

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1936
TO BE ANSWERED ON: 05.12.2019

CYBER ATTACKS ON INDIAN SITES FROM CHINA

1936. SHRI V. VIJAYASAI REDDY:

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

- (a) whether it is a fact that as per the report of the Indian Computer Emergency Response Team (CERT-In) of the Ministry, 35 per cent of cyber attacks on Indian sites are from China;
- (b) if so, the details of malicious activities that have been identified and what remedial measures are being taken against such attacks; and
- (c) the steps taken/proposed to be taken to contain such attacks?

ANSWER

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

(a): There have been attempts from time-to-time to penetrate systems/devices of cyber networks operating in cyber space of the country. These attacks include website intrusions, scanning/probing and malicious code and have been observed to be originating from the cyber space of a number of countries including China.

(b) and (c): The Government has taken several measures for preventing unauthorised access to data and enhancing the cyber security of information technology infrastructure in the country. These, *inter alia*, include:

- (i) Enactment of the Information Technology Act 2000 which has provisions to deal with cyber attacks.
- (ii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology (IT) Act, 2000.
- (iii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.
- (iv) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

- (v) All the government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications will be conducted on a regular basis after hosting also.
- (vi) Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.
- (vii) 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.
- (viii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 44 such drills have so far been conducted by CERT-In where 265 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.
- (ix) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 19 trainings covering 515 participants conducted in the year 2019 till October.
- (x) 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.
- (xi) Government has set up 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. Phase-I of NCCC has been made operational.
