GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

STARRED QUESTION NO:91
ANSWERED ON:14.07.2014
CYBER ATTACK TERRORISM
Ahir Shri Hansraj Gangaram;Mahtab Shri Bhartruhari

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

(a) whether there has been significant increase in number of cyber attacks/terrorism 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 cyber attacks/terrorism in the country;

(c) whether a number of incidents of cyber attacks/terrorism from certain foreign countries have also come to the notice of the Government during the said period and if so, the details thereof, country-wise;

(d) whether the Government proposes to review the norms/guidelines to counter such cyber attacks/terrorism and if so the details thereof; and

(e) 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) to (e): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. 91 FOR 14.07.2014 CYBER ATTACK / TERRORISM

(a) During the years 2011, 2012, 2013 and 2014 (till May), a total no. of 21699, 27605, 28481 and 9174 Indian websites were hacked by various hacker groups spread across worldwide. In addition, during these years, a total no. of 13301, 22060, 71780 and 62189 security incidents respectively were reported to the Indian Computer Emergency Response Team (CERT-In). These incidents included phishing, scanning, spam, malicious code, website intrusions etc.

(b) The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks. The Government has also circulated 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. Further to address the issues of cyber security in a holistic manner, the Government had released the "National Cyber Security Policy-2013" on 02.07.2013, for public use and implementation by all relevant stakeholders.

(c) There have been attempts from time to time to launch cyber attacks on Indian cyber space. These attacks have been observed to be originating from the cyber space of a number of countries including USA, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and UAE. It has been observed that the attackers compromise computer systems located in different parts of the World and use masquerading techniques and hidden servers to hide the identity of actual system from which the attacks are being launched. Cyber space is virtual, borderless and anonymous due to which it becomes difficult to actually trace the origin of a cyber attack.

(d) The security guidelines as circulated by the Government are updated regularly to include the countermeasures for mitigating latest cyber attacks. CERT-In also publishes security alerts and advisories on the latest cyber threats and vulnerabilities, available on CERT-In website (www.cert-in.org. in). Crisis Management Plan (CMP) for countering Cyber-Attacks and Cyber Terrorism is updated periodically on annual basis to take into account changing scenario of cyber threat landscape. The updated version is circulated to all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors for implementation. Workshops are organized regularly to provide training to officials in Central and State Government in the area of implementation of CMP.

(e) Apart from the steps as mentioned in (b) & (d) above, the Government has also taken the following key steps to enhance the cyber security of systems in the country:

i) Cyber Security Mock Drills are being conducted by the Government to help the organisations to assess their preparedness to withstand cyber attacks. Two such drills are being conducted every year with the involvement of organizations.

ii) Government has setup National Critical Information Infrastructure Protection Centre (NCIIPC) to protect the critical information infrastructure in the country.

iii) The action has been initiated to setup Centre for collection & analysis of malicious software, notify and clean the systems infected with malicious software.

iv) India has been recognized as Certificate Issuing Nation in the area of cyber security under Common Criteria Recognition Arrangement (CCRA). Under this arrangement, the certificates issued by India will be recognized internationally. This recognition will help country to setup chain of test centres for testing of Information Technology (IT) products with respect to cyber security.

v) All Central Government Ministries / Departments and State / Union Territory Governments have been advised to conduct security auditing of entire Information Technology infrastructure. All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting also. CERT-In provides necessary expertise to audit IT infrastructure of critical and other ICT sectors.

vi) All government websites are to be hosted on infrastructure of National Informatics Centre (NIC), ERNET India or any other secure infrastructure service provider in the country.

vii) Sectoral CERTs have been functioning in the areas of Defence and Finance for catering to critical domains. They are equipped to handle and respond to domain specific threats emerging from the cyber systems.

viii) Information Sharing and Analysis Centres (ISACs) for financial services has been set up at Institute for Development and Research in Banking Technology (IDRBT). Such a centre exchange information on cyber incidents in financial sector and advises them for appropriate mitigation. Action has been initiated to set up similar ISACs in power and petroleum sector.

ix) The organizations operating critical information infrastructure are regularly advised to implement information security management practices based on International Standard ISO 27001. Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems.

x) Centres have been setup in the States to train the police officers in area of cyber forensics for investigation of cyber crimes.

xi) Programmes for creating awareness about cyber security among Government officials and public are continuously being pursued by the government along with organisations from Government and Public.

xii) The Government is engaged with the Industry to evolve model of Public-Private Partnership (PPP) in the area of cyber security.

xiii) 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 the websites, which are available on its website (www.cert-in.org.in). CERT-In also conducts regular training programme to make the system administrators aware about secure hosting of the websites and mitigating cyber attacks.

xiv) Information Technology Act, 2000 provides legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

xv) The Government is encouraging development of indigenous technology by carrying out Research and Development 55735

xvi) (R&D) in the area of cyber security.