Questions to ask about government use of deepfakes

March 13 2024, by Amanda Morris

Credit: AI-generated image

Will the lure of deepfakes prove irresistible to democratic governments? What questions should governments ask—and who in government should be asking them—when a deepfake is being considered?

Two Northwestern University professors coauthored a new report

examining several hypothetical scenarios in which democratic governments might consider using deepfakes to advance their foreign policy objectives and the potential harms this use might pose to democracy.

The report was published March 12 by the Center for Strategic & International Studies (CSIS).

Co-authors are VS Subrahmanian, the Walter P. Murphy Professor of Computer Science at Northwestern's McCormick School of Engineering and a fellow at the Buffett Institute for Global Affairs; and Daniel W. Linna Jr., a senior lecturer and director of law and technology initiatives at the Northwestern Pritzker School of Law. They led the report with Daniel Byman, a senior fellow on the CSIS Transnational Threats Project.

A digitally altered video, photo or audio recording, deepfakes are typically used maliciously to spread disinformation and create confusion. A well-known example includes a fake video that surfaced in March 2022, in which a digitally altered version of Ukrainian president Volodymyr Zelensky tells his soldiers to lay down their arms.

"As AI has improved, deepfakes have gone from primitive to highly realistic, and they will only get harder to distinguish," the authors write in the report. "This proliferation of AI provides an unparalleled opportunity for state actors to use deepfakes for national security purposes."

The researchers posit that the lure of deepfakes will eventually become irresistible to democratic governments. "It will not be long before major democracies, including the United States, start or at least consider using deepfakes to achieve their ends, if they have not already done so," they said.

According to the authors officials should consider several factors when considering the use of deepfakes:

- the likely efficacy of the deepfake,
- its audience,
- the potential harms,
- the legal implications,
- the nature of the target,
- the goal of the deepfake, and
- the traceability of the deepfake back to the originating democratic government.

In general, the authors argue that deepfakes should not be used as they are likely to reduce the credibility of democratic governments. There may be rare circumstances, however, when the use of deepfakes deserves serious consideration. In these cases, the authors say, governments should develop a process for approving or rejecting deepfakes that ensures a wide variety of perspectives are brought to the table.

More information: Government Use of Deepfakes: The Questions to Ask. csis-website-prod.s3.amazonaws … eIjOKhzqi672claqU.if

Provided by Northwestern University

Citation: Questions to ask about government use of deepfakes (2024, March 13) retrieved 1 May 2024 from https://phys.org/news/2024-03-deepfakes.html