Mains Practice Question

Q. Deepfakes present an opportunity to the cyber-criminal and a challenge to everyone else. Discuss (250 words)

28 Dec, 2022 GS Paper 3 Internal Security

Approach

- Start your answer by briefly explaining deep fake technology.
- Discuss its challenges of deepfake technology.
- Suggest some measures to overcome challenges of deepfake technology.
- Conclude accordingly.

Introduction

- Deepfake technology is a method for manipulating videos, images, audios utilizing powerful computers and deep learning.
- It is 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; cybercriminals use Artificial Intelligence technology.

Body

- Deepfake technology is now being used for nefarious purposes like scams and hoaxes, celebrity pornography, election manipulation, social engineering, automated disinformation attacks, identity theft and financial fraud etc.
- **Challenges of Deepfake Technology:**
    - **Cyber Crime:**
        - The potential use of deepfakes is in phishing campaigns, as it would make them more difficult for the individual to detect as a scam.
        - For example, in social media phishing, a faked video of a celebrity could be used to extort money from unwitting victims.
    - **Fabricated Media:**
        - Deep Fake technology makes it possible to fabricate media like swap faces, lip-syncing, and puppeteers, mostly without consent and bring threat to psychology, security, political stability, and business disruption.
        - Deepfake 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.
    - **New Front of Warfare:**
        - A deepfake could act as a powerful tool by a nation-state to undermine public safety and create uncertainty and chaos in the target country.
        - Nation-state actors with geopolitical aspirations, ideological believers, violent extremists, and economically motivated enterprises can manipulate media narratives using deepfakes.
        - It can be used by insurgent groups and terrorist organisations, to represent their adversaries as making inflammatory speeches or engaging in provocative actions to

stir up anti-state sentiments among people.

- **Undermining Democracy:**
  - A deepfake can also aid in altering the democratic discourse and undermine trust in institutions and impair diplomacy.
  - False information about institutions, public policy, and politicians powered by a deepfake can be exploited to spin the story and manipulate belief.
- **Disrupting Electioneering:**
  - A deepfake of a political candidate can sabotage their image and reputation. A well-executed one, a few days before polling, of a political candidate spewing out racial epithets or indulging in an unethical act can damage their campaign.
  - A high-quality deepfake can inject compelling false information that can cast a shadow of illegitimacy over the voting process and election results.
  - Leaders can also use them to increase populism and consolidate power.
  - Deepfakes can become a very effective tool to sow the seeds of polarization, amplifying division in society, and suppressing dissent.

- **Measures to Overcome Challenges of Deepfake Technology:**
  - **Enhancing Media Literacy:** Media literacy for consumers and journalists is the most effective tool to combat disinformation and deep fakes.
    - Improving media literacy is a precursor to addressing the challenges presented by deepfakes.
    - Media literacy efforts must be enhanced to cultivate a discerning public.
    - As consumers of media, they must have the ability to decipher, understand, translate, and use the information.
    - Even a short intervention with media understanding, learning the motivations and context, can lessen the damage.
  - **Need for Regulation:** Meaningful regulations with a collaborative discussion with the technology industry, civil society, and policymakers can facilitate disincentivizing the creation and distribution of malicious deep fakes.
  - **Technological Interventions:** There is also a need for easy-to-use and accessible technology solutions to detect deep fakes, authenticate media, and amplify authoritative sources.
  - **Behavioural Change:** 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 be part of the solution to this infodemic.

Conclusion

- As media consumers, we must be able to decipher, understand, translate, and use the information we encounter.
- The best method to deal with this problem 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 has to be improved.
- There is a need to create cyber arm, which would work on to tackle these types of new and emerging threats.
- There is also a need for easy-to-use and accessible technology solutions to detect 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 be part of the solution.

PDF Refernece URL: https://www.drishtiias.com/mains-practice-question/question-1509/pnt