IAS GS World PCS
Committed To Excellence

exclusive Editorial Simplified

02 January 2023

The Danger of Deepfakes:

Digital Media can use AI to Influence people's lives and their Public Discourse

The Hindu

Paper - III
(Sci. & Tech.)

How is it employed by various groups and how can society overcome the 'infodemic'?

Disinformation and hoaxes have evolved from mere annoyance to warfare that can create social discord, increase polarisation, and in some cases, even influence the election outcome. Nation-state actors with geopolitical aspirations, ideological believers, violent extremists, and economically motivated enterprises can manipulate social media narratives with easy and unprecedented reach and scale. The disinformation threat has a new tool in the form of deepfakes.

What Are Deepfakes?

Deepfakes are digital media - video, audio, and images edited and manipulated using Artificial Intelligence. It is basically hyper-realistic digital falsification. Deepfakes are created to inflict harm on individuals and institutions. Access to commodity cloud computing, public research AI algorithms, and abundant data and availability of vast media have created a perfect storm to democratise the creation and manipulation of media. This synthetic media content is referred to as deepfakes.

Artificial Intelligence (AI)-Generated Synthetic media or deepfakes have clear benefits in certain areas, such as accessibility, education, film production, criminal forensics, and artistic expression. However, as access to synthetic media technology increases, so does the risk of exploitation. Deepfakes can be used to damage reputation, fabricate evidence, defraud the

Why In News

China's cyberspace administration, the cyberspace watchdog, is drawing up new rules to restrict the use of deep synthesis technology and curb misinformation.

Deep Fake based on Artificial Intelligence (AI)

- ➥ Deep Fake is a more advanced and dangerous form of fake news. It has emerged as a new option to spread misinformation and rumours. Normal fake news can be checked in many ways, whereas it is very difficult for a common man to identify deep fake.
- ➥ Deep Fake is a combination of 'Deep Learning' and 'Fake', in this, using Artificial Intelligence (AI), a fake copy of a media file such as picture, audio and video is created, which looks and sounds like the original file. does.
- ➥ The issue of deep fakes first came to light in the year 2017 when an account named 'Deep Fake' on the social media site 'Reddit' posted objectionable deep fake photos of several celebrities by one of its users. Since this incident, many other cases of deep fakes have also come to light.

public, and undermine trust in democratic institutions. All this can be achieved with fewer resources, with scale and speed, and even micro¬targeted to galvanise support.

Who Are The Victims?

The first case of malicious use of deepfake was detected in pornography. According to a sensity.ai, 96% of deepfakes are pornographic videos, with over 135 million views on pornographic websites alone. Deepfake pornography exclusively targets women. Pornographic deepfakes can threaten, intimidate, and inflict psychological harm. It reduces women to sexual objects causing emotional distress, and in some cases, lead to financial loss and collateral consequences like job loss.

Deepfake can depict a person as indulging in antisocial behaviors and saying vile things that they never did. Even if the victim could debunk the fake via alibi or otherwise, that fix may come too late to remedy the initial harm. Deepfakes can also cause short¬term and long¬term social harm and accelerate the already declining trust in traditional media. Such rosion can contribute to a culture of factual relativism, fraying the increasingly strained civil society fabric. Deepfake could act as a powerful tool by a malicious nation¬state to undermine public safety and create uncertainty and chaos in the target country. Deepfakes can undermine trust in institutions and diplomacy.

Deepfakes can be used by non¬state actors, such as insurgent groups and terrorist organisations, to show their adversaries as making inflammatory speeches or engaging in provocative actions to stir antistate sentiments among people. Another concern from deepfakes is the liar's dividend; an undesirable truth is dismissed as deepfake or fake news. The mere existence of deepfakes gives more credibility to denials. Leaders may weaponise deepfakes and use fake news and alternative¬facts narrative to dismiss an actual piece of media and truth.

Undermining Democracy:

- A deepfake can also help to change democratic discourse and undermine trust in institutions and diplomacy.
- Misinformation about institutions, public policy and politicians powered by deepfakes can be used to spin the story and manipulate belief.
- A deep lie of a political candidate can tarnish his image and reputation.
- Leaders can also use them to increase populism and consolidate power. Deepfakes can become a very effective tool for sowing the seeds of polarization, increasing division in society, and stifling dissent.
- Another concern is a false dividend is an undesirable truth that is dismissed as deep fake or fake news.

Other countries to deal with deep fakes

The European Union:

- The European Union has an updated code of conduct to stop the spread of disinformation through deep fakes. The revised code requires tech companies including Google, Meta and Twitter to take measures to combat deep fakes and fake accounts on their platforms. After signing the code, they have six months to implement their measures.
- According to the updated code, these companies could face fines of up to 6% of their annual global turnover if not complied with. Introduced in 2018, the Code of Practice on Disinformation brings together industry players from around the world to combat misinformation for the first time.

United States of America:

- The US introduced the bipartisan Deepfake Task Force Act to assist the Department of Homeland Security (DHS) in combating deep fake technology. The measure directs DHS to conduct an annual study of deep fakes, assess the technology used, track its use by foreign and domestic entities, and come up with available countermeasures to combat it.

What Is The Solution?

Media literacy efforts must be enhanced to cultivate a discerning public. Media literacy for consumers is the most effective tool to combat disinformation and deepfakes. We also need meaningful regulations with a collaborative discussion with the technology industry, civil society, and policymakers to develop legislative solutions to disincentivising the creation and distribution of malicious deepfakes. Social media platforms are taking cognizance of the deepfake issue, and almost all of them have some policy or acceptable terms of use for deepfakes.

We also need easy¬to¬use and accessible technology solutions to detect deepfakes, authenticate media, and amplify authoritative sources. To counter the menace of deepfakes, we all must take the responsibility to be critical consumers of media on the Internet, think and pause before we share on social media, and be part of the solution to this ‘infodemic’.

➥ California and Texas have passed laws that criminalize the publication and distribution of deep fake videos intended to influence the outcome of an election. The law in Virginia has criminal penalties for the distribution of non-consensual deepfake pornography.

India:

There are no legal regulations against the use of deep fake techniques in India. However, specific laws may be sought regarding misuse of this technology, which may include copyright infringement, defamation and cybercrime etc.

Expected Question

Que. The term "Deepfake" which has been seen in News Recently is related to which one of the following?

A. It is related to the “Sagarmala Project”.

(a) It is related to the “Sagarmala Project”.

(b) It is related to “Mission Sagar”.

(c) It refers to an image, video or audio of a person whose face or body has been digitally altered so that they look or sound like someone else.

(d) It is related to waste management where some of the waste is recycled by separating the waste.

Answer : C

Mains Expected Question & Format

Que.: What do you understand by Deepfake based on Artificial Intelligence (AI)? How can it pose a threat to the individual, society, and democracy, and suggest ways to avoid it?

Answer Format :

- Explain Deepfake based on Artificial Intelligence (AI).
- Explain how deepfakes can pose a threat to individuals, society and democracy.
- Write about how to avoid deepfakes.

Note: - The question of the main examination given for practice is designed keeping in mind the upcoming UPSC mains examination. Therefore, to get an answer to this question, you can take the help of this source as well as other sources related to this topic.