GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3291
TO BE ANSWERED ON: 23.03.2018

HACKING OF GOVERNMENT WEBSITES

3291. SHRI HUSAIN DALWAI:

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

(a) whether a French national with pseudonym, Elliot Anderson, is penetrating/ hacking into several Government websites;
(b) if so, whether Government is aware of all the websites broken into by this foreign national and how much of sensitive data has been affected by his actions; if so, the details thereof and if not, the reasons therefor;
(c) whether Government carried out forensic audits of these websites to establish identity of this French national; and
(d) the action Government has taken to prevent foreigners from breaking into Government websites?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K. J. ALPHONS)

(a) to (c): No such incident has been reported to Ministry of Electronics and Information Technology or to CERT-In.

(d): Government has taken following measures for preventing cyber attacks and securing websites:

(i) All the new government websites and applications are required to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting. The Indian Computer Emergency Response Team (CERT-In) has empanelled 67 security auditing organizations to support and audit implementation of Information Security Best Practices.
(ii) CERT-In regularly tracks the hacking of websites and alerts the website owners concerned to take actions to secure the websites to prevent recurrence. CERT-In also issues alerts and advisories, on regular basis, regarding latest cyber threats and countermeasures.
(iii) 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.
(iv) Government has issued general guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications/infrastructure and compliance.
(v) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 25 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.
(vi) CERT-In conducts regular training programmes for network / system administrators and CISOs of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 22 training programs covering 610 participants were conducted during the year 2017.
(vii) 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.
(viii) National Informatics Centre (NIC) provides IT/E-Governance related services to Government Departments. NIC protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies. Also, relevant advisories are circulated among the NICNET users

for taking precautionary measures from time-to-time. NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems, anti-virus/anti-malware solution. Additionally, periodic security audits of computer resources are performed followed by hardenings. These are complemented by round-the-clock monitoring of security events.

******