Misinformation woes could multiply with 'deepfake' videos

January 28 2019, by Rob Lever

Paul Scharre of the Center for a New American Security looks at a "deepfake" video of former US President Barack Obama manipulated to show him speaking words from actor Jordan Peele on January 24, 2019, in Washington

If you see a video of a politician speaking words he never would utter, or a Hollywood star improbably appearing in a cheap adult movie, don't adjust your television set—you may just be witnessing the future of "fake news."

"Deepfake" videos that manipulate reality are becoming more sophisticated due to advances in artificial intelligence, creating the potential for new kinds of misinformation with devastating consequences.

As the technology advances, worries are growing about how deepfakes can be used for nefarious purposes by hackers or state actors.

"We're not quite to the stage where we are seeing deepfakes weaponized, but that moment is coming," Robert Chesney, a University of Texas law professor who has researched the topic, told AFP.

Chesney argues that deepfakes could add to the current turmoil over disinformation and influence operations.

"A well-timed and thoughtfully scripted deepfake or series of deepfakes could tip an election, spark violence in a city primed for civil unrest, bolster insurgent narratives about an enemy's supposed atrocities, or exacerbate political divisions in a society," Chesney and University of Maryland professor Danielle Citron said in a blog post for the Council on Foreign Relations.

Paul Scharre, a senior fellow at the Center for a New American Security, a think tank specializing in AI and security issues, said it was almost inevitable that deepfakes would be used in upcoming elections.

Digital manipulation may be good for Hollywood but new "deepfake" techniques could create a new kind of misinformation, according to researchers

A fake video could be deployed to smear a candidate, Scharre said, or to enable people to deny actual events captured on authentic video.

With believable fake videos in circulation, he added, "people can choose to believe whatever version or narrative that they want, and that's a real concern."

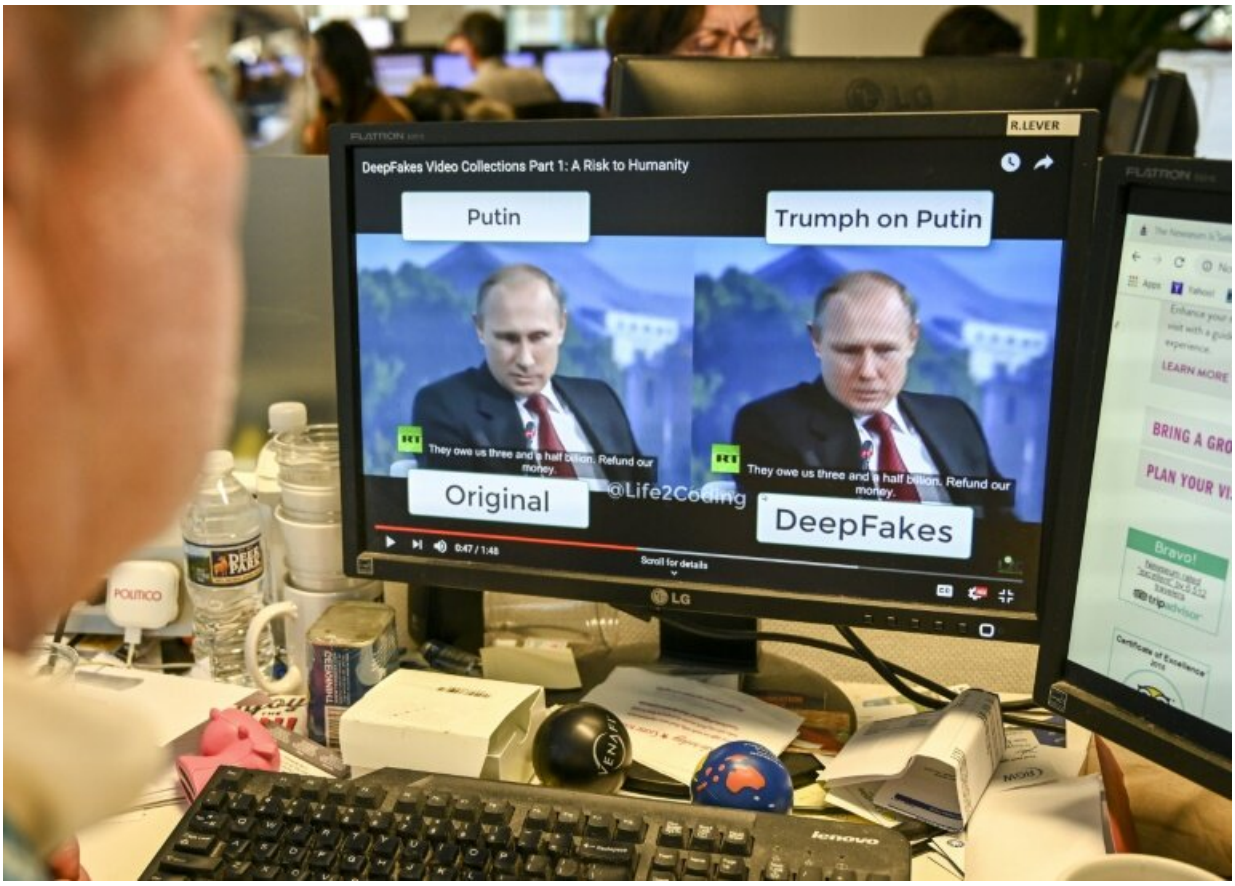
Chaplin's return?

