GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 5515
TO BE ANSWERED ON: 05.04.2023

INCIDENTS OF CYBER ATTACKS

5515. DR. NISHIKANT DUBEY:
SHRI MANOJ TIWARI:

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

(a) the year-wise number of cyber attacks on India's critical infrastructure from 2014 till date;
(b) whether the Government deems the current legal framework adequate to address the increase in the number of cyber attacks, especially in the light of recent security breaches;
(c) if so, the details thereof;
(d) whether the Government is planning to introduce a new targeted legislation to address the increase in cyber attack sand if so, the details thereof; and
(e) the details of the measures taken by the Government to set up requisite infrastructure and schemes to provide a greater security against cyber attacks in the country?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The Central Government, in exercise of its powers under section 70A of the Information Technology Act, 2000 ("IT Act"), has designated the National Critical Information Infrastructure Protection Centre (NCIIPC) as the national nodal agency in respect of Critical Information Infrastructure (CII) protection. Under the said section, NCIIPC is responsible for all measures relating to protection of CII. Further, section 70 of the IT Act provides that the appropriate Government may declare computer resource which directly or indirectly affect the facility of CII as a protected system. As per inputs given by NCIIPC, no cyber-attack has been reported to it in the computer resources declared to be a protected system.

(b) to (d): The IT Act penalises various offences relating to computer resources, including tampering with computer source documents (section 65), dishonestly or fraudulently damaging computer system (section 66), identity theft (section 66C), cheating by impersonation (section 66D), and cyber terrorism (section 66F). Further, under section 70, in respect of a protected system thereunder, the appropriate Government may, by order, authorise the persons authorised to access such system and any unauthorised access or an attempt to so access it is punishable with imprisonment of up to 10 years.

Furthermore,under section 70A, the functions and duties of NCIIPC have been prescribed by the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.These provide that NCIIPC shall protect and deliver advice aimed at reducing the vulnerabilities of CII, against cyber-terrorism, cyber-warfare and other threats; provide strategic leadership and coherence across Government to respond to cybersecurity threats against identified CII; coordinate, share, monitor, collect, analyse and forecast national-level threats to CII for policy guidance, expertise-sharing and situational awareness for early warning or alerts; assist in development of appropriate plans, adoption of standards, sharing of best practices and refinement of procurement processes in respect of CII protection; evolve protection strategies, policies, vulnerability assessment and auditing methodologies for CII protection; and issue guidelines, advisories and vulnerability/audit notes relating to CII protection and practices, procedures, prevention and response.

In addition, under section 70 of the IT Act, the practices and procedures for protected system have been prescribed bythe Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018. These provide that the organisation having the protected system shall constitute an Information Security Steering Committee, nominate a Chief Information Security Officer, establish an Information Security Management System, ensure documentation as specified in the rules, carry out vulnerability/threat/risk analysis, prepare a Cyber Crisis Management Plan, conduct periodic Information Security audits, establish a Cyber Security Operation Centre and a Network Operation Centre, and take regular backup of logs.

In addition to the above, under section 70B of the IT Act, the Indian Computer Emergency Response Team (CERT-In) has been appointed as the national agency for incident response and, further, under section 69B,in order to enhance cybersecurity and identify, analyse and prevent intrusion or spread of computer contaminant in the country, it has been authorised to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. Under section 70 of the IT Act, its functions, responsibilities and services have been prescribed by the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. These provide that CERT-In shall function as the trusted referral agency for cyber users in India for responding to cybersecurity incidents and shall assist them in implementing measures to reduce the risk of such incidents. They also provide that CERT-In shall provide the services of response to and prediction, prevention, analysis and forensics of cybersecurity incidents; information security assurance and audit; cybersecurity awareness and technology exposition; training or upgrade of technical knowhow; and scanning of cyberspace with respect to cybersecurity vulnerabilities, breaches and malicious activities.

Section 70B of the IT Act also empowers CERT-In to give directions to the service providers, intermediaries, data centres, body corporate and any other person for carrying out its functions, in exercise of which CERT-In issues, from time to time, suitable directions to address cybersecurity concerns.

To help achieve Government's aim of ensuring an Open, Safe and Trusted and Accountable Internet for its users, the Ministry of Electronics and Information Technology engages with and receives inputs from the public and stakeholders, including in respect of changes required to existing legislation and the need to introduce fresh legislation. Such engagement includes all aspects of law, including addressing cybersecurity concerns. Once a legislative proposal is formulated, in accordance with the Government's policy on pre-legislative consultation and the procedure detailed in the Manual of Parliamentary Procedures published by the Ministry of Parliamentary Affairs, proposed legislation is published in the public domain for feedback/comments from the public, the Ministry of Law and Justice consulted thereon, approval of the Cabinet obtained, and notice of the motion for introduction of a Bill given to the Secretariat of relevant House of Parliament. The said procedure is observed in respect of introduction of any new legislation, including legislation to address cybersecurity concerns. No notice has been given for introduction of new legislation to target cyber-attacks.

(e): The details of the measures taken to set up requisite infrastructure and schemes to provide greater security against cyber-attacks in the country are as under:

(i) The National Cyber Security Coordinator under the National Security Council Secretariat coordinates with different agencies at the national level for cybersecurity matters.

(ii) NCIIPC provides near real-time threatintelligence and situational awareness, based on which regular alerts and advisories are sent to CII and protected system entities.

(iii) The National Cyber Coordination Centre,established under a multi-stakeholder project implemented by CERT-In, scans the cyberspace in the country on the metadata level to generate near-real-time macroscopic views of cybersecurity threats. It provides a structured system and facilitates coordination among different agencies by sharing with them the metadata for taking actions to mitigate cybersecurity threats.

(iv) CERT-In operates the Cyber Swachhta Kendra, a botnet cleaning and malware analysis centre. The centre provides detection of malicious programs and free tools to remove the same.

(v) CERT-In operates an automated cyber-threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(vi) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.

(vii) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of information security best practices.

(viii) Government websites and applications are audited with respect to cybersecurity prior to hosting. Their audit is conducted after hosting as well.

(ix) Government has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber-terrorism for implementation by all Ministries/ Departments of the Central Government, State Governments and their organisations and critical sectors.

(x) Cybersecurity mock drills are conducted on an ongoing basis to enable assessment of the cybersecurity posture and preparedness of organisations in the government and critical sectors. 74 such drills have so far been conducted by CERT-In, in which990 organisations from different States and sectors participated.

(xi) CERT-In,from time to time, conductsworkshops for Ministries, Departments, States and organisations to sensitise them about the cybersecurity threat landscape and enable them to prepare and implement CCMP. 150such workshops have been held till February 2023.

(xii) Government has issued guidelines regarding the key roles and responsibilities of Chief Information Security Officers (CISOs) for securing applications and infrastructure and cybersecurity compliance.

(xiii) CERT-In conducts training programmes on an ongoing basis for network and system administrators and CISOs of government and critical sector organisations on securing the information technology infrastructure and mitigating cyber-attacks. A total of 192 training programmes, covering 16,922 participants, were conducted during the period from January 2014 to February 2023.

(xiv) CERT-In co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as law enforcement agencies.

****