issued a Circular to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI has also advised Banks to leverage technology to support Business processes and implement all stipulations outlined by RBI from time to time. Banks are also advised to ensure implementation of basic Organizational framework and put in place policy and procedures to prevent financial frauds through Internet.

(xii) Reserve Bank of India (RBI) has issued several advisories on Credit Card operations by Banks. Use of PIN has been made mandatory in the transactions. The Banks have been advised to set up internal control system to combat frauds and to take proactive fraud control and enforcement measures. RBI has also issued advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds. RBI also has cautioned public through Notification against fictitious offers of remitting cheap funds from abroad.

(xiii) The framework for enhancing Cyber Security formulated by the Government envisages creation of sectoral CERT for banking sector. Information Security Analysis Centre (ISAC) for Banking sector has been set up at Institute for Development & Research in Banking Technology (IDRBT), Hyderabad.

(xiv) 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.