GOVERNMENT OF INDIA
HOME AFFAIRS
LOK SABHA

UNSTARRED QUESTION NO:336
ANSWERED ON:26.02.2013
MISUSE OF ELECTRONIC COMMUNICATION
Rajesh Shri M. B.

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Government has taken note of increasing instances of misuse of electronic communication by terrorists and criminals;

(b) if so, the measures taken by the Government to prevent such misuse; and

(c) the details of the mechanism put in place to check/monitor the cyber threats?

Answer

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS (SHRI R.P.N. SINGH)

(a): Yes, Madam. As per the intelligence inputs, terrorists are known to use internet for communication by using e-mails, facebook, chat forms, VOIP over broadband/data card/GPRS, etc.

(b): The Information Technology Act, 2000 amended by the Information Technology (Amendment) Act, 2008 with effect from 17.10.2009 has adequate provisions to deal with prevalent cyber crimes carried out by misusing electronic communication. Further, there exists a very close and effective coordination amongst intelligence agencies at the Center and the State levels. Intelligence inputs about possible designs and threats are shared with the State Governments concerned on a regular basis. The Multi

Agency Center (MAC) has been strengthened and re-organised to enable it to function on 24x7 basis for real time collation and sharing of intelligence with other intelligence agencies and security intelligence inputs are shared with the concerned States through the established mechanism, which ensures close coordination and sharing of intelligence and seamless flow of information between the States and the Central Security and Law Enforcement Agency. This has resulted in busting of terrorist modules.

(c) : The salient features of the legal, technical and administrative steps taken by the Government to effectively deal with the issue of cyber security in the country are as under:

(i) The "Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism" is in place.

(ii) Computer Security Policies, Standard Operating Procedures and Guidelines were formulated by the Government.

(iii) All Central Government Ministries/Departments and States/UTs have been advised to conduct security auditing of entire information technology infrastructure including websites periodically to discover gaps with respect to security practices and take appropriate corrective actions.

(iv) The Information Technology Act, 2000 as amended in 2008 provides legal framework to address the issues connected with security breaches of information technology infrastructure.

(v) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and counter measures on regular basis.