Video manipulation has been around for decades and can be innocuous

or even entertaining—as in the digitally-aided appearance of Peter Cushing in 2016's "Rogue One: A Star Wars Story," 22 years after his death.

Carnegie Mellon University researchers last year revealed techniques that make it easier to produce deepfakes via machine learning to infer missing data.

In the movie industry, "the hope is we can have old movie stars like Charlie Chaplin come back," said Aayush Bansal.



Experts say an important way to deal with deepfakes is to increase public awareness, making people more skeptical of what used to be considered incontovertible proof

The popularization of apps which make realistic fake videos threatens to undermine the notion of truth in news media, criminal trials and many other areas, researchers point out.

"If we can put any words in anyone's mouth, that is quite scary," says Siwei Lyu, a professor of computer science at the State University of New York at Albany, who is researching deepfake detection.

"It blurs the line between what is true and what is false. If we cannot really trust information to be authentic it's no better than to have no information at all."

Representative Adam Schiff and two other lawmakers recently sent a letter to National Intelligence Director Dan Coats asking for information about what the government is doing to combat deepfakes.

"Forged videos, images or audio could be used to target individuals for blackmail or for other nefarious purposes," the lawmakers wrote.

"Of greater concern for national security, they could also be used by foreign or domestic actors to spread misinformation."

The producers of "Rogue One: A Star Wars Story," digitally recreated actors Peter Cushing and Carrie Fisher after their deaths using techniques similar to those employed for "deepfake" videos

