GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO.1184
TO BE ANSWERED ON: **11.02.2021**

CYBER ATTACKS AND HACKING OF INDIAN WEBSITES

1184. SHRI JYOTIRADITYA M. SCINDIA:

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

(a) whether several incidents of cyber attacks and hacking of Indian websites from foreign countries were reported in the recent past;
(b) if so, the details thereof; and
(c) the steps Government has since taken to check such cyber attacks and to maintain high security in the system?

ANSWER

MINISTER OFSTATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a) and (b): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 17560, 24768 and 26121 Indian websites were hacked during the year 2018, 2019 and 2020 respectively.

There have been attempts from time to time to launch cyber attacks on Indian cyber space. It has been observed that attackers are compromising computer systems located in different parts of the world and use masquerading techniques and hidden servers to hide the identity of actual systems from which the attacks are being launched.

According to the logs analyzed and made available to CERT-In, the Internet Protocol (IP) addresses of the computers from where the attacks appear to be originated belong to various countries including Algeria, Brazil, China, France, Indonesia,Netherlands, North Korea, Pakistan, Russia, Serbia, South Korea, Taiwan, Thailand, Tunisia, Turkey,USA, Vietnam etc.

(c): For resolution of incidents involving systems outside the country, CERT-In devises response measures in coordination with its counterpart agencies in foreign countries.
Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

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

iii. 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.

iv. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.

v. 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.

vi. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 50 such drills have so far been conducted by CERT-In where 450 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

vii. 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.

viii. Government is operating 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.

ix. Government has set up the 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 is operational.

****