University of Virginia | National Security Data and Policy Institute

NATIONALSECURITY.VIRGINIA.EDU
NSDPI@VIRGINIA.EDU

Addressing the Role of Deepfake Technology in Foreign Interference in U.S. Elections

Cole Leis

Due to significant gaps in artificial intelligence (AI) policy in the U.S., it is too easy for foreign adversaries to use deepfake technology to spread election disinformation and therefore interfere in U.S. elections. The U.S. must act to preserve election integrity, prevent the public's interests from being undermined, and maintain public trust in democratic institutions.

Foreign Interference in U.S. Elections, Disinformation, and Artificial Intelligence

- Foreign interference in U.S. elections has become an increasingly prevalent issue in recent years. Interference primarily comes from Russia, China, and Iran.
- Election interference frequently comes in the form of disinformation, "intentionally false information spread with the purpose of deceiving its recipients" (American Security Project, n.d.).
- Social media platforms exacerbate the issue of disinformation, threatening elections. When foreign adversaries use disinformation to influence electoral outcomes, there is a risk that action from officials who benefitted from the interference electorally will undermine U.S. interests. When the public is deceived, it may mistakenly act against its own interests.
- As technology advances, it becomes cheaper, quicker, and easier to create seemingly legitimate disinformation. AI has vastly expanded adversaries' ability to create and spread disinformation.
- AI has already transformed the elections of at least 50 countries.
- As AI becomes better equipped to revise its methods in real time and target specific audiences with its messaging, the threat that AI poses will continue to grow.
- Enforcement of social media platforms and AI companies' AI misuse policies consistently falls short.

Deepfake Technology

- Deepfake technology creates new opportunities for foreign actors to interfere in elections.
- A deepfake is generally considered to be an image, video, or audio recording that is created or altered using AI to depict a person doing or saying something that they did not actually do or say.
- Deepfakes are created through deep learning, a form of machine learning whereby a generative adversarial network takes input and learns to generate output comparable to the input from which it learned. Deep learning advancements have made it possible for anyone to create deepfakes quickly and at little cost.
- Deepfakes have already seen significant use as a tool for swaying voters through disinformation in elections.
    - Prior to Taiwan's presidential election in 2024, a CCP-linked group distributed deepfaked audio of one candidate endorsing another.
    - In August 2024, a Russian influence network shared articles with deepfaked audio of former president Barack Obama expressing dismay at the failure of the Trump assassination attempt.
    - In October 2024, a deepfake video spread by a Russian-aligned propaganda network purported to show a former student of vice president candidate Tim Walz accusing Walz of sexual assault.
- Experts argue that deepfakes and AI in general did not disrupt the U.S. presidential election in 2024, but misuse of such tools increasingly threatens to blur the line between fact and fiction, worsen polarization, and reduce confidence in the institutions crucial to democracy.

Policy History, Challenges, and Options

- There is currently no comprehensive federal legislation addressing AI-related issues in the U.S. Since federal efforts to handle deepfakes have been inadequate, states have attempted to mount a patchwork defense against AI's harms. Two states have durational prohibitions, and 24 states have requirements surrounding disclosure.
- Critics of deepfake laws argue that the laws threaten free speech and American competitiveness, and they say the laws are impotent since they are hard to enforce. Congressional Republicans and President Donald Trump have worked to undermine AI regulation efforts.
- Challenges in crafting and passing policy addressing political AI use include avoiding First Amendment lawsuits, defining AI properly, determining when legal restrictions should be triggered, developing procedures for establishing liability, keeping up with technological advancements, and figuring out what to regulate.
- Election disinformation policy is also relevant. Federal and state laws ban voter intimidation, and many of these laws ban certain forms of election disinformation. Some states ban certain kinds of false election-related speech, but these bans are sometimes legally controversial.
- To counter foreign adversaries' use of deepfakes to interfere in elections, policymakers should consider transparency and disclosure mandates, prohibitions on certain kinds of deceptive AI content, foreign influence threat report requirements for social media platforms, investment in AI detection capabilities, media literacy promotion through educational initiatives, collaboration with foreign partners, and additional research into foreign adversaries' use of generative AI.