GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1132
ANSWERED ON:11.12.2013
INTERCEPTION OF COMMUNICATIONS
Bhagora Shri Tarachand;Manian Shri O. S.;Natarajan Shri P.R.;Siddeswara Shri Gowdar Mallikarjunappa

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

-

(a) whether the Government has worked out any strategy to counter hate mails that are spreading fast in the country;

(b) if so, the details thereof;

(c) whether the Indian security agencies have access to Intercept all the telephone and Internet communications of Indian and foreign websites/operators;

(d) if so, the details thereof and if not, the mechanism in place or likely to be put in place to monitor such communications without the assistance of the concerned operators and web sites;

(e) whether Government proposes to extend telecom laws to give more teeth to Indian security agencies for gaining real time access to all forms of lawfully targeted communications and also have systems in place for ferreting out any spy software or malware hidden in imported gear used in telephone networks; and

(f) if so, the details thereof and if not, the action taken/proposed to be taken by the Government in this regard?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI MILIND DEORA)

(a) and (b): Government has recently notified National Cyber Security policy - 2013 in order to protect information and information infrastructure in Cyber space, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of intuitional structures, people, process, technology and cooperation. Further, Government has recently approved cyber security framework to achieve the objectives set out in National Cyber Security policy. Besides, Section 69A of Information Technology Act provides for blocking access to the public or cause to be blocked for access by the public information generated, transmitted, received, stored or hosted in any computer resource.

(c) and (d): Government has mandated all the Telecom Service Providers and the Internet Service Providers in India to provide the Lawful Interception and Monitoring facilities to the Indian security agencies for all the communication services. As such Security agencies are able to intercept the encrypted services through the lawful interception facilities provided by the Telecom Service Providers. However, Security Agencies have intimated that they are not able to decrypt some of encrypted intercepted communication to readable format. World over several services providers are providing services across the globe for sharing audio, video, image, email, data and accessing other web services anytime and anywhere by everyone in the world in a secure manner. The security of these services is achieved through encryption technology. These services are mostly availed by the citizens across world through Internet either in their individual capacity or as part of commercial activities. There are multifarious aspects involved in dealing with the issues related to such communication services such as technical, international relationship, legal and regulatory policy, commercial and security requirements etc. Therefore, the Government regularly interacts with all stakeholders to resolve this issue on subject arising from time to time.

(e) and (f): As per the provisions contained in section 5(2) of Indian Telegraph Act 1885 read with Indian Telegraph Rule 419A as well as Section 69 of the Information Technology Act read with Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of information) Rules, 2009, Security agencies can intercept and monitor the communication on real time basis in accordance with Sanction by the competent authority. A Standard Operating Procedure (SOP) for interception, handling, usage, sharing, copying, storage and destruction of messages / telephone / emails etc. and certification was notified by Ministry of Home Affairs in May 2011. Further, to automate this process of interception and monitoring the Government has decided to set up a Centralized Monitoring System (CMS), which will result in reducing the time for provisioning of lawful interception and monitoring request and better secrecy of the targeted communication.

In order to address the issue of spyware, malware etc. hidden in telecom and Information Technology equipment, the Government has issued instructions to the Telecom Service Providers through licence amendment that they should get any telecom equipment being inducted into telecom network security tested as per relevant contemporary Indian or International security standards from third party certified labs or provide a certificate to this effect if such third party lab do not exist for any particular element. From 1st July 2014, such security certification needs to be obtained from labs located in India. Government has also decided to set up Telecom Testing and Security Certification Centre to develop system, processes, procedure and tools for security testing of telecom equipment. The

centre will accredit the security testing labs in private, joint or public sector based on the system, process and procedures developed by it.