GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(DEPARTMENT OF ELECTRONICS & INFORMATION TECHNOLOGY)

LOK SABHA

UNSTARRED QUESTION NO. 1769

TO BE ANSWERED ON: 04.05.2016

CYBER ATTACKS

1769 DR. SWAMI SAKSHIJI MAHARAJ:
SHRI SANKAR PRASAD DATTA:
SHRI JYOTIRADITYA M. SCINDIA:
SHRI B. V. NAIK:
SHRI ARJUN MEGHWAL:
DR. MANOJ RAJORIA:
SHRI AJAY NISHAD:
SHRIMATI KOTHAPALLI GEETHA:
SHRI P. P. CHAUDHARY:

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

(a) whether there has been significant increase in the number of cyber attacks/ hacking of Websites in the country during the last three years and the current year;

(b) if so, the details of the norms/guidelines or the policy formulated to counter such attacks and hackings;

(c) whether the Government proposes to review these norms/guidelines and if so, the details thereof; and

(d) the preventive steps taken/being taken by the Government to address the issue?

ANSWER

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a): With the proliferation of Information Technology and related services there is a rise in number of cyber security incidents in the country like elsewhere in the world. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 41319, 44679, 49455 and 14363 cyber security incidents including phishing, scanning, malicious code, website intrusion, denial of service etc, were reported to CERT-In during the year 2013, 2014, 2015 and 2016 (till March) respectively. These cyber security incidents include a total number of 28481, 32323, 27205 and 8056 website hacking incidents during the year 2013, 2014, 2015 and 2016 (till March) respectively. In addition, 54677, 85659, 61628 and 13851 spam (unsolicited email) incidents were reported to CERT-In during the year 2013, 2014, 2015 and 2016 (till March) respectively. Over a period, the nature and pattern of incidents have become more sophisticated and complex.

(b) and (c): The “National Cyber Security Policy” is released for public use and implementation by all relevant stakeholders. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country. In addition, 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.

CERT-In has published guidelines for securing the websites, computer systems and application, which are available on its website (www.cert-in.org.in).

National Informatics Centre (NIC) which provides Information Technology related services to Government departments, publishes cyber security policies, procedures, guidelines and advisories in the security portal for its users.

The Cyber Crisis Management Plan is updated periodically. The cyber security policies, procedures and guidelines are updated regularly to address emerging cyber threats and to enhance the security of Information Technology infrastructure.

(d): In order to enhance the cyber security posture of the country and improve the ability to resist cyber attacks the following key actions are being pursued:

i) Government is implementing a Framework for Enhancing Cyber Security for setting up institutions and mechanisms for enhancing cyber security, capacity building, strengthening of assurance and certification framework, promoting R&D and indigenization, human resource development and engagement with private sector on cyber security.

ii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In also conducts regular training programme to make the network and system administrators aware about securing the IT infrastructure and mitigating cyber attacks.

iii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

iv) Efforts towards setting up of National Cyber Coordination Centre (NCCC) to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

v) Efforts towards establishing the “Botnet cleaning and Malware Analysis centre” to detect and clean infected systems in the country.

vi) National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology Act 2000, for protection of Critical Information Infrastructure in the country. NCIIPC is providing tailored advisories on software/hardware vulnerabilities and alerts on cyber attacks are being issued regularly to Chief Information Security Officers of Critical Information Infrastructure organizations. In addition policy, audit and compliance reports of Critical Information Infrastructure organizations are being analysed.

vii) All Central Government Ministries / Departments and State / Union Territory Governments have been advised to conduct security auditing of entire Information Technology infrastructure.

viii) The National Informatics Centre (NIC) is operating a security monitoring centre for detecting and responding to security incidents.

****