GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1782
TO BE ANSWERED ON:21.09.2020

CYBER ATTACKS

1782. SHRI RITESH PANDEY:

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

(a) the number of cyber-attacks on Indian citizens and India-based commercial and legal entities during each of the last five years;
(b) whether the Government is aware that India has been identified as one of the top 5 countries with the most number of cyber-attacks, by multiple international and national organizations such as Data Security Council of India, Center for Strategic and International Studies, etc. and if so, the details thereof and the reaction of the Government thereto;
(c) the reasons for high incidence of cyber-attacks in India;
(d) whether the Government is planning to introduce a new cyber security policy;
(e) if so, the details thereof and if not, the reasons there of; and
(f) the time by which the said policy is likely to be implemented and the steps taken by the Government in this regard?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), 49455, 50362, 53117, 208456, 394499 and 696938 cyber security incidents are reported during the year 2015, 2016, 2017, 2018, 2019 and 2020 (till August) respectively.

(b) and (c): There was a media article in March 2020 by a vendor stating that India has been identified as one of the top 5 countries with the most number of cyber-attacks. Such vendor reports are not validated.

With proliferation in internet and mobile phone usage, there is a rise in number of cyber security incidents in the country as well as globally. Proactive tracking by CERT-In including its Cyber Swachhta Kendra and National Cyber Coordination Centre (NCCC) and improved cyber security awareness among individuals and organisations across sectors has led to increased reporting of incidents.

In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners to protect networks and systems by way of hardening and deploying appropriate security controls.

Government has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

(i) The Indian Computer Emergency Response Team (CERT-In) regularly issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.

(ii) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(iii) Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.

(iv) 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.

(v) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 49 such drills have so far been conducted by CERT-In where 434 organisations from different States and 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.

(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 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 actions by individual entities. Phase-I of NCCC has been made operational.

(d), (e) and (f): Public opinion and Stakeholder consultations were taken to draft a National Cyber Security Strategy. The National Cyber Security Strategy is under finalisation.

****