CYBER ATTACK DURING PANDEMIC

1742. SHRI VISHNU DAYAL RAM:

Will the Minister of Electronics and Information Technology be pleased to state:

    (a) whether incidents of cyber attacks have shown a rising trend during the COVID-19 pandemic and if so, the details thereof, State/UT-wise;

    (b) the budgetary provisions made, funds released and utilized by the Government to deal with the incidents of cyber attacks along with the status of the performance of Computer Emergency Response Team India (CERT-In) over the last three years?

    (c) the details of schemes/programmes launched by the Government for ensuring the protection of the cyberspace in the country;

    (d) whether the Government is satisfied with the achievements made by these said schemes and programmes and if so, the details thereof; and

    (e) if not, the proposed plan of action decided and timeline fixed by the Government for mitigating the alarming rise in cyber crimes in the country?

ANSWER

MINISTER OF STATES FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), 113334, 230223 and 353381 cyber security incidents are reported during January to March, April to June and July to August of year 2020 respectively indicating a rise in the cyber incidents during COVID-19 pandemic.

(b) and (c): The funds details for cyber security by Ministry of Electronics and Information Technology for last three financial years are as follows :

(Rs. Crore)

Year	Funds Released	Funds utilised
2017-18	86.48	78.62
2018-19	141.33	137.38
2019-20	135.75	122.04

The Indian Computer Emergency Response Team (CERT-In) is serving as national agency for responding to cyber security incidents as per provisions of Section 70B of Information Technology Act, 2000. CERT-In is operating 24X7 Incident Response Helpdesk. CERT-In has tracked, received reports and handled a total number of 53117, 208456, 394499 and 696938 cyber security

incidents during the year 2017, 2018, 2019 and 2020 (till August) respectively. Cyber security incidents such as phishing, Distributed Denial of Service attacks, Website intrusions, malware infections, vulnerable services and targeted attacks were handled by CERT-In through coordinated measures within and outside the country with concerned organisations, service providers, product and security companies, research institutions and academia, law enforcement agencies, international CERTs, regulators and stakeholders.

CERT-In has taken following measures to enhance the cyber security posture and prevent cyber-attacks in the country:

(i) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis. A total number of 276, 451, 444, 734 alerts and advisories were issued during the year 2017, 2018, 2019 and 2020 (till August) respectively. CERT-In issued 23 advisories on various topics such as Secure use of web conferencing software, Securing mobile devices and apps, Secure use of Virtual Private Network (VPN), Security Best Practices for Working from Home, security measures for Healthcare Sector, Online Safety of Children, various Phishing attack campaigns pretending to be from popular Apps and services, Securely managing Business Continuity during crisis situation due to COVID- 19 Pandemic etc. CERT-In also issued 37 advisories regarding securing digital payments, for users and institutions.

(ii) CERT-In is proactively collecting, correlating, contextualizing, analyzing and sharing tailored alerts with various organisations across sectors and stakeholders to enable active threat prevention.776 tailored alerts were shared with key organisations during 2017 to 2020 (till August)

(iii) CERT-In has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.

(iv) CERT-In is enabling formulation and implementation ofCyber 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.

(v) Cyber security mock drills are being conducted by CERT-In regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 49 such drills have so far been conducted by CERT-In where 434 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

(vi) Webcast for citizens and 4 Table top exercise during the outbreak of Wanna Cry ransomware for 70 critical and Government sector organisations were conducted to enable them to counter global WannaCry ransomware attack in June 2017.

(vii) 3 cyber crisis exercises were conducted for organizations during July and August 2020 to train and guide them to respond to COVID-19 pandemic related cyber-attacks wherein 72 organisations including key stakeholders participated.

(viii) CERT-In also participated in 10 international drills conducted by Asia Pacific CERT (APCERT), ASEAN Cyber Incident Drills, Organisation of Islamic Countries CERT (OIC CERT) during 2017 to 2020 (till August 2020). CERT-In took part in the bilateral India – United Kingdom cyber security exercise conducted by Chatham house in 2019. CERT-In is

also contributing as exercise coordinator for APCERT Drill Working Group. CERT-In participated in Quantum Dawn V exercise, conducted by Securities Industry and Financial Markets Association, which had 600 participants from over 180 financial institutions and government agencies from across the globe.

(ix) 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. A total number of 80 training programs covering 2535 participants from across sectors were conducted during 2017 to 2020 (till September).

(x) CERT-In imparts training for law enforcement agencies and judiciary through workshops organised on computer forensics and mobile device forensics through lectures, demonstrations and hands on practical sessions, which covers seizing, preservation, imaging and analysis of the data retrieved from the digital data storage devices. CERT-In also provides support to the other training institutes in imparting training by delivering lectures with demonstrations on various aspects of cyber forensics.

(xi) The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been operationalised by CERT-In in February 2017. The centre is providing detection of malicious programs and free tools to remove the same for citizens and organisations.

(xii) The National Cyber Coordination Centre (NCCC) is being implemented by CERT-In, 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.

(xiii) Cyber security cooperation arrangements in the form of Memorandum of Understanding (MoU) have been signed between CERT-In and its overseas counterpart agencies for collaborating and providing swift response to critical cyber incidents. At present, CERT-In has active MoUs with Australia, Bangladesh, Brazil, Estonia, Finland, Israel, Japan, Kingdom of Morocco, Seychelles, Singapore, South Korea, United Kingdom and Vietnam.

(xiv) CERT-In as convener is leading of two technical working groups across Asia Pacific CERTs namely "Internet of Things (IoT) Security" and "Secure Digital Payments".

(xv) CERT-In is participating and actively contributing as task force member in the Cyber Incident Management and Critical Information Protection working group of the Global Forum for Cyber Expertise (GFCE), a global platform for countries, international organisation and private companies to exchange best practices and expertise on cyber capacity building by identifying successful policies, practices and ideas so as to multiply these on a global level. CERT-In conducted a Table Top Exercise for 70 participants from across the African Union, developed and developing countries as well as the industry and academia in this multilateral global workshop in April 2019.

(xvi) CERT-In is participating and actively contributing as a member in the Financial Stability Board (FSB) Working Group on Cyber Incident Response and Recovery (CIRR), to develop guidance and policies related to cyber resilience and cyber security. The FSB was created by G20 to coordinate at the international level the work of national financial authorities and international standard setting bodies and to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies in the interest of financial stability.

(xvii) CERT-In was an observer at the North Atlantic Treaty Organization (NATO) "Cooperative Cyber Defense Centre of Excellence" organised Cyber Defense Exercise "Locked Shields

2018". Locked shields is the world's largest and most complex international technical cyber defense exercise.

(xviii) CERT-In is a contributing member of review group of the Second Security, Stability, and Resiliency (SSR2) of the Domain Name System (DNS) Review mandated by Internet Corporation for Assigned Names and Numbers (ICANN) to review effectiveness of the operational stability, reliability, resiliency, security and global interoperability of the internal/external systems/processes that affect the Internet's unique identifiers.

(xix) CERT-In has participated in meetings of United Nations Group of Governmental Experts (UNGGE) and Open Ended Working Group (OEWG), Internet Governance Forum (IGF) and the discussions under the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

(xx) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology (IT) Act, 2000.

(d) and (e) : Cyber space is ever evolving and dynamic and is a complex environment of people, software, hardware and services on the Internet. Protection of cyberspace is a continuous effort and Government is taking necessary measures for the same.

****