# GOVERNMENT OF INDIA
# COMMUNICATIONS AND INFORMATION TECHNOLOGY
# LOK SABHA

UNSTARRED QUESTION NO:1398
ANSWERED ON:14.08.2013
CYBER ESPIONAGE
Abdulrahman Shri ;Gowda Shri D.B. Chandre;Ponnam Shri Prabhakar

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

(a) whether India has been prime target of some hostile nations including China for cyber espionage;

(b) if so, the details thereof and the reaction of the Government thereto;

(c) whether the Government has received any warning about the possible security threat posed by Huawei Technologies and other Chinese equipment makers; and

(d) if so, the details thereof and the reaction of the Government thereto along with the action taken thereon?

## Answer

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

(a) and (b): There have been attempts from time to time to penetrate cyber networks and systems operating in Government. These attacks have been observed to be directed 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.

The Government has taken several measures to detect and prevent cyber attacks. The details are:

i) Government has released the `National Cyber Security Policy - 2013` for public use and implementation with all relevant stakeholders. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

ii) The Government, industry and other organizations are regularly strengthening their Information Technology infrastructure by installing devices and security controls to protect their infrastructure from such attacks.

iii) All the Ministries/ Departments of Central Government and State Governments have been asked to implement the Crisis Management Plan to counter cyber attacks and cyber terrorism.

iv) The Government has circulated Computer Security Policy and Guidelines to all the Ministries /Departments on taking steps to prevent, detect and mitigate cyber attacks.

In addition, all state governments and UTs have been advised to implement appropriate security measures to prevent hacking of websites.

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

vi) The organizations operating critical information infrastructure are regularly advised to implement information security management practices based on International Standard ISO 27001. Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems.

vii) Cyber Security Mock Drills to assess preparedness of organizations to withstand cyber attacks are being conducted by the Government.

viii) The Government and industry are focusing on training their operations staff for protecting the infrastructure and handling incidents. The infrastructure w.r.t Cyber Forensics has been enhanced considerably.

(c) and (d): There have been reports in media and Government agencies of other countries raising concerns on vulnerabilities in the Telecom equipment manufactured by companies belonging to China. Measures for ensuring security and trustworthiness of equipment used in strategic sectors and Governments have been considered by way of formulation of appropriate polices and implementation of the same. Specific steps taken by Government in this regard are:

(i) The National Cyber Security Policy (NCSP) 2013 released on 2nd July 2013 provides for taking steps for reducing supply chain risks.

(ii) Department of Telecommunications in consultation with Ministry of Home Affairs and after due deliberations with Industry has issued comprehensive guidelines mandating Telecom Service Providers to secure their networks and inducting only those network elements into their Telecom Network, which have been tested as per relevant contemporary Indian or International Security Standards.

(iii) Standardisation, Testing and Quality Certification (STQC) Directorate has established ICT product security testing facility as per ISO/IEC 15408 standard in Kolkata. The testing infrastructure is being enhanced considerably both in Government and Private sector.