GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1547
TO BE ANSWERED ON: 28.07.2017

STUDY TO IDENTIFY CYBER THREATS

1547 SHRI ANIL DESAI:
SHRI SANJAY RAUT:
SHRI K.C. RAMAMURTHY:

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

(a) whether Government has taken any steps to control the rising trend of cyber attacks in the country, if so, the details thereof; and

(b) whether any study has been conducted to identify the cyber threats in the country?

ANSWER

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

(a): Government has taken a number of legal, technical and administrative policy measures for addressing cyber security. These include the following, namely:-

(i) Enactment of the Information Technology (IT) Act, 2000 which has adequate provisions for safety of sensitive personal information.

(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 CERT-In, a statutory authority under IT Act, 2000, 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 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 action by individual entities.

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

(vii) 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 personnel and Judiciary in these States.

(viii) 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.

(ix) A number of Cyber forensics tools for collection, analysis and presentation of the digital evidence have been developed indigenously and such tools are being used by law enforcement agencies.

(x) 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.

(xi) 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.

(xii) All banks have been mandated to report cyber security incidents to CERT-In expeditiously.

(xiii) All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised to carry out audit by the empanelled auditors of CERT-In on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices. Government has empanelled 54 security auditing organisations to support and audit implementation of Information Security Best Practices.

(xiv) Government has formulated Cyber Crisis Management Plan for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. Regular workshops are conducted for Ministries, Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan.

(xv) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.

(xvi) Ministry of Home Affairs has issued National Information Security Policy and Guidelines (NISPG) to Government organizations to ensure safety of data and minimize cyber threats.

(xvii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different states and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc have participated.

(xviii) CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 14 training programs covering 431 participants and 13 training programs covering 329 participants were conducted during 2016 and 2017 (till June).

(xix) Ministry of Electronics & Information Technology (MEITY) regularly conducts programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like http://infosecawareness.in/ and "www.cyberswachhtakendra.gov.in"

(b): In tune with the dynamic nature of Information Technology and limited window time available for an effective response, continuous efforts are required to be made to detect and prevent cyber attacks by way of continuous threat assessment and near real-time situational awareness. Such timely information enables coordinated actions by the stakeholders to take appropriate proactive and preventive action.

Concerted efforts are made to harvest the requisite information from multiple sources. These include incidents reported to and tracked by CERT-In, technical measures, security cooperation arrangement with overseas Computer Emergency Response Teams (CERTs) and leading security product and service vendors as well as agencies within the government. In addition, the study reports published by various agencies across the world are also studied to understand the historical data with respect to global threat landscape and threat predictions. As such, Government has not conducted a separate study to identify cyber threats.

****