GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:364
ANSWERED ON:25.02.2015
CYBER CRIMES
Chavan Shri Ashok Shankarrao;Dhotre Shri Sanjay Shamrao;Gupta Shri Sudheer;Kirtikar Shri Gajanan Chandrakant;Mahtab Shri Bhartruhari;Maragatham Smt. K.;Rathod Shri Dipsinh Shankarsinh;Shinde Dr. Shrikant Eknath;Singh Shri Kunwar Haribansh;Sundaram Shri P.R.

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

(a) the total number of cyber crimes registered during each of the last three year in the country, State / UT-wise;

(b) whether as per a recent study by ASSOCHAM there is an alarming rise of cyber crimes in the country which may double in 2015 and pose serious economic and national security challenges;

(c) if so, the details of the study, the response of the Government thereto and the steps taken/being taken by the Government to check such menace; and

(d) whether the National Crime Records Bureau Statistics has also reported 350 percent surge in cyber crimes in the last three years and if so the details thereof and the reaction of the Government thereto?

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 1791, 2876 and 4356 Cyber Crime cases were registered under Information Technology Act 2000 (IT Act 2000) during 2011, 2012 and 2013 respectively. A total of 422, 601 and 1337 cases were registered under Cyber Crime related Sections of Indian Penal Court (IPC) during 2011, 2012 and 2013 respectively. State/Union Territory wise cases registered under IT Act 2000 and cyber crime related sections of IPC during 2011-2013 are enclosed at Annexure. A total number of 22060, 71780 and 130338 cyber security incidents including phishing, scanning, spam, malicious code, website intrusion etc, were reported to the Indian Computer Emergency Response Team (CERT-In) during the year 2012, 2013 and 2014 respectively. In addition, a total number of 27605, 28481 and 32323 websites were hacked by various hacker groups during the year 2012, 2013 and 2014 respectively.

(a) and (c): Government is aware of the media reports on the recent study by ASSOCHAM. The study is based on the cyber security incidents reported to Indian Computer Emergency Response Team (CERT-In). These incidents include phishing, scanning, spam, malicious code, website intrusion etc. Information relating to Cyber Crime cases registered in the country is maintained by National Crime Records Bureau (NCRB). As per the data made available by NCRB, a total of 4356 cyber crime cases were registered under Information Technology Act 2000 (IT Act 2000) during the year 2013 as compared to 2876 cases during 2012, thus showing an increase of 51.5 percent in 2013 over 2012. The ASSOCHAM study has predicted figures based on the cyber security incidents of CERT-In.

To combat the cyber crimes and cyber attacks in the country effectively, Government has taken various steps which include:

1. 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 Enfor- cement and Judiciary in these States.

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

3. 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.

4. 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.

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

6. It is proposed to set up two National Centres of Excellence in the area of Investigation of Cyber Crimes and Digital Evidence.

7. Number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed and are being

used by Law Enforcement Agencies.

8. 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.

9. Steps have been taken to monitor and prevent financial frauds through phishing attacks, Credit / Debit card frauds, money laundering schemes etc.

10. 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.

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

12. CERT-In, Deity has also initiated action with active parti- cipation of Service Providers and Industry to set up a Centre for detection of computer systems infected by malware & botnets and to notify, enable cleaning and securing systems of end users to prevent further such infections.

(d): As per the cyber crime data available with National Crime Records Bureau (NCRB), there is a 143 percent increase in registered cyber crimes cases in the country. With the introduction of technologies, devices including smart phones and complex applications, and rise in usage of cyber space for businesses, the cyber crimes and attacks are also on the rise worldwide as well as in the country. Use of social media has also emerged as a key tool committing cyber crimes and attacks that affect nation and society. Government is conscious of such increase in cyber crimes and has taken various steps in the form of awareness, training, legal framework, emergency response and implementation of best practices to prevent occurrence of such cyber crimes.