

Check on hate mails

*114. SHRI BAISHNAB PARIDA: Will the Minister of COMMUNICATION AND INFORMATION TECHNOLOGY be pleased to state:

- (a) the action plan to counter hate mails that are spreading fast in the country and had led to exodus of North-East people to their own region;
- (b) whether Government has worked out certain kind of strategy in the matter;
- (c) if so, the details thereof;
- (d) whether some of the threats relating to cyber terror had originated from across the border; and
- (e) if so, the details thereof?

THE MINISTER OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI KAPIL SIBAL): (a) to (c) The action plan and strategy of the Government to deal with the issue include the following:

- (i) Use of social media for dissemination of information on Government policies and programmes, as well as countering false information.
- (ii) Issuing advisory to all intermediaries including national and international social networking sites, advising them to take necessary action to disable inflammatory and hateful content hosted on their websites on priority basis.
- (iii) Maintaining regular dialogue with the intermediaries.
- (iv) Awareness campaign on the issue.
- (v) Use of existing legal provisions as contained in the Section 69A of the Information Technology Act 2000 to block such information for public access under certain circumstances.
- (vi) Using the provisions of Section 79 of the Information Technology Act 2000 to require the intermediaries to follow due diligence and guidelines with regard to malicious information hosted and posted on their infrastructure.

- (vii) Building/updating both legal and technical safeguards to prevent the misuse of Internet.

In addition, Government has notified a 'Framework and Guidelines' for use of Social Media by its agencies. It will help the Government to interact with the common citizens and disseminate information and at the same time effectively counter the spread of hate mails and malicious information.

(d) and (e) Cyber space by its very nature is borderless and anonymous. Anyone can exploit vulnerabilities in any system connected to the Internet and attack it from anywhere in the world without being identified. With the growing sophistication in technology, it is very difficult and challenging to positively attribute the origin of attack and to ascertain the identity of the perpetrator. As such, even though some of the cyber threats in the form of cyber attacks have been observed to be emanating from cyber space from across the border, conclusive attack attribution is very difficult.

Spectrum allocation

*115. SHRI D.P. TRIPATHI: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that Government has not taken any decision on spectrum allocation;

(b) if so, the reasons for the delay in this regard; and

(c) whether it is also a fact that Government would consider the grievances of operators and consumers while taking a decision thereon?

THE MINISTER OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI KAPIL SIBAL): (a) No, Sir. Government has taken decision on spectrum allocation.

(b) Pursuant to Supreme Court judgment dated 02-02-2012 Government has decided that administrative allotment of spectrum in the various categories *i.e.* [CMRTS, PMRTS, Commercial VSATs, Wide Area Paging service providers, All Captive users, which include Govt. Ministries/ Departments, PSU and Private users] be made, pending response of the Supreme Court on the Presidential Reference, in the following cases: