

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 574
TO BE ANSWERED ON: 14.12.2018

AGENCY FOR TACKLING CYBER THREATS

574. DR. T. SUBBARAMI REDDY:
SHRIMATI AMBIKA SONI:

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

- (a) whether according to security solutions provider, Symantec, India is the third most vulnerable country to cyber threats;
- (b) if so, the measures taken to find solutions to malware, spam, phishing, network attacks, web attacks, ransomware and cryptominers; and
- (c) whether any coordinated agency has been created to tackle the increasing attacks, especially when the country is going for more and more online and digital transactions, if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a): There are media reports about India emerging as the third most vulnerable country to cyber threats.

(b) and (c): Government has taken a number of legal, technical and administrative measures to address the issue of cyber threats. These *inter alia*, include:

- (i) Information Technology Act, 2000 was enacted to deal with cyber crime. IT Act has adequate deterrent provisions for cyber threats and cyber attacks.
- (ii) 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.
- (iii) 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).
- (iv) 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 already been made operational.
- (v) Government has launched the Cyber Swachhhta 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.
- (vi) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 38 such exercises have so far been conducted by CERT-In wherein organisations from

different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc. participated.

- (vii) Government has empanelled 76 security auditing organisations to support and audit implementation of Information Security Best Practices. 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.
