

6. Cyber-attacks on Health Care Institutions

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?

- The **International Criminal Police Organisation (Interpol)** has warned member countries that cybercriminals are attempting to target major hospitals and other institutions on the front lines of the fight against COVID-19 with ransomware.

About International Criminal Police Organization (INTERPOL):

- Interpol is an intergovernmental organization that helps coordinate the police force of 194 member countries.
- Each of the member countries hosts an Interpol National Central Bureau (NCB). This connects their national law enforcement with other countries and with the General Secretariat.
 - ✓ The Central Bureau of Investigation (CBI) is designated as the National Central Bureau of India.
 - ✓ The General Secretariat provides a range of expertise and services to the member countries.
- It is headquartered in Lyon, France**
- Interpol Notices are international requests for cooperation or alerts allowing police in member countries to share critic.



Key Points:

- In an alert sent to 194 nations, including India, Interpol said that the hospitals and institutions had become targets of ransomware attacks.
- Interpol's Cybercrime Threat Response Team had detected an increase in the number of attempted ransomware attacks against key organisations and infrastructure engaged in the virus response.
- Cybercriminals are using ransomware to hold hospitals and medical services digitally hostage, preventing them from accessing vital files and systems until a ransom is paid.
 - ✓ The attacks were designed to lock these institutions out of their critical systems in an attempt to extort payments.
 - ✓ Locking hospitals out of their critical system will delay the swift medical response required during these unprecedented times and it could also directly lead to deaths.
- The ransomware appears to be spreading primarily via e-mails, often falsely claiming to contain information or advice regarding the coronavirus from a government agency, which encourages the recipient to click on an infected link or attachment.
- Prevention and Mitigation efforts are crucial to stopping the attacks.
 - ✓ Interpol continues to stand by its member countries and provide any assistance necessary to ensure vital healthcare systems remain untouched and the criminals targeting them held accountable.
 - ✓ Interpol also issued a Purple Notice to seek or provide information on modus operandi, objects, devices and concealment methods used by criminals.

Changed Pattern of Crimes:

- Interpol warned that with a majority of people working from home due to the pandemic, there was a change in the pattern of crimes.
- Following is the change
 - ✓ Fraudulent trade in personal protective equipment and anti-viral medicines,
 - ✓ Individuals/businesses on reduced income becoming potential targets of loan sharks (Persons who loan money at extremely high interest rates and often use threats of violence to collect debts).
 - ✓ The lockdown period has made business establishments/factories vulnerable to thefts.
 - ✓ Since more people were at home, the number of burglaries had dropped. But thieves are increasingly targeting factories or business premises that were locked.

-
- Domestic violence cases have risen since the start of coronavirus-related quarantines, with reports showing women and children at greater risk of abuse.
 - Recent weeks have seen increased online activity by paedophiles (persons who are sexually attracted to children) seeking child sexual abuse material.
 - ✓ This is being intensified by a shortage of moderators who identify and remove offensive material from networks.

Steps Taken by the Government:

- Alerts received by the Government of India on the threat of ransomware/malware attacks have been communicated to the concerned departments.
- Institutions and individuals have been appealed not to open any mail or link on coronavirus data or home remedies unless it is from a trusted source like a government agency.
 - ✓ They were also cautioned about a possibility of e-mail spoofing, where a suspect operating from a remote location would send a mail that would appear as if it came from a known person.

