Cyber Slavery

Why in news?

Over 5,000 Indians have been trapped and forced to commit cyber frauds, with victims in India losing approximately Rs 500 crore in the last six months.

What is cyber slavery?

- It is also known as digital slavery is an *organized crime* which refers to the practice of exploiting individuals through digital means for labor or other purposes, often under coercive or deceptive conditions.
- While traditional forms of slavery involve physical captivity, cyber slavery occurs in the virtual realm, where individuals are manipulated, controlled, and exploited through various online channels.
- **Coercion-** Cyber slavery involves coercing or deceiving individuals into exploitative situations, it includes false promises of employment, threats, manipulation, or other forms of coercion to compel individuals to perform certain tasks or activities.
- **Online exploitation**- It typically involves the use of digital platforms, technology, and communication channels for exploitation.
- **Virtual captivity**- While individuals may not be physically confined, they may be effectively held captive through digital means. For example, their personal information, financial assets, or reputation may be controlled or threatened, making it difficult for them to escape or seek help.
- **Global presence**- Cyber slavery is not confined by geographical boundaries and can occur on a global scale, perpetrators may operate from different countries, targeting vulnerable individuals worldwide through the internet.
- **Diverse forms**- Cyber slavery can manifest in various forms, including but not limited to forced labour in *online scams*, coerced participation in cybercrime activities, exploitation in the digital gig economy, or involuntary servitude through online platforms.

What is the recent issue of cyber slavery in Cambodia?

- Over 5,000 Indians are reported to be trapped in Cambodia, where they are allegedly being coerced into carrying out cyber frauds.
- Individuals are lured to Cambodia under false pretenses, often promised data entry jobs. However, upon arrival, they are forced to engage in cyber fraud activities, including posing as law enforcement officials or using fake social media profiles to scam people.
- The scams involve various tactics, including posing as women on dating apps to convince targets to invest in cryptocurrency trading or fake stock investments.
- The Indian government, particularly the *Ministry of Home Affairs (MHA),* is actively

engaged in addressing the issue, they have held meetings with various ministries and security experts to devise a strategy for rescuing those trapped in Cambodia.
- Law enforcement agencies, such as the Rourkela Police in Odisha, have taken actions against cyber-crime syndicates involved in this scam. They have made arrests and are coordinating with immigration authorities to detain suspects attempting to return from Cambodia.
- Some individuals have been successfully rescued with the help of government agencies and organizations like the Non-Resident Indian Forum of the Government of Karnataka (NRIFK).
- Authorities are considering seeking assistance from Interpol to arrest key players involved in the scam.

What are the challenges in cyber slavery?

- **Challenges in detection**- Cyber slavery operates in the digital shadows, making it difficult to track down perpetrators, their anonymity allows them to hide behind pseudonyms, encrypted communication channels, and virtual private networks (VPNs).
- **Jurisdictional challenges-** The internet transcends national borders, complicating legal jurisdiction. Perpetrators can operate from one country while victimizing individuals in another.
- **Pseudonymity**- Perpetrators often use fake identities, making it challenging to identify and trace them.
- **Ephemeral evidence**- Digital evidence can vanish quickly due to data deletion, encryption, or rapid changes in online platforms.
- **Resource constraints**- Law enforcement agencies face resource limitations, both in terms of personnel and technology.

What lies ahead?

- *Raising awareness* about cyber slavery is crucial, it can be done through public campaigns, educational programs and media coverage can inform people about the risks and signs of exploitation.
- Governments must enact and enforce *robust legislation* specifically targeting cyber slavery, these laws should cover both domestic and international cases, addressing jurisdictional challenges.
- The need of the hour is *international cooperation* it can be facilitated through Mutual legal assistance treaties (MLATs) that fosters information sharing, extradition, and joint investigations.
- The *victims should be empowered* through establishing helplines, counselling services, safe spaces etc., this would make them come forward.
- Technology companies should adopt *ethical supply chain practices*, ensuring their products and services are not inadvertently linked to cyber slavery.

Quick facts

Steps taken by India to combat cyber attacks

• **Indian Computer Emergency Team (CERT- In)-** It is operational since 2004, it collects, analyses, and disseminates information on cyber incidents.
• **National Cyber Security Coordinator** -It is under the National Security Council Secretariat, it coordinates with different agencies at the national level on cybersecurity issues.
• **National Critical Information Infrastructure Protection Centre** - It has been set up for the protection of national critical information infrastructure.
• **Cyber Swachhta Kendra** - It is a Botnet Cleaning and Malware Analysis Centre that has been launched for detection of malicious software programmes and to provide free tools to remove them.
• **Indian Cyber Crime Coordination Centre (I4C)-** It is an initiative of the Ministry of Home Affairs (MHA) to combat cyber-crime in the country.
• **Cyber Crisis Management Plan** - It has been formulated by the government to counter cyber-attacks
• **Cyber Surakshit Bharat**- It aims to ensure awareness about cybercrime and adequate safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
• **Cyberdome**- It is Kerala State police department's premier facility dedicated to prevent cybercrime and mitigate security threats to the State's critical information infrastructure.

References

1. Indian Express- Cyber slavery in Cambodia
2. PIB- Steps to deal with cyber-crime and cyber security

SHANKAR IAS PARLIAMENT
Information is Empowering