Deepfake Technology

written by iasexam.com | 21/12/2022

Topic- Internal Security [GS Paper-3]

Context- The Cyberspace Administration of China is rolling out new regulations to restrict the use of deep synthesis technology and curb disinformation.

Key Highlights

- The policy needs deep synthesis service providers and users to ensure that any doctored content using the technology is explicitly labelled and can be traced back to its source.

Deep Synthesis

- Deep synthesis is defined as the use of technologies, which includes deep learning and augmented reality, to generate text, images, audio and video to create virtual scenes.
- One of the scandalous applications of the technology is deep fakes, where synthetic media is used to swap the face or voice of one person for another.
- Deepfakes are getting difficult to detect with the advancement of technology.

Deepfake Technology

- Deepfake technology is a method used for manipulating videos, images, audios utilizing powerful computers and deep learning.
- The technology is particularly used to generate fake news and commit financial fraud among other wrong doings.

- It overlays a digital composite over an already-existing video, picture, or audio; which is further used by the cybercriminals as Artificial Intelligence technology.

Origin of the Term

- The word deepfake originated in 2017, when an anonymous Reddit user called himself “Deepfakes.”
- This Reddit user manipulated Google’s open-source, deep-learning technology to create and post pornographic videos.

Misuse of the technology

- Deepfake technology is now being used for unethical purposes like scams and hoaxes, celebrity pornography, election manipulation, social engineering, automated disinformation attacks, identity theft and financial fraud etc.
- The technology has been used to impersonate notable personalities like former U.S. Presidents Barack Obama and Donald Trump, India’s Prime Minister Narendra Modi, etc.

Measures by other Countries to Combat Deepfakes

- **European Union:**
    - The EU has an updated Code of Practice to stop the spread of disinformation through deepfakes.
    - The revised Code needs tech companies including Google, Meta, and Twitter to take measures in countering deepfakes and fake accounts on their platforms.
    - They have six months to implement their preventive measures once they have signed up to the Code.
    - If found non-compliant, these companies have to face fines as much as 6% of their annual global turnover, according to the updated Code.
    - The Code of Practice on Disinformation, introduced in 2018 brought together for the first-time worldwide industry players to commit to counter disinformation.
- **United States**:
    - The U.S. introduced the bipartisan Deepfake task Force Act in order to assist the Department of Homeland Security (DHS) to counter deepfake technology.
    - The measure directs the DHS to conduct an annual study of deepfakes, assess the technology used, track its uses by foreign and domestic entities, and come up with available countermeasures to tackle the issue.
- California and Texas have also passed laws that criminalize the publishing and distributing of deepfake videos that intend to influence the outcome of an election. The law in Virginia imposes criminal penalties on the distribution of nonconsensual deepfake pornography.
- **India**:
    - In India, however, there are no such legal framework against using deepfake technology.
    - However, certain specific laws can be addressed for misusing the tech, which include Copyright Violation, Defamation and cyber felonies.

Way forward

- As media consumers, we need to be able to decipher, understand, translate, and use the information we encounter.
- The best method to deal with this issue is with technical solutions supported by artificial intelligence that can recognize and block deep fakes.
- Prior to resolving the issues associated with deep fakes, media literacy needs to be improved.
- There is also a need for easy-to-use and accessible technology solutions for detecting deep fakes, authenticate media, and amplify authoritative sources.
- On the part of society, to counter the menace of deep fakes, there is a need to take the responsibility to be a critical consumer of media on the Internet, think and pause before sharing on social media, and it can be part of the solution.