GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:2927
ANSWERED ON:10.12.2014
CYBER ATTACK HACKING
Agrawal Shri Rajendra;Ajmal Shri Sirajuddin;Dhotre Shri Sanjay Shamrao;Mahtab Shri Bhartruhari;Rao Shri Rayapati Sambasiva;Subbareddy Shri Yerram Venkata

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

-

(a) the details of cases of cyber attacks and hacking of Indian websites reported by Indian and foreign hackers separately during the last three years and the current year, year-wise;

(b) whether the Government has taken up the matter of cyber attack/hacking with the concerned countries;

(c) if so, the details thereof and the response of these nations;

(d) whether the Government has entered into bi-lateral cooperation/agreement with foreign countries on the issue; and

(e) if so, the details thereof, country-wise and other measures taken by the Government on Cyber Security and Surveillance ?

Answer

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

(a): 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 system from which the attacks are being launched. It is difficult to attribute the origin of cyber attacks be it from within the country or outside the country. A total number of 13301, 22060, 71780 and 101087 security incidents were reported to Indian Computer Emergency Response Team (CERT-In) during the year 2011, 2012, 2013 and 2014 (upto October) respectively. These incidents included phishing, scanning, spam, malicious code, denial of service, website intrusion etc. In addition, a total number of 21699, 27605, 28481 & 22034 Indian websites were hacked by various hacker groups spread across the world during the year 2011, 2012, 2013 and 2014 (upto October) respectively. Innovation and advancement in technology has helped the adversaries to apply sophisticated techniques to launch attacks and hide their identity.

(b) and (c): CERT-In reports the security incidents on the Indian cyberspace coming from international cyberspace to the CERTs of the respective countries and work with them to identify the hackers and take appropriate actions to stop such incidents. Besides this, such issues are also discussed for necessary action during the bilateral meetings.

(d) and (e): Indian Computer Emergency Response Team (CERT-In) enters into international cyber security cooperation arrangement with organizations engaged in similar activities, in the form of Memorandum of Understanding (MoU), to enhance its operational readiness. At present such MoUs have been entered into with US-CERT, Japanese - CERT, Korea Internet & Security Agency (KISA), CERT − Mauritius and CERT-Kazakhstan. Besides this, Government of Finland and Government of India have also signed a MoU on cooperation in the area of cyber security. Further, bilateral consultations have been initiated with Canada, Germany, Sweden, Malaysia and Brunei. CERT-In has also established collaborations with international security organisations for exchange of information related to latest cyber security threats and international best practices. CERT-In is a member of Forum of Incident Response and Security Teams (FIRST) and Asia Pacific CERT (APCERT). In addition, the Government has taken various other measures on cyber security, these include:

i) In order to address the issues of cyber security in a holistic manner, the Government has released the "National Cyber Security Policy-2013" on 02.07.2013, for public use and implementation by all relevant stakeholders. This policy aims at facilitating creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders' actions for protection of cyber space.

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

iii) Action is being initiated to set up a centre for tracking all the compromised systems connected on the Internet in the country and clean them on online basis so that the infection does not carry forward. The prototype of such centre is functioning. The centre will also collect and analyze malicious software so as to install appropriate software to prevent malicious activities.

iv) 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.

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) Indian Computer Emergency Response (CERT-In) has empanelled a total no. of 45 security auditors to carry out security audit of the IT infrastructure of Government, Public and Private sector organisations.

vii) All major websites are being monitored regularly to detect malicious activities.

viii) Close watch is kept to scan malicious activities on the important networks in the Government, Public and Service Providers.

ix) All the Ministries/ Departments of Central Government and State Governments have been asked to implement the Crisis Management Plan (CMP) to counter cyber attacks and cyber terrorism.

x) The National Watch and Alert System - Indian Computer Emergency Response (CERT-In) team is working 24/7 and scanning the cyber space in the country. The team works with Government, Service Providers, private sector and citizens both on pro-active and reactive basis and help in mitigating cyber incidents. The team also disseminate information and advise on the steps for strengthening the security of the systems. They work with the service providers to identify the computer systems which are compromised and are participating in launching attacks, isolate them and create corrective steps to clean them.. The system is being strengthened regularly in terms of the resources to address all incidents.

xi) 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.

xii) 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.

xiii) A major programme has been initiated on development of cyber forensics tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyse the digital evidence and present them in Courts.

xiv) 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.