GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *16
TO BE ANSWERED ON: 16.11.2016

CYBER ATTACKS

***16 ADV. M. UDHAYAKUMAR:**
SHRI RAM CHARITRA NISHAD:

Will the Minister of ELECTRONICS & INFORMATION TECHNOLOGY be pleased to state:-

(a) whether the incidents of cyber attacks have shown a rising trend in recent times and if so, the details thereof and reasons therefor;

(a) whether any study has been conducted to identify the cyber threats from outside the country, particularly from Pakistan and if so, the details thereof;

(b) whether the Computer Emergency Response Team India (CERT-In) has issued warning to all banks cautioning of impending attacks by cyber criminals from Pakistan and if so, the details thereof and measures taken by CERT-In in this regard; and

(c) the new initiatives taken/proposed to be taken by the Government to protect cyber space in the country?

ANSWER

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

(a) to (d): A Statement is laid on the Table of the House.

STATEMENT REFERED TO IN REPLY TO LOK SABHA STARRED QUESTION *16 FOR 16.11.2016 REGARDING CYBER ATTACKS

(a): With the proliferation of Information Technology and related services there is a rise in number of cyber security incidents in the country like elsewhere in the world. 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.

(b): The area of Information Technology (IT) is characterized by rapid developments and dynamic growth. With every IT product and service introduced into the market, newer vulnerabilities are discovered, leaving scope for malicious actions. 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 from outside the country 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 actions.

Concerted efforts are being made to harvest the requisite information from multiple sources. These include incidents reported to and tracked by Indian Computer Emergency Response Team (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 from outside the country. As per current trends, the cyber attacks observed on networks/systems in Indian cyber space are observed to be directed from cyber space of different countries including Pakistan.

(c): CERT-In tracks information on cyber security threats, vulnerabilities and events of cyber attacks. Based on this information and patterns, alerts and advisories are issued on emerging cyber threats and possible cyber attacks. In October 2016, CERT-In has issued alert to key organizations including banks regarding possible attempts of attacks by hacker groups with advice to monitor network activities, strengthen security of systems/websites and reporting of anomalies to CERT-In.

(d): In order to enhance the cyber security of the country and protect cyber space, the following key actions are taken by the Government:

i. 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.
ii. 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. The Crisis Management Plan is updated periodically on annual basis to take into account changing scenario of cyber threat landscape. 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. So far 41 workshops have been conducted.
iii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 11 such drills have so far been conducted by CERT-In where 110 organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc participated.
iv. Government has empaneled security auditing organisations to support and audit implementation of Information Security Best Practices. Currently, 57 organisations have been empaneled.
v. Operationalising the National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology Act 2000, for protection of Critical Information Infrastructure in the country. NCIIPC is providing tailored advisories on software/hardware vulnerabilities and alerts on cyber attacks are being issued regularly to Chief Information Security Officers of Critical Information Infrastructure organizations. In addition policy, audit and compliance reports of Critical Information Infrastructure organizations are being analysed.
vi. Government is establishing Botnet cleaning and malware analysis centre to detect and clean infected systems in the country. The project is initiated in coordination with the Internet Service Providers and Industry.
vii. Government is setting up of National Cyber Coordination Centre (NCCC) is initiated 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. Government is implementing 'Information Security Education and Awareness (ISEA)' project to train professionals / government officials and create mass information security awareness among citizens. The Project is implemented by 51 institutions across the country. So far, 11,110 persons have been trained/undergoing training in various formal/non-formal courses focusing on Cyber Security. 2,384 Government personnel have been trained in direct training programs. CDAC Hyderabad has conducted 377 Awareness workshops for various user groups covering 42,379 participants from 22 States/UT.

ix. 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 such training programs were conducted covering 431 participants during the year 2016.

x. Government has set up cyber forensic training & investigation labs at CBI Academy and 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. More than 1250 police officers in North Eastern states have been trained. The objective of these labs is to train police officers for seizing and imaging electronic evidence. In addition, National Institute of Technical Teachers Training and Research(NITTTR), Chandigarh has trained 2756 Engineering and Polytechnic college teachers, whereas National Law School of India University (NLSIU), Bangalore imparted training to 1398 officials including judiciary, law teachers & practitioners, law students, law researchers, etc.

****