3. Zoom not a Safe Platform, Says MHA

Prelims Syllabus: Cyber Space Challenges

Mains Syllabus: GS-III Awareness in the fields of IT, Space, Computers, robotics, Nano technology, Bio-Technology and Issues Relating to Intellectual Property Rights.

Why in News?

- Recently, the Ministry of Home Affairs (MHA) has issued an advisory that Zoom video conference is not a safe platform.

What is the Issue?

- Zoom has seen an exponential rise in usage in India as office-goers remain at home due to the lockdown, imposed to curb the Covid-19 pandemic.
- Over 90,000 schools across 20 countries have started using it regularly.
- The maximum number of daily meeting participants of approximately 10 million at the end of December 2019 grew to more than 200 million daily meeting participants in March.
- It has been used extensively by everyone including the central and state ministers for official purposes and Conducting Meetings.

About Zoom:

- Zoom is a US-based video communication and videoconferencing platform.
- This Silicon Valley-based company appears to own three companies in China through which at least 700 employees were paid to develop Zoom's software.
- This arrangement is apparently an effort at labour arbitrage in which Zoom can avoid paying US wages while selling to US customers, thus increasing their profit margin.
- However, this arrangement may make Zoom responsive to pressure from Chinese authorities. Reportedly, few calls made through the app are routed through servers in China.

Cautions made by CERT-IN:

- Earlier, the **Computer Emergency Response Team, India (CERT-In)** had also issued advisories cautioning on the use of Zoom for office meetings.
  - ✓ CERT-IN 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 cyber security threats like hacking and phishing.
  - ✓ It collects, analyses and disseminates information on cyber incidents, and also issues alerts on cyber security incidents.

- ✓ CERT-IN provides Incident Prevention and Response Services as well as Security Quality Management Services.

- It warned that the insecure usage of the platform may allow cyber criminals to access sensitive information such as meeting details and conversations giving rise to cyber frauds.
- It also highlighted multiple vulnerabilities which could allow an attacker to gain elevated privileges or obtain sensitive information.

Why Zoom is Not Safe?

- Citizen Lab, based at the University of Toronto, found significant weakness in Zoom's encryption that protects meetings.
- It identified the transmission of meeting encryption keys through China.
- The lab has raised two primary concerns- **geo-fencing** and **Meeting Encryption**.
  - ✓ **Geo-fencing** is a location-based service in which an app or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a geo-fence.

What is the Response from Zoom?

- Zoom Founder and CEO Eric S Yuan has apologised and assured the people that the privacy and security expectations would be taken care of.
- Zoom has added additional features such as placing a new security icon in the meeting controls, changing Zoom's default settings and enhancing meeting password complexity, among others.
- It has also added that soon, account admins will have the ability to choose whether or not their data is routed through specific Data Center Regions.

Suggestions given by the Ministry:

- The users are suggested to set strong passwords and enable "waiting room" features so that call managers could have better control over the participants.
- Users should also avoid using personal meeting ID to host events and instead use randomly generated meeting IDs for each event.
- People using the app should not share meeting links on Public platforms.

Who deals with Cyber-crime Issues in India?

- **Indian Cyber Crime Coordination Centre (I4C):**
  - ✓ The scheme to set up I4C was approved in October 2018, to deal with all types of cybercrimes in a comprehensive and coordinated manner.
  - ✓ **It has Seven Components:**
    1. National Cyber Crime Threat Analytics Unit
    2. National Cyber Crime Reporting Portal
    3. National Cyber Crime Training Centre
    4. Cyber Crime Ecosystem Management Unit
    5. National Cyber Crime Research and Innovation Centre
    6. National Cyber Crime Forensic Laboratory Ecosystem
    7. Platform for Joint Cyber Crime Investigation Team.
- Various States and Union Territories (UTs) have consented to set up Regional Cyber Crime **Coordination Centres.**
- This state-of-the-art Centre is located in New Delhi.