GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 689
TO BE ANSWERED ON: 08.02.2019

CYBER ATTACKS IN THE COUNTRY

689. SHRI DEREK O'BRIEN:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether it is a fact that the country witnessed over 4.36 lakh cyber attacks between January to June, 2018;
(b) the details of cyber attacks over the period of 2014-2018, year-wise; and
(c) the measures taken by Government to address the issue of cyber attacks in the country.

ANSWER

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

(a) : There were media articles, citing a report published by a cyber security company named M/s F-Secure, stating that around 4.36 lakh cyber attacks were observed towards India. The findings of such reports by cyber security vendors are generally based on data generated by their products and details of such data is not available and hence cannot be verified.

(b) : As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 44679, 49455, 50362, 53117 and 208456 cyber security incidents including phishing, network scanning and probing, virus / malicious code and website hacking were reported during the year 2014, 2015, 2016, 2017 and 2018 respectively.

(c) : Government has taken several measures to enhance the cyber security posture and prevent cyber attacks. These, *inter alia*, include :

(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).
(ii) Government has formulated Cyber 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.
(iii) Government has issued guidelines for Chief Information Security Officers (CISOs) of organisations regarding their key roles and responsibilities for securing applications/infrastructure and compliance.
(iv) Government has empanelled 76 cyber security auditing organisations to support and audit implementation of Information Security Best Practices.
(v) 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 various sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc. participated.
(vi) 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. 24 trainings covering 845 participants were conducted in the year 2018.
(vii) 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.
(viii) Government has set 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 actions by individual entities. Phase-I of NCCC has been made operational.

****