GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2657

TO BE ANSWERED ON THE 09TH JULY, 2019/ ASHADHA 18, 1941 (SAKA)

RANKING IN CYBER CRIMES

2657. SHRI KUNWAR PUSHPENDRA SINGH CHANDEL:
DR. PRITAM GOPINATHRAO MUNDE:
SHRI GIRISH BHALCHANDRA BAPAT:
DR. SHRIKANT EKNATH SHINDE:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether India is ranked third after US and China in terms of cyber crime incidents;

(b) whether citizens have started relying more on digital transactions and corresponding features have shown an increase in cyber attacks;

(c) whether the Union Government does not have adequate in house capability/ expertise or inherent strength to deal with cyber crime/cyber attacks and if so, the reasons therefor;

(d) whether internet providing companies are not having their servers in India and if so, the steps taken by the Union Government in this regard;

(e) whether cyber crimes can be regulated if the servers of internet providing companies are installed in India; and

(f) if so, the steps taken by the Union Government to control the cyber crimes in the country and the success achieved so far?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI G. KISHAN REDDY)

(a): Any formal rankings about country-wise cyber crime incidents is not available.

(b) & (c): Use of digital transactions is on the rise globally, including India. Continuous efforts are made to secure data and protect systems and networks by deploying appropriate security controls and prevent cyber attacks.

Government has taken several steps to prevent and mitigate cyber security incidents. These include:

(i) Establishment of National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.

(ii) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

(iii) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes.

(iv) Issue of alerts and advisories regarding cyber threats and counter-measures by CERT-In.

(v) Issue of guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(vi) Provision for audit of the government websites and applications prior to their hosting, and thereafter at regular intervals.

(vii) Empanelment of security auditing organisations to support and audit implementation of Information Security Best Practices.

(viii) Formulation of Crisis Management Plan for countering cyber attacks and cyber terrorism.

(ix) Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

(x) Conducting 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.

(d): The internet service providing companies are governed by Licence Framework of Department of Telecommunications. The licencing conditions inter-alia may include setting up nodes i.e., Routers/ servers within the geographical limits of the service area for which the licence is obtained.

(e) & (f): Cyber crime can be committed even if servers of internet service providers are installed in India. However, legal provisions exist

under the Information Technology Act, 2000 for detection, investigation and prosecution of cyber crimes.

'Police' and 'Public Order' are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of law against the cyber crime offenders. However, Central Government has taken steps to spread awareness about cyber crimes, issue of alerts/advisories, capacity building/training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensics facilities etc. to prevent such crimes and to speed up investigation. The Government has launched the online cybercrime reporting portal, www.cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content. The Central Government has rolled out a scheme for establishment of Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

****