GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:6610
ANSWERED ON:06.05.2015
CYBER SPYING BY CHINA
Dhurve Smt. Jyoti;Gandhi Shri Dilip Kumar Mansukhlal;Pandey Shri Ravindra Kumar;Singh Shri Sunil Kumar

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

(a) whether the Government is aware of the cyber spying being carried out by China;

(b) if so, the details thereof along with the details of the institutions targeted in India;

(c) whether Indian security agencies are well equipped to provide protection against such cyber spying attacks; and

(d) if so, the details thereof and the steps taken/being taken by the Government to deal with the issue comprehensively in future?

Answer

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

(a) and (b): There have been attempts from time to time to penetrate cyber networks and systems operating in Government organisations. These attacks have been observed to be directed from the cyber space of a number of countries including China. It has been observed that the 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.

(c) and (d): Government is aware of the nature of the threats in Cyber Space and accordingly, Government is following an integrated approach with a series of legal, technical and administrative steps to ensure that necessary systems are in place to address the growing threat of cyber attacks in the country.

The Government has taken following steps to enhance cyber security and prevent cyber spying attacks:

i) The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks.

ii) Equipping the Security agencies with suitable technical support to prevent and safeguard against cyber threats.

iii) Air gap between Internet and official networks is being maintained by organisations involved in strategic activities.

iv) The Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations.

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

vi) Indian Computer Emergency Response Team (CERT-In) is conducting mock cyber security drills to enable assessment of preparation of organizations to withstand cyber attacks. Organisations from key sectors of Government are participating in the drills.

vii) CERT-In issues the alerts advisories regarding latest Cyber threats and counter measures.

viii) All Central Government Ministries/Departments have been advised to conduct security auditing of Information Technology infrastructure periodically to discover gaps with respect to security practices and take appropriate corrective actions.

ix) CERT-In has empanelled 51 information security auditors through a stringent mechanism of selection to carryout audits.

In order to address the issues of cyber security in a holistic manner, the Government has released the "National Cyber Security Policy", 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. It aims to facilitate creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders actions for protection of cyber space. The policy is expected to serve as a long-term template for continuous evolution, guided actions and measurement of effectiveness of such actions. It also provides for creation of national level systems, processes, structures and mechanisms 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. As provided in the policy, steps have been initiated for adopting a prioritised approach to implement the policy so as to address the most critical areas in the first instance.

Further, Government has also taken steps to put in place a Framework for Enhancing Cyber Security, which envisages a multi-layered approach for ensuring defence-in-depth with clear demarcation of responsibilities among the stakeholder organizations in the country. The salient features of the Framework include setting up institutions and mechanisms for enhancing cyber security, capacity building and manpower augmentation by stakeholders, strengthening of assurance and certification framework, promoting R&D and indigenization, human resource development and engagement with private sector on cyber security.