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

UNSTARRED QUESTION NO:4824
ANSWERED ON:26.04.2010
HACKING OF CLASSIFIED INFORMATION
Das Shri Bhakta Charan;Deora Shri Milind Murli;Gaddigoudar Shri P.C.;Lagadapati Shri Rajagopal;Ray Shri Rudramadhab ;Singh Shri Ganesh;Singh Shri Yashvir;Sivasami Shri C.

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

(a) Whether the Government is aware that Shadow Network, a Canadian Cyber Security has revealed that some foreign based hackers hacked defence, sensitive and classified information including India's missile systems, threatening the national security;

(b) if so, the details thereof; and

(c) the corrective action taken by the Government in this regard?

## Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI SACHIN PILOT)

(a) & (b): Yes, Sir. The Government is aware of report titled "Shadows in the Cloud − Investigating Cyber Espionage 2.0" published by the group of researchers from the Munk school of Global Affairs, University of Toronto, Canada.

An agency of the Government has been investigating such types of attacks by adversaries for some time. An investigation had already been launched into the matter prior to the reports that appeared in the media. The agency is working in close coordination with various agencies and service providers to identify reportedly affected computer systems, their locations and thereafter sanitizing them. The investigation will enable a comprehensive view on the subject to deal with the threats to be worked out.

(c): The Government has taken several measures to detect cyber attacks/hacking attempts.

1. As per existing computer security guidelines issued by Government, no sensitive information is to be stored on the systems that are connected to Internet.

2. The Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

3. The organizations operating critical information infrastructure have been advised to implement information security management practices based on International Standard ISO 27001.

4. Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems. CERT-IN has already empanelled a number of penetration testing professionals through a stringent mechanism of selection to carryout audits.

5. National Informatics Centre (NIC) is continuously strengthening the security of the network operated by them and its services by enforcing security policies, conducting regular security audits and deploying various technologies at different levels of the network to defend against the newer techniques being adopted by the hackers from time to time.

6. The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address the issues connected with hacking and security breaches of information technology infrastructure.

Section 70 of the Act provides to declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Further, Section 70B has empowered Indian Computer Emergency Response Team to serve as national nodal agency in the area of cyber security.

7. The Indian Computer Emergency Response Team (CERT-In) scans the Indian Cyber Space to detect traces of any untoward incident that poses a threat to the cyber space. CERT-In performs both proactive and reactive roles in computer security incidents prevention, identification of solution to security problems, analyzing product vulnerabilities, malicious codes, web defacements, open proxy servers and in carrying out relevant research and development.

Sectoral CERTs have been functioning in the areas of Defence and Finance for catering critical domains. They are equipped to handle and respond to domain specific threats emerging from the cyber systems.

CERT-In has published several Security Guidelines for safeguarding computer systems from hacking and these have been widely circulated. All Government Departments/ Ministries, their subordinate offices and public sector undertakings have been advised to implement these guidelines to secure their computer systems and information technology infrastructure.

CERT-In issues security alerts, advisories to prevent occurrence of cyber incidents and also conducts security workshops and training programs on regular basis to enhance user awareness.