# AI supercharges threat of disinformation in a big year for elections globally

March 14, 2024

**Online *Desk:*** Artificial intelligence is supercharging the threat of election disinformation worldwide, making it easy for anyone with a smartphone and a devious imagination to create fake – but convincing – content aimed at fooling voters.

It marks a quantum leap from a few years ago, when creating phony photos, videos or audio clips required teams of people with time, technical skill and money. Now, using free and low-cost generative artificial intelligence services from companies like Google and OpenAI, anyone can create high-quality "deepfakes" with just a simple text prompt.

A wave of AI deepfakes tied to elections in Europe and Asia has coursed through social media for months, serving as a warning for more than 50 countries heading to the polls this year.

"You don't need to look far to see some people … being clearly confused as to whether something is real or not," said Henry Ajder, a leading expert in generative AI based in Cambridge, England.

The question is no longer whether AI deepfakes could affect elections, but how influential they will be, said Ajder, who runs a consulting firm called Latent Space Advisory.

As the U.S. presidential race heats up, FBI Director Christopher Wray recently warned about the growing threat, saying generative AI makes it easy for "foreign adversaries to engage in malign influence."

With AI deepfakes, a candidate's image can be smeared, or softened. Voters can be steered toward or away from candidates — or even to avoid the polls altogether. But perhaps the greatest threat to democracy, experts say, is that a surge of AI deepfakes could erode the public's trust in what they see and hear.

Some recent examples of AI deepfakes include:

— A video of Moldova's pro-Western president throwing her support behind a political party friendly to Russia.

— Audio clips of Slovakia's liberal party leader discussing vote rigging and raising the price of beer.

— A video of an opposition lawmaker in Bangladesh — a conservative Muslim majority nation — wearing a bikini.

The novelty and sophistication of the technology makes it hard to track who is behind AI deepfakes. Experts say governments and companies are not yet capable of stopping the deluge, nor are they moving fast enough to solve the problem.

As the technology improves, "definitive answers about a lot of the fake content are going to be hard to come by," Ajder said.

ERODING TRUST
Some AI deepfakes aim to sow doubt about candidates' allegiances.

In Moldova, an Eastern European country bordering Ukraine, pro-Western President Maia Sandu has been a frequent target. One AI deepfake that circulated shortly before local elections depicted her endorsing a

Russian-friendly party and announcing plans to resign.

Officials in Moldova believe the Russian government is behind the activity. With presidential elections this year, the deepfakes aim “to erode trust in our electoral process, candidates and institutions — but also to erode trust between people,” said Olga Rosca, an adviser to Sandu. The Russian government declined to comment for this story.

China has also been accused of weaponizing generative AI for political purposes.

In Taiwan, a self-ruled island that China claims as its own, an AI deepfake gained attention earlier this year by stirring concerns about U.S. interference in local politics.

The fake clip circulating on TikTok showed U.S. Rep. Rob Wittman, vice chairman of the U.S. House Armed Services Committee, promising stronger U.S. military support for Taiwan if the incumbent party’s candidates were elected in January.

Wittman blamed the Chinese Communist Party for trying to meddle in Taiwanese politics, saying it uses TikTok — a Chinese-owned company — to spread “propaganda.”

A spokesperson for the Chinese foreign ministry, Wang Wenbin, said his government doesn’t comment on fake videos and that it opposes interference in other countries’ internal affairs. The Taiwan election, he stressed, “is a local affair of China.”

## BLURRING REALITY

Audio-only deepfakes are especially hard to verify because, unlike photos and videos, they lack telltale signs of manipulated content.

In Slovakia, another country overshadowed by Russian influence, audio clips resembling the voice of the liberal party chief were shared widely on social media just days before parliamentary elections. The clips purportedly captured him talking about hiking beer prices and rigging the vote.

It’s understandable that voters might fall for the deception, Ajder said, because humans are “much more used to judging with our eyes than with our ears.”

In the U.S., robocalls impersonating U.S. President Joe Biden urged voters in New Hampshire to abstain from voting in January’s primary election. The calls were later traced to a political consultant who said he was trying to publicize the dangers of AI deepfakes.

In poorer countries, where media literacy lags, even low-quality AI fakes can be effective.

Such was the case last year in Bangladesh, where opposition lawmaker Rumeen Farhana — a vocal critic of the ruling party — was falsely depicted wearing a bikini. The viral video sparked outrage in the conservative, majority-Muslim nation.

“They trust whatever they see on Facebook,” Farhana said.

Experts are particularly concerned about upcoming elections in India, the world’s largest democracy and where social media platforms are breeding grounds for disinformation.

## A CHALLENGE TO DEMOCRACY

Some political campaigns are using generative AI to bolster their candidate’s image.

In Indonesia, the team that ran the presidential campaign of Prabowo Subianto deployed a simple mobile app to build a deeper connection with supporters across the vast island nation. The app enabled voters to upload photos and make AI-generated images of themselves with Subianto.

As the types of AI deepfakes multiply, authorities around the world are scrambling to come up with guardrails.

The European Union already requires social media platforms to cut the risk of spreading disinformation or "election manipulation." It will mandate special labeling of AI deepfakes starting next year, too late for the EU's parliamentary elections in June. Still, the rest of the world is a lot further behind.

The world's biggest tech companies recently — and voluntarily — signed a pact to prevent AI tools from disrupting elections. For example, the company that owns Instagram and Facebook has said it will start labeling deepfakes that appear on its platforms.

But deepfakes are harder to rein in on apps like the Telegram chat service, which did not sign the voluntary pact and uses encrypted chats that can be difficult to monitor.

Some experts worry that efforts to rein in AI deepfakes could have unintended consequences.

Well-meaning governments or companies might trample on the sometimes "very thin" line between political commentary and an "illegitimate attempt to smear a candidate," said Tim Harper, a senior policy analyst at the Center for Democracy and Technology in Washington.

Major generative AI services have rules to limit political disinformation. But experts say it remains too easy to outwit the platforms' restrictions or use alternative services that don't have the same safeguards.

Even without bad intentions, the rising use of AI is problematic. Many popular AI-powered chatbots are still spitting out false and misleading information that threatens to disenfranchise voters.

And software isn't the only threat. Candidates could try to deceive voters by claiming that real events portraying them in an unfavorable light were manufactured by AI.

"A world in which everything is suspect — and so everyone gets to choose what they believe — is also a world that's really challenging for a flourishing democracy," said Lisa Reppell, a researcher at the International Foundation for Electoral Systems in Arlington, Virginia.