Deepfakes in an election year — is Asia ready to handle misinformation campaigns?

Chelsea Ong
CNBC, 13 March 2024

Ahead of the Indonesian elections on Feb. 14, a video of late Indonesian president Suharto advocating for the political party he once presided over went viral.

The AI-generated deepfake video that cloned his face and voice racked up 4.7 million views on X alone.

This was not a one-off incident.

In Pakistan, a deepfake of former prime minister Imran Khan emerged around the national elections, announcing his party was boycotting them. Meanwhile, in the U.S., New Hampshire voters heard a deepfake of President Joe Biden's asking them to not vote in the presidential primary.

Deepfakes of politicians are becoming increasingly common, especially with 2024 set up to be the biggest global election year in history.

Reportedly, at least 60 countries and more than four billion people will be voting for their leaders and representatives this year, which makes deepfakes a matter of serious concern.

According to a Sumsub report in November, the number of deepfakes across the world rose by 10 times from 2022 to 2023. In APAC alone, deepfakes surged by 1,530% during the same period.

Online media, including social platforms and digital advertising, saw the biggest rise in identity fraud rate at 274% between 2021 and 2023. Professional services, healthcare, transportation and video gaming were were also among industries impacted by identity fraud.

Asia is not ready to tackle deepfakes in elections in terms of regulation, technology, and education, said Simon Chesterman, senior director of AI governance at AI Singapore.

In its 2024 Global Threat Report, cybersecurity firm Crowdstrike reported that with the number of elections scheduled this year, nation-state actors including from China, Russia and Iran are highly likely to conduct misinformation or disinformation campaigns to sow disruption.

"The more serious interventions would be if a major power decides they want to disrupt a country's election — that's probably going to be more impactful than political parties playing around on the margins," said Chesterman.

However, most deepfakes will still be generated by actors within the respective countries, he said.

Carol Soon, principal research fellow and head of the society and culture department at the Institute of Policy Studies in Singapore, said domestic actors may include opposition parties and political opponents or extreme right wingers and left wingers.

Deepfake Dangers

At the minimum, deepfakes pollute the information ecosystem and make it harder for people to find accurate information or form informed opinions about a party or candidate, said Soon.

Voters may also be put off by a particular candidate if they see content about a scandalous issue that goes viral before it's debunked as fake, Chesterman said. "Although several governments have tools (to prevent online falsehoods), the concern is the genie will be out of the bottle before there's time to push it back in."

"We saw how quickly X could be taken over by the deep fake pornography involving Taylor Swift — these things can spread incredibly quickly," he said, adding that regulation is often not enough and incredibly hard to enforce. "It's often too little too late."

Adam Meyers, head of counter adversary operations at CrowdStrike, said that deepfakes may also invoke confirmation bias in people: "Even if they know in their heart it's not true, if it's the message they want and something they want to believe in they're not going to let that go."

Chesterman also said that fake footage which shows misconduct during an election such as ballot stuffing, could cause people to lose faith in the validity of an election.

On the flip side, candidates may deny the truth about themselves that may be negative or unflattering and attribute that to deepfakes instead, Soon said

Who should be responsible?

There is a realization now that more responsibility needs to be taken on by social media platforms because of the quasi-public role they play, said Chesterman.

In February, 20 leading tech companies, including Microsoft, Meta, Google, Amazon, IBM as well as Artificial intelligence startup OpenAI and social media companies such as Snap, TikTok and X announced a joint commitment to combat the deceptive use of AI in elections this year.

The tech accord signed is an important first step, said Soon, but its effectiveness will depend on implementation and enforcement. With tech companies adopting different measures across their platforms, a multi-prong approach is needed, she said.

Tech companies will also have to be very transparent about the kinds of decisions that are made, for example, the kinds of processes that are put in place, Soon added.

But Chesterman said it is also unreasonable to expect private companies to carry out what are essentially public functions. Deciding what content to allow on social media is a hard call to make, and companies may take months to decide, he said.

"We should not just be relying on the good intentions of these companies," Chesterman added. "That's why regulations need to be established and expectations need to be set for these companies."

Towards this end, Coalition for Content Provenance and Authenticity (C2PA), a non-profit, has introduced digital credentials for content, which will show viewers verified information such as the creator's information, where and when it was created, as well as whether generative AI was used to create the material.

C2PA member companies include Adobe, Microsoft, Google and Intel.

OpenAI has announced it will be implementing C2PA content credentials to images created with its DALL·E 3 offering early this year.

In a Bloomberg House interview at the World Economic Forum in January, OpenAI founder and CEO Sam Altman said the company was “quite focused” on ensuring its technology wasn’t being used to manipulate elections.

“I think our role is very different than the role of a distribution platform” like a social media site or news publisher, he said. “We have to work with them, so it’s like you generate here and you distribute here. And there needs to be a good conversation between them.”

Meyers suggested creating a bipartisan, non-profit technical entity with the sole mission of analyzing and identifying deepfakes.

“The public can then send them content they suspect is manipulated,” he said. “It’s not foolproof but at least there’s some sort of mechanism people can rely on.”

But ultimately, while technology is part of the solution, a large part of it comes down to consumers, who are still not ready, said Chesterman.

Soon also highlighted the importance of educating the public.

“We need to continue outreach and engagement efforts to heighten the sense of vigilance and consciousness when the public comes across information,” she said.

The public needs to be more vigilant; besides fact checking when something is highly suspicious, users also need to fact check critical pieces of information especially before sharing it with others, she said.

“There’s something for everyone to do,” Soon said. “It’s all hands on deck.”