Separating fake from real

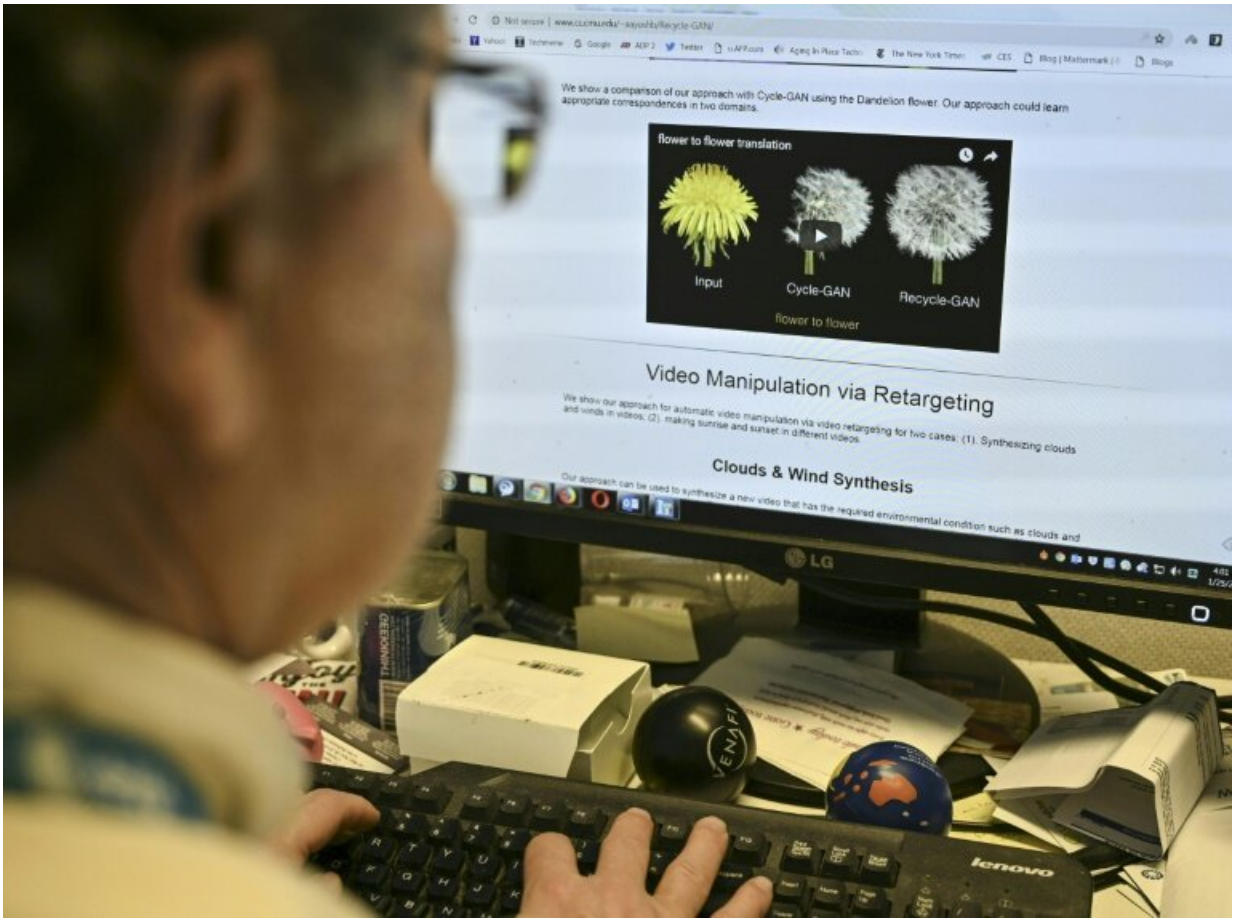
Researchers have been working on better detection methods for some time, with support from private firms such as Google and government entities like the Pentagon's Defense Advanced Research projects Agency (DARPA), which began a media forensics initiative in 2015.

Lyu's research has focused on detecting fakes, in part by analyzing the rate of blinking of an individual's eyes.

But he acknowledges that even detecting fakes may not be enough, if a video goes viral and leads to chaos.

"It's more important to disrupt the process than to analyze the videos," Lyu said.

While deepfakes have been evolving for several years, the topic came into focus with the creation last April of video appearing to show former president Barack Obama using a curse word to describe his successor Donald Trump—a coordinated stunt from filmmaker Jordan Peele and BuzzFeed.



An AFP journalist views an example of a "deepfake" video manipulated using

Also in 2018, a proliferation of "face swap" porn videos that used images of Emma Watson, Scarlett Johansson and other celebrities prompted bans on deepfakes by Reddit, Twitter and Pornhub, though it remained unclear if they could enforce the policies.

Scharre said there is "an arms race between those who are creating these videos and security researchers who are trying to build effective tools of detection."

But he said an important way to deal with deepfakes is to increase public awareness, making people more skeptical of what used to be considered incontrovertible proof.

"After a video has gone viral it may be too late for the social harm it has caused," he said.

Citation: Misinformation woes could multiply with 'deepfake' videos (2019, January 28) retrieved 21 September 2024 from https://phys.org/news/2019-01-misinformation-woes-deepfake-videos.html