Synthetic Media and Election Integrity
Defending our Democracies

Di Cooke

The views expressed in this article are those of the authors, and do not necessarily represent the views of The Alan Turing Institute or any other organisation.
Introduction: the genesis of the issue

The 2016 US presidential elections saw the terms ‘fake news’ and ‘disinformation’ rise to prominence in public discourse. This has continued to be the case in various elections since then, with disinformation a widespread presence in today’s political landscape.

Countries worldwide are now having to contend with a growing deluge of fake news which threatens to manipulate voting, exacerbate societal tensions, and even incite violence – such as the 2021 attack on the US Capitol Building.

The growing accessibility of highly sophisticated products and services which use generative artificial intelligence (AI) to produce digital content (like text, images, audio and video) has now added a new dimension to this threat. Generative AI is lowering the costs of disinformation, enabling falsehoods to be produced and disseminated at greater speed and scale, and with wider scope than before. Today, this means that an individual with little technical know-how can manufacture convincing digital content in only minutes using a wide range of publicly available applications.

Despite there being significant cause for concern with the status quo, the growing ubiquity of this technology poses additional risks for future election integrity and societal stability. A number of significant elections around the world will soon be facing this challenge, including the upcoming 2024 presidential elections in Taiwan, a longstanding target and testing ground for Chinese disinformation operations.

There are also growing international concerns about the 2023 Polish elections, and Russian disinformation campaigns targeting the close relationship between Poland and Ukraine, as well as domestically produced disinformation by the Polish government itself. With synthetic media reportedly already being used to influence several recent elections, these issues are becoming even more acute. With the frequency of AI-enabled disinformation expected to grow, experts can look to existing examples to better anticipate how upcoming elections may be undermined.

This article first explores how convincing AI-generated content has become today, and how the technology has been employed for both beneficial and harmful purposes. Next, the article examines incidents of synthetic media use within election campaigns and discusses other threats outside of disinformation which security officials and policymakers should prioritise. Finally, specific responses are identified which should be prioritised by stakeholders across government, industry, and civil society to successfully combat the growing threat to political elections posed by the weaponisation of synthetic media.
Introduction: the genesis of the issue

Viral synthetic images of Donald Trump’s arrest and sentencing on Twitter\(^7\) (2023) and a synthetic image of Barack