AI presents political peril for 2024 with threat to mislead voters

Associated Press

Thanks to recent advances in artificial intelligence, tools that can create lifelike photos, video and audio are now cheap and readily available. AI experts and political scientists say these new programs will have significant implications for next year's U.S. elections

Computer engineers and tech-inclined political scientists have warned for years that cheap, powerful artificial intelligence tools would soon allow anyone to create fake images, video and audio that was realistic enough to fool voters and perhaps sway an election.

The synthetic images that emerged were often crude, unconvincing and costly to produce, especially when other kinds of misinformation were so inexpensive and easy to spread on social media. The threat posed by AI and so-called deepfakes always seemed a year or two away.

No more.

Sophisticated generative AI tools can now create cloned human voices and hyper-realistic images, videos and audio in seconds, at minimal cost. When strapped to powerful social media algorithms, this fake and digitally created content can spread far and fast and target highly specific audiences, potentially taking campaign dirty tricks to a new low.

The implications for the 2024 campaigns and elections are as large as they are troubling: Generative AI can not only rapidly produce targeted campaign emails, texts or videos, it also could be used to mislead voters, impersonate candidates and undermine elections on a scale and at a speed not yet seen.

“We’re not prepared for this,” warned A.J. Nash, vice president of intelligence at the cybersecurity firm ZeroFox. ”To me, the big leap forward is the audio and video capabilities that have emerged. When you can do that on a large scale, and distribute it on social platforms, well, it’s going to have a major impact.”

AI experts can quickly rattle off a number of alarming scenarios in which generative AI is used to create synthetic media for the purposes of confusing voters, slandering a candidate or even inciting violence.

Here are a few: Automated robocall messages, in a candidate’s voice, instructing voters to cast ballots on the wrong date; audio recordings of a candidate supposedly confessing to a crime or expressing racist views; video footage showing someone giving a speech or interview they never gave. Fake images designed to look like local news reports, falsely claiming a candidate dropped out of the race.

"What if Elon Musk personally calls you and tells you to vote for a certain candidate?" said Oren Etzioni, the founding CEO of the Allen Institute for AI, who stepped down last year to start the nonprofit AI2. "A lot of people would listen. But it's not him."

Former President Donald Trump, who is running in 2024, has shared AI-generated content with his followers on social media. A manipulated video of CNN host Anderson Cooper that Trump shared on his Truth Social platform on Friday, which distorted Cooper's reaction to the CNN town hall this past week with Trump, was created using an AI voice-cloning tool.

A dystopian campaign ad released last month by the Republican National Committee offers another glimpse of this digitally manipulated future. The online ad, which came after President Joe Biden announced his reelection campaign, and starts with a strange, slightly warped image of Biden and the text "What if the weakest president we've ever had was re-elected?"

A series of AI-generated images follows: boarded up storefronts in the United States as the economy crumbles; soldiers and armored military vehicles patrolling local streets as tattooed criminals and waves of immigrants create panic.

"An AI-generated look into the country's possible future if Joe Biden is re-elected in 2024," reads the ad's description from the RNC.

The RNC acknowledged its use of AI, but others, including nefarious political campaigns and foreign adversaries, will not, said Petko Stoyanov, global chief technology officer at Forcepoint, a cybersecurity company based in Austin, Texas. Stoyanov predicted that groups looking to meddle with U.S. democracy will employ AI and synthetic media as a way to erode trust.

"What happens if an international entity — a cybercriminal or a nation state — impersonates someone. What is the impact? Do we have any recourse?" Stoyanov said. "We're going to see a lot more misinformation from international sources."

AI-generated political disinformation already has gone viral online ahead of the 2024 election, from a doctored video of Biden appearing to give a speech attacking transgender people to AI-generated images of children supposedly learning satanism in libraries.

AI images appearing to show Trump’s mug shot also fooled some social media users even though the former president didn’t take one when he was booked and arraigned in a Manhattan criminal court for falsifying business records. Other AI-generated images showed Trump resisting arrest, though their creator was quick to acknowledge their origin.

Legislation that would require candidates to label campaign advertisements created with AI has been introduced in the House by Rep. Yvette Clarke, D-N.Y., who has also sponsored legislation that would require anyone creating synthetic images to add a watermark indicating the fact.

Some states have offered their own proposals for addressing concerns about deepfakes.

Clarke said her greatest fear is that generative AI could be used before the 2024 election to create a video or audio that incites violence and turns Americans against each other.