GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:4671
ANSWERED ON:22.04.2015
BUDGETARY ALLOCATION TO COUNTER CYBER CRIME
Kalvakuntla Smt. Kavitha;Singh Shri Bharatendra;Venugopal Shri K. C.

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

(a) whether the budget allocation made to tackle cyber crimes during the last three years has decreased and if so, the details thereof and the reasons therefor;

(b) whether the Government has taken note of the huge allocations made by USA to check cyber crimes in the back drop of serious security breaches and ATM hacking in that country;

(c) if so, the reaction of the Government thereto; and

(d) whether in the light of above instances the Government proposes to make a similar increase in the budget allocation to check cyber threats in the country and if so, the details thereof?

Answer

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

(a): The budget allocation for Cyber Security Programme has steadily increased from Rs.36.06 crores during 2012-13 to Rs. 85 crores during 2015-16. The budget allocation during 2012-13, 2013-14, 2014-15 and 2015-16 were 36.06 crores, 42.37 crores, 62.0 crores and 85.0 crores respectively. The budget includes funds for measures and initiatives for tackling cyber crimes effectively.

(b) and (c): The Government is following the developments taking place in other countries including United States of America (USA) to check cyber crimes. The Government has adopted an integrated, multi pronged strategy covering aspects such as technical, administrative, and legal steps to protect and enhance cyber security. The government has taken the following specific measures and policy decisions to tackle cyber crimes:

i) The Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008, provides legal framework to address various types of prevalent cyber crimes and security breaches of information technology infrastructure.

ii) A major programme has been initiated on development of cyber forensics 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 analyze the digital evidence and present them in Courts.

iii) Cyber forensics 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, cyber forensic training and investigation labs have been set up 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) 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.

v) The Department 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.

vi) 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.

(d): The actions for checking cyber crime is a continuous process and strengthened to meet the requirements of the dynamic cyber threat environments. CERT-In, Deity has also initiated action with active participation 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.

An allocation of Rs. 85 crores has been made during 2015-16 for regular operational requirements of Indian Computer Emergency

Response Team (CERT-In) and Cyber Appellate Tribunal (CAT) and Cyber Security Research and Development (R&D).

In addition, the Government has initiated action to create a national level mechanism to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive and protective actions by individual entities. For this purpose, a financial outlay of Rs. 775 crores over a period of five years has been projected.