GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3452
TO BE ANSWERED ON: 16.12.2016

INCREASE IN CYBER CRIMES

3452 DR. T. SUBBARAMI REDDY

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether it is a fact that there is an unprecedented increase in cyber crimes in the country and it has grown to 350 percent in five years;
(b) if so, the response of Government to deal with internet crimes;
(c) how many persons out of 32,000 cyber crimes reported between 2011 and 2015, were convicted and why the conviction rate is very meagre; and
(d) whether, in view of recent demonetisation and increased cashless transactions, Government would review present cyber laws and legal framework to make them more stringent and comprehensive, if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a) and (b): With the proliferation of Information Technology and related services there is a rise in instances of cyber crimes in the country like elsewhere in the world. As per the data maintained by National Crime Record Bureau (NCRB), a total of 2213, 3477, 5693, 9622 and 11592 cyber crime cases were registered during the years 2011, 2012, 2013, 2014 and 2015 respectively, showing a rise of 424% during 2011 to 2015.

As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455 and 39730 cyber security incidents were observed during the year 2014, 2015 and 2016 (till October) respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, Denial of Service attacks, etc. Over a period, the nature and pattern of incidents have become more sophisticated and complex.

Further, CBI has registered a total of 93 cases during 2013–2016 (up to 31-10-2016) under IT Act, 2000.

Government has taken various steps in the form of legal framework, emergency response, awareness, training and implementation of best practices to prevent occurrence of cyber crimes. Such steps include:

i) The Information Technology (IT) Act, 2000 provides a comprehensive legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

ii) Government is implementing a Framework for enhancing cyber security, with a multi-layered approach for ensuring defence-in-depth and clear demarcation of responsibilities among the stakeholder organizations in the country.

iii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the IT Act, 2000 for protection of Critical Information Infrastructure in the country.

iv) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in). In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out.

v) Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

vi) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

vii) Government has initiated setting up of National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

viii) CERT-In is setting up a Botnet Cleaning and Malware Analysis centre for detection of computer systems infected by malware and to notify, enable cleaning and securing systems of end users to prevent further malware infections.

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

x) 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.

xi) Industry associations such as Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs, set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime investigation. Academia like 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.

xii) A number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed indigenously and such tools are being used by Law Enforcement Agencies.

xiii) CERT-In and Centre for Development of Advanced Computing (C-DAC) 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.

xiv) Reserve Bank of India (RBI) issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI also issues advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds.

(c): NCRB has started collecting data on cases convicted since 2014. As per data collected from States/UTs, out of 9,622 cases registered during 2014 and 11,592 cases registered during 2015, a total of 310 cases and 234 cases have resulted into conviction.

(d): The electronic payment in the country is governed by relevant provisions of Reserve Bank of India Act, 1934, Payment and Settlement Systems Act, 2007 and the IT Act, 2000 and rules and guidelines formulated therein. Moreover, under power conferred under section 70(b) of the IT Act, 2000, Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures in respect of various form of electronic payments.

****