

**GOVERNMENT OF INDIA  
DEFENCE  
LOK SABHA**

UNSTARRED QUESTION NO:5452  
ANSWERED ON:13.12.2010  
CYBER WARFARE STRATEGY  
Tewari Shri Manish

**Will the Minister of DEFENCE be pleased to state:**

- (a) whether the Government has a Cyber Warfare strategy to deal with attempts to infiltrate and cripple the command, control and communication systems of the Defence Establishments of the three Services and other establishments under the Ministry and if so, the details thereof;
- (b) if so, whether the Government has a Cyber Warfare doctrine like the neighbouring countries to engage in asymmetric warfare given India's prowess in the software aspect of Information Technology (IT);
- (c) if so, whether there are rules of engagement that have been formulated internationally or multilaterally for engagement in cyber space/warfare;
- (d) the number of occasions when Information Technology networks of the Indian Defence Establishments were infected by the Stuxnet worm that caused havoc in Indonesia and Iran;
- (e) whether the failed launches of GSLV and Prithvi could be attributed to the presence of Stuxnet in ISRO and DRDO systems as Symantec reported that eight per cent of all Stuxnet infestations were reported from India; and
- (f) if so, the details of efficiency of firewall processes adopted by the Defence Establishments to protect their IT systems and the frequency with which the same is upgraded?

**Answer**

MINISTER OF DEFENCE (SHRI A.K. ANTONY)

(a) to (f): The Government has elaborate cyber security policies. Various organizations have prepared Cyber Crisis Management Plans for appropriate responses. No formal rules of engagement in cyber space/warfare exist at present at international or multilateral level. No Defence establishment has reported being effected by Stuxnet worm. Defence networks have adequate defensive measures which are upgraded as per Standard Operating Procedures.