35% of Cyber Attacks on Indian Sites from China

The Indian Computer Emergency Response Team (CERT-In) has submitted its report to the National Security Council Secretariat (NSCS) and other security agencies on the basis of its analysis of cyber attacks from April-June 2018.

Key Highlights

- **Cyber attacks from China**: The maximum number of cyber attacks on official Indian websites are from China followed by the US and Russia. The cyber attacks from China made up 35% of the total number of cyber attacks on official Indian websites, followed by US (17%), Russia (15%), Pakistan (9%), Canada (7%) and Germany (5%).
- **Attacks from Pakistan**: It has been observed that intruding activities are coming from Canadian and German cyberspace — most possibly suspected to have originated from Pakistan to target Indian websites.
- Many of the **institutions impacted by the malicious activities have been identified** and advised to take appropriate preventive action. These include Oil and Natural Gas Corporation (ONGC), National Informatics Centre (NIC), Indian Railway Catering and Tourism Corporation (IRCTC), Railways, Centre for Railway Information Systems (CRIS) and some banks like Punjab National Bank, Oriental Bank of Commerce, State Bank of India and state data centres, particularly in Maharashtra, Madhya Pradesh and Karnataka.
- The cyber **attacks are usually in the form of a trusted source** where they ask for personal details such as bank details, personal details, passwords. They are targeted by sending phishing emails with malware attachments.

Computer Emergency Response Team - India (CERT-IN)

- It is an organisation of the Ministry of Electronics and Information Technology, Government of India, with the objective of securing Indian cyberspace.
- It is the nodal agency which deals with cybersecurity threats like hacking and phishing.
- It collects, analyses and disseminates information on cyber incidents, and also issues alert on cybersecurity incidents.
- CERT-IN provides Incident Prevention and Response Services as well as Security Quality Management Services.

Some important government initiatives for cyberspace security

- National Cyber Security Policy, 2013: The Policy is aimed at building a secure and resilient cyberspace for citizens, businesses and the Government. Its mission is to protect cyberspace information and infrastructure, build capabilities to prevent and respond to cyber attacks, and minimise damages through coordinated efforts of institutional structures, people, processes, and technology.
- Cyber Swachhta Kendra’ (Botnet Cleaning and Malware Analysis Centre): To combat cyber security violations and prevent their increase,Government of India’s Computer Emergency Response Team (CERT-in) in 2017 launched ‘Cyber Swachhta Kendra’ (Botnet Cleaning and Malware Analysis

Centre) a new desktop and mobile security solution for cyber security in India.

- Creating mechanisms for security threats and responses to the same through national systems and processes. National Computer Emergency Response Team (CERT-in) functions as the nodal agency for the coordination of all cybersecurity efforts, emergency responses, and crisis management.
- In 2014, the Prime Minister's Office created the position of the National Cyber Security Coordinator. National Critical Information Infrastructure Protection Centre (NCIIPC) is an organisation of the Government of India created under Section 70A of the Information Technology Act, 2000 (amended in 2008).