Research Report

Topic 3 : Drawing attention to the issue of "deepfakes" in regard to politics.



By Enora Lagarde & Nivranshu Saha

Outline

Introduction	2
Key Terms	2
Background Information	3
Major Countries and Organisations Involved	4
Relevant UN Resolutions	5
Previous Attempts to Solve the Issue	5
Possible Solutions	5
Bibliography	7

Introduction

In August 2019, a team of Israeli researchers announced a new technique for making deepfakes that creates realistic videos by substituting the face of one individual onto another's (who is actually speaking). Unlike previous methods, this one works on any two people without extensive, iterated focus on their faces. This method cuts hours or even days from previous deepfake processes without the need for expensive hardware. Today, deepfakes are all over the internet sometimes without anyone noticing it, showing both how powerful and how dangerous this invention might be. Used in politics, deepfakes and fakes, combined with artificial intelligence (AI) might represent a complex threat to democracy and freedom of information. As an example, in 2022 a video appeared of the Ukrainian president Volodymyr Zelenskiy, calling on his soldiers to lay down their weapons and return to their families. It was an amateurish example of a deepfake, the term for a hoax that uses AI to create a counterfeit image, most commonly being, fake videos of people. The clip, of unknown provenance, was clearly fake and unconvincing. It was also taken down by mainstream social media platforms including Facebook and Instagram¹. From the Turkish election to Joe Biden's presidency, the presence of deepfakes in regards to politics gains more and more importance and it is now considered urgent to solve this issue.

Key Terms

Artificial Intelligence : The use or study of computer systems or machines that have some of the qualities that the human brain has, such as : the ability to interpret and produce language in

¹: Dan Milmo, "Doctored Sunak picture is just latest in string of political deepfakes » <u>https://www.theguardian.com/technology/2023/aug/03/doctored-sunak-picture-is-just-latestin-string-of-political-deepfakes</u>

a way that seems human, recognize or create images, solve problems, and learn from data supplied to them.²

Fake news : False stories that appear to be news, spread on the internet or using other media, usually created to influence political viewers or as a joke³

Political deepfakes : Political deepfakes specifically refer to the application of deepfake technology in the realm of politics. This involves the creation and dissemination of manipulated content targeting political figures candidates, or public figures with the aim of shaping public opinion and perception, destabilizing democrating processes, or causing reputational harm. Political deepfakes can take various forms, including forged speeches, fabricated endorsment or manipulated interactions, all designed to compromise the trust essential to democratic governance.

Deepfake : A video or sound recording that replaces someone's face or voice with that of someone else, in a way that appears real

Background information

The evolution and increasing sophistication of deepfakes technology is visible.⁴

It all started in 1997, when the «video rewrite» program by Christoph Bregler, Michele Covell, and Malcolm Slaney modified existing video footage of a person speaking, to depict that person mouthing the words contained in a different audio track ⁵. This was the first system to fully automate this kind of facial reanimation. It did so using machine learning techniques to make connections between the sounds produced by a video's subject and the shape of their face. The program was originally intended to be used in movie dubbing, enabling the movie sequence to be modified to sync the actors' lip motions to a new soundtrack. It is since around 2010 that deepfakes gained social and political importance due to the devloping technological innovation of artificial intelligence. Today deepfakes are deeply impacting politics. For example, it altered some democratic values during the Turkish election in May 2023; days before Turkey's parliamentary and presidential election in May, the president, Recep Tayyip Erdoğan, showed a political rally an alleged video of his main opponent, Kemal Kılıçdaroğlu, receiving an endorsement from the Kurdistan Workers' party (PKK). The PKK is designated as a terrorist organisation in Turkey, the US and the UK. The video was in fact two separate clips edited together but an independent factchecking group said the video was widely circulated online nonetheless. Erdoğan won the election.⁶

² <u>https://dictionary.cambridge.org/dictionary/english/artificial-intelligence</u>

³ https://dictionary.cambridge.org/dictionary/english/fake-news

⁴ <u>https://www.researchgate.net/figure/Timeline-of-the-evolution-of-Deepfakes_fig3_361086563</u>

⁵ <u>https://www.historyofinformation.com/detail.php?id=4792</u>

⁶ <u>https://www.theguardian.com/technology/2023/aug/03/doctored-sunak-picture-is-just-latest-in-string-of-political-deepfakes</u>

Developments in generative AI are significantly boosted by the availability of large-scale language and image generation models. Developments have focused on making the models more powerful, capable, and accessible while giving users more control over the style and content of the generated media through detailed text prompts.

Disinformation is a tool that has been used by state and non-state actors throughout history in their attempts to discredit and downplay democratic institutions, amplify conspiracies & radicalization, and encourage distrust of authority. Deepfakes facilitate the speed and effectiveness of these efforts, while expediting the targeting of government/military personnel, phishing and social engineering, and mimicking of biometric data.

From a public safety and security perspective, deepfakes can be employed to commit fraud, engage in coercion and/or extortion, create fake evidence for criminal activities, or to impersonate and/or incriminate individuals in unlawful activities.⁷

Major Countries and Organizations Involved

United States

The government of the united stated have shown a lot of interest in countering deepfakes and the congress has also been seeing the effect of deepfakes on national security

India

The government of India has released advisory to leading social media platforms to remove any deepfake content reported by users within 36 hours, failing which they will lose 'safe harbor immunity' and be liable to criminal and judicial proceedings under the Indian laws⁸

China

To regulate "deep synthesis" content, China's administrative measures implemented on January 10 require service providers to "conspicuously mark" AI-generated content that "may cause public confusion or misidentification" so that users can tell authentic media content from deepfake

⁷ Canadian security Intelligence Service, « The evolution of disinformation a deepfake future »<u>https://www.canada.ca/content/dam/csis-</u>

scrs/documents/publications/2023/The%20Evolution%20of%20Disinformation%20-%20Deepfake%20Report_EN_DIGITAL.pdf

⁸<u>https://www.livemint.com/news/deepfakes-major-violation-of-it-law-harm-women-in-particular-rajeev-chandrasekhar-</u>

<u>11699358904728.html#:~:text=New%20Delhi%3A%20The%20government%20on,proceedings%20under%20the%20Indian%20laws</u>.

Social Media Platforms

Facebook have spent 10 million dollars on technology to able to detect deepfakes, and massive tech companies such as Twitter (X) and Google are joining the struggle to detect and stop the spread of deepfakes.

Universities

Many universities such as MIT and University of Albany are joining forces with the tech giants to enhance the technology that has the ability to detect deepfakes.

Relevant UN Resolutions

The United Nations sees deepfakes as a serious threat and they believe some kind of serious action is needed against deepfakes before it gets too powerful or the usage gets out of hand. "The U.N. said false information and hate speech generated by AI is "convincingly presented to users as fact." Last month, the S&P 500 briefly dipped due to an AI-generated image and faked news report of an explosion near the Pentagon"⁹. To fight against the quickly growing problem of deepfakes the UN "calls for international cooperation and the development of a comprehensive code of conduct"¹⁰.

In terms of past resolutions, the UN has not passed a resolution specifically regarding deepfakes, but there have been discussions regarding topics similar to the spread of misinformation using technology.

- UNRIC A/75/982 (Report of the Secretary-General)
- The 2021 UNIDIR Innovations Dialogue: Deepfakes, Trust and International Security

Previous Attempts to Solve the Issue

Previous attempts to solve the issue have been made from different directions, for example technological advancements in order to be able to detect the deepfakes. In many countries, the option of banning deepfakes by making them illegal has also been brought up. The European Parliament has also had some previous attempts to solve issues through means such as investing in education and raising awareness amongst IT professionals to try and limit the spread of the deepfakes.

Possible Solutions

One of the most attempted solutions to stop deepfakes is the advancement and progress in the creation and development in AI detecting technology.

⁹ <u>https://cointelegraph.com/news/un-serious-concerns-about-ai-deepfakes</u>

¹⁰<u>https://www.analyticsinsight.net/un-ai-deepfakes-pose-serious-threat-action-needed/#:~:text=To%20combat%20the%20growing%20AI,Artificial%20Intelligence%20and%20deepf</u>

needed/#:~:text=To%20combat%20the%20growing%20AI,Artificial%20Intelligence%20and%20deepf ake%20technologies.

Another way to try and stop deepfakes is the ability to educate the average person to spot a deepfake to the best of its ability and also try and to double think before sharing something which has the possibility of being false.

Bibliography

(1) : Dan Milmo, "Doctored Sunak picture is just latest in string of political deepfakes "<u>https://www.theguardian.com/technology/2023/aug/03/doctored-sunak-picture-is-just-latest-in-string-of-political-deepfakes</u>

(2) https://dictionary.cambridge.org/dictionary/english/artificial-intelligence

(3) https://dictionary.cambridge.org/dictionary/english/fake-news

(4) https://www.researchgate.net/figure/Timeline-of-the-evolution-of-Deepfakes_fig3_361086563

(5) <u>https://www.historyofinformation.com/detail.php?id=4792</u>

(6) https://www.theguardian.com/technology/2023/aug/03/doctored-sunak-picture-is-justlatest-in-string-of-political-deepfakes

(7)https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_BRIE(2021)6 90039(ANN)_EN.pdf

(8) https://www.nytimes.com/2023/01/22/business/media/deepfake-regulation-difficulty.html

(9) Canadian security Intelligence Service, « The evolution of disinformation a deepfake future » <u>https://www.canada.ca/content/dam/csis-</u>
<u>scrs/documents/publications/2023/The%20Evolution%20of%20Disinformation%20-</u>
%20Deepfake%20Report_EN_DIGITAL.pdf