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

(a) whether the Government has taken any step to control the rising trend of cyber attacks in the country;

(a) if so, the details of the steps taken in this regard;

(b) whether any study has been conducted to identify the cyber threats in the country; and

(c) if so, the details thereof ?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI K. J. ALPHONS)

(a) and (b): Government has taken various measures for preventing cyber attacks and enhancing the cyber security of information technology infrastructure in the country. These, inter alia, include:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers on regular basis. Security tips have been published to enable users to secure their Desktops and mobile/smart phones. Tailored alerts are sent to key organisations to enable them to detect and prevent cyber attacks.
ii. Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of section 70A of the Information Technology (IT) Act, 2000 for protection of critical information infrastructure in the country. NCIIPC has been regularly advising the critical information infrastructure (CII) sector organisation to reduce vulnerabilities to all kinds of threats and attacks, by sharing threat intelligence, guidelines, best practices and frameworks for protection and guiding them with policies and protection strategies. In addition, training and awareness programs are regularly conducted to improve the cyber hygiene in CII organisations.
iii. Government has formulated Cyber 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.
iv. Government has issued general guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
v. CERT-In has empanelled 67 security auditing organizations to support and audit implementation of Information Security Best Practices.
vi. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. In addition 3 drills were conducted in coordination with The Reserve Bank of India and The Institute for Development and Research in Banking Technology.

vii. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 22 training programs covering 610 participants were conducted during the year 2017.

viii. Government has initiated setting up of National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.

ix. Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

(c) and (d): In tune with the dynamic nature of Information Technology and limited window time available for an effective response, continuous efforts are required to be made to detect and prevent cyber attacks by way of continuous threat assessment and near real-time situational awareness. Such timely information enables coordinated actions by the stakeholders to take appropriate proactive and preventive actions. Concerted efforts are made to harvest the requisite information from multiple sources. These include incidents reported to and tracked by Indian Computer Emergency Response Team (CERT-In), technical measures, security cooperation arrangement with overseas Computer Emergency Response Teams (CERTs) and leading security product and service vendors as well as agencies within the Government.

****