GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1508
ANSWERED ON:06.03.2013
CYBER SECURITY THREAT
Mani Shri Jose K.

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

(a) whether the Government proposes to put in place telecom security policy in the emergence of serious cyber security threat from hostile nations/groups;

(b) if so, the details thereof and the extent to which the findings of US Congressional Security Review Commission is likely to help in its formulation;

(c) whether hacking of India`s high security cyber network has been on the increase by cyber intelligence agencies of foreign countries including China;

(d) if so, the details thereof;

(e) whether India has to activate its cyber security system urgently in the wake of threat by stuxnet malware; and

(f) if so, the details thereof?

Answer

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI MILIND DEORA)

(a) & (b) The Draft Telecom Security Policy has been prepared by the Department of Telecommunications to address the issues related to telecom security due to threats emanating from various sources like anti-social, anti-national, terrorist groups including hostile nations. The Salient feature of the Draft Telecom Security Policy are as follows:

(i) It is based on the principles of involvement of Stakeholders, International Cooperation, Suitable Regulatory framework, technical Solutions to take Precedence over Regulations and adopting a Practical and Progressive approach.

(ii) It addresses the various aspects of Telecom Security like communication assistance to Security Agencies, security of Communication, Information and Data, security of Telecom Network and Disaster Management.

(iii) It envisages 'Safe to Connect' Policy, which means every network element should be inducted into the network only after getting it security tested and certified from certified / authorized security testing labs.

(iv) Periodic security testing of the telecom network.

(v) Progressively develop indigenous capacity to manufacture electronic telecom equipment and software being inducted into the Network.

(c) & (d) There have been attempts from time to time to penetrate cyber networks operating in Government. These attacks have been observed to be originating 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. Hence, it is difficult to attribute cyber attack to a particular country.

(e) & (f) A sophisticated virus called as "Stuxnet" was reported to be spreading worldwide since July 2010. The virus targets Industrial Control Systems. The following specific steps were taken by the Government immediately after the threat was reported:

(i) Alerts and advisories about the Stuxnet threat were issued on website of the Indian Computer Emergency Response Team (CERT-In). Measures to be taken to detect infected systems, dis-infect the same and prevent further propagation were advised to all critical sector organizations in the country.

(ii) Government in association with Internet Service Providers (ISPs) and security vendors tracked the infected systems and advised the owners of the systems to dis-infect the same. Workshops were conducted by CERT-In and other government agencies jointly for critical sector organizations to create awareness and suggest steps to be taken to counter the threat.

Further, the government has taken the following measures to protect cyber networks:

Department of Information Technology and Electronics has circulated Computer Security Guidelines and Cyber Security Policy to all the Ministries/ Departments on taking steps to prevent, detect and mitigate cyber attacks.

All Central Government Ministries/ Departments and State/Union Territory Governments have been advised to conduct security audit of entire Information Technology Infrastructure, including websites, periodically to discover gaps with respect to security practices and take appropriate corrective actions.

Setting up of Early Warning and Response to cyber security incidents through the Indian Computer Emergency Response Team (CERT-In) and to have collaboration at national and international level for information sharing and mitigation of cyber attacks. CERT-In regularly publishes Security Guidelines and advisories for safeguarding computer systems and these are widely circulated. CERT-In also conducts security workshops and training programs on regular basis to enhance user awareness.

The 'Crisis Management Plan for countering cyber attacks and cyber terrorism' was prepared and circulated for implementation by all Ministries/ Departments of Central Government, State Government and their organizations and critical sectors.

CERT-In is conducting mock cyber security drills to enable assessment of preparation of organizations to withstand cyber attacks.

The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address the issues connected with security breaches of information technology infrastructure.

National Informatics Centre (NIC) managing Govt. websites and providing e-mail service is implementing measures to secure the Govt. IT infrastructure from cyber attacks.