ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON
THE
INFORMATION DOMAIN

Issue 4/22 (April)

The Threat of Deepfakes in the Online Space

INTRODUCTION

1. Over the years, deepfakes have become increasingly common on social media platforms such as Facebook, Instagram and TikTok. Deepfakes are known as synthetic media in which a person from an existing image or video is replaced with someone else's likeness. The rise in such deepfakes is worrisome due to the potential for abuse for disinformation purposes.

2. Deepfakes utilise a form of Artificial Intelligence (AI) technology called Deep Learning to analyse people's expressions, speech patterns and even movements to mimic how they would speak or do something. With access to such technology and sufficient skills, one can create deepfakes that are realistic-looking. In one example, deepfakes of Tom Cruise started appearing on TikTok in 2021. These deepfakes were of such high-quality that it was difficult for audiences to discern that it was not actually Tom Cruise performing the actions, which included putting on a hat or sunglasses (see Figure 1 for examples) in the videos.

Figure 1: Comparison of the Deepfake Versions (left and middle) and Actual Person (right)

Photo Credits: CNN Business, Amber Maas/SWNS

3. According to *Engineering News*, deepfakes were initially created with good intentions. For instance, in 2019, a malaria awareness campaign video featuring a deepfake of the famous English footballer David Beckham speaking in nine different languages went viral, thus succeeding in helping to raise awareness.

Issues Arising From Deepfake Technology

4. Deepfakes contribute to the problem of verifying media content that are spread on social media. With many people relying on social media for information on such events, deepfakes that are posted onto these platforms could be widely shared and misunderstood by some users as facts. *Forbes* has reported that deepfakes have become a tool that is utilised to mislead and sow uncertainty regarding the facts of ongoing conflicts.

5. According to *Business Standard*, deepfakes are dangerous as the technology allows one to create realistic videos of anyone – including political leaders or celebrities – doing and saying things that they in reality have not. For instance, according to *National Herald India News*, a deepfake video of Ukrainian president Volodymyr Zelensky issuing a statement of surrender and urging citizens to lay down arms was circulated on social media platforms such as Facebook, Twitter and YouTube on 16 Mar 2022. Such statements, if believed and acted upon by people, could sow confusion and chaos.

6. While deepfakes might not have significant impact under normal circumstances, they become problematic during stressful situations when people's ability to think rationally are impeded and attention span significantly reduced. The visual, emotional and visceral nature of deepfakes also make it hard to discern what is real from what is fake. According to *CNN*, even bad deepfakes can erode users' confidence in navigating the online environment.

7. The existence of deepfakes can cause social media users to lose confidence in their ability to tell fact from fiction and doubt everything, especially in an online environment that is already rife with misinformation. In the example of the Zelensky deepfake above, keen-eyed users were able to identify the visual inconsistencies such as the skewed proportions of the head to the body, the different skin tone, as well as the pixilation around the head due to the poor video-editing (see Figure 2 for the comparison between the deepfake version and the actual version of Zelensky). The video was subsequently taken down by Meta, which also notified the other platforms.

Figure 2: Comparison of the Deepfake Version (left) and Actual Person (right)

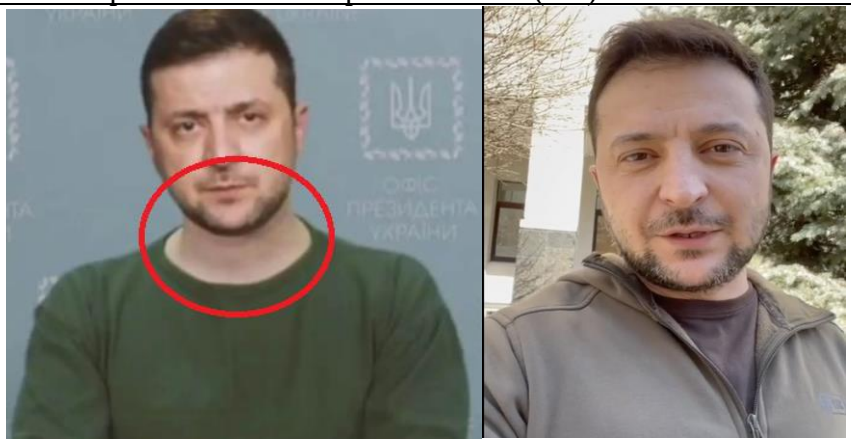

Photo Credits: New York Post, Joshua Rhett Miller

ASSESSMENT

8. As deepfake technology improves, many companies have been developing video authentication tools to combat them. According to *CNN*, DeepFake-o-meter is a tool developed by a cyber company that allows anyone to upload videos to check their authenticity. Although the software allows people to spot deepfake videos, the results can take hours to generate. Authentication tools can also be defeated by deliberate improvements in deepfake technology.

9. According to *ISEAS-Yusof Ishak Institute*, regulation should keep up with the latest deepfakes trends in order to better manage the spread of such disinformation. Governments should also act swiftly to debunk disinformation propagated via deepfakes. For instance, according to *National Herald News*, the Ukranian government later released a video of Zelensky addressing the falsified clip.

10. According to *Engineering News*, there is ultimately no technology that would be able to counter deepfakes perfectly as traces of manipulation cannot always be identified. Educating the public should be the priority, as it is everyone's responsibility to perform their due diligence to fact-check information seen online.

CONTACT DETAILS

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

REFERENCES

News Articles

1 Deepfakes are now trying to change the course of war
[Link: https://edition.cnn.com/2022/03/25/tech/deepfakes-disinformation-war/index.html]

2 'Star Wars' fans love CGI Luke Skywalker, but deepfake implications are dangerous
[Link: https://dailytargum.com/article/2022/03/star-wars-fans-love-cgi-luke-skywalker-but-deepfake-implications-are]

3 Facebook removes deepfake video of Ukrainian President
[Link: https://www.nationalheraldindia.com/international/fb-removes-deepfake-video-of-Ukrainian-president]

4 Social media has provided a skewed account of the war in Ukraine
[Link: https://www.forbes.com/sites/petersuciu/2022/03/31/social-media-has-provided-a-skewed-account-of-the-war-in-ukraine/?sh=562e93287826]

5 Seeing or hearing is not always believing – deepfakes are a growing cyberthreat
[Link: https://www.engineeringnews.co.za/article/seeing-or-hearing-is-not-always-believing-deepfakes-are-a-growing-cyberthreat-2022-03-10/rep_id:4136]

6 The deceptive world of deepfakes
[Link: https://www.business-standard.com/podcast/technology/the-deceptive-world-of-deepfakes-122032100015_1.html]

7 From deepfakes to hoax calls: 'Fake news war' in Russia-Ukraine crisis
[Link: https://www.wionews.com/world/from-deepfakes-to-hoax-calls-fake-news-war-in-russia-ukraine-crisis-463476]

8 2022/33 “Stronger Social Media Influence in the 2022 Philippine Elections” by Aries A. Arugay
[Link: https://www.iseas.edu.sg/articles-commentaries/seas-persepctive/2022-33-stronger-social-media-influence-in-the-2022-phillippine-elections-by-aries-a-arugay/]

9 Photo Credits
[Links:
https://edition.cnn.com/2022/03/25/tech/deepfakes-disinformation-war/index.html
https://www.mirror.co.uk/3am/celebrity-news/tom-cruise-real-life-top-26676515
https://news.sky.com/story/ukraine-war-deepfake-video-of-zelensky-telling-ukrainians-to-lay-down-arms-debunked-12567789
https://nypost.com/2022/03/17/deepfake-video-shows-volodymyr-zelensky-telling-ukrainians-to-surrender/]