MIND STROM

QUALITY MIND MAPS ON
IMPORTANT TOPICS FOR UPSC CSE.
For more, Visit on www.pmias.in

PM IAS

PMIAS
be inspired

CYBER SECURITY & DISINFORMATION

- Cyber security focuses on protecting and defending the networks and our digital life.
- Disinformation is similar to the attack & compromise of our cognitive being.
- It can create social discord, increase polarisation, and can influence the election results.

THE ATTACKS

- major targeting areas are critical infrastructure nationally important establishments.
- Cyberattacks are aimed at computer infrastructure while disinformation exploits our inherent cognitive biases and logical fallacies.
- Cybersecurity attacks are executed using malware,viruses, trojans, botnets, and social engineering
- Disinformation attacks use manipulated, mis contextualised, misappropriated information, deep fakes, and cheap fakes.
- Despite of various counter measures to protect and defend the attacks, the issues persist.
- The lack of coordination between teams leaves a huge gap that is exploited by malicious actors.
- For example, QAnon spread false messages claiming that the U.S. 2020 presidential election was fraudulent, and conspiracy theorists burned down 5G towers because they believed it caused the novel coronavirus pandemic.
- COVID-19 disinformation campaigns have prevented people from wearing masks, and not getting vaccinated.
- A well-coordinated disinformation campaign fills broadcast and social channels with so much false information and noise, and thus drowning the truth.
- Balancing the rights of speech with the dangers of disinformation is a challenge for policymakers and regulators.

COGNITIVE HACKING

- Meaning: Cognitive hacking is a threat from disinformation.
- It attempts to change the target audience's thoughts and actions, galvanise societies and disrupt harmony using misinformation.
- The goal is to manipulate the way people perceive reality.
- The storming of the U.S. Capitol on January 6, 2021, is a prime example of the effects of cognitive hacking.
- The implications of cognitive hacking are more devastating than cyberattacks on critical infrastructure.
- Revolutions throughout history have used cognitive hacking techniques to overthrow governments and change society.

WAY FORWARD

- We must develop disinformation defence systems by studying strategy and tactics to understand the activities and behaviours of malicious attacks.
- By treating disinformation as a cybersecurity threat, we can find effective countermeasures to cognitive hacking.
- Information sharing will help disinformation countermeasures to scale better and respond quickly.
- Technology industry, civil society and the government should coordinate to make users aware of cyber threat vectors such as phishing, viruses, and malware.
- The industry with public-private partnerships must also invest in media literacy efforts to reach out to discerning public.
- It is time that cybersecurity as a specialised discipline becomes an integral component of any IT syllabus being taught within our university systems as well as outside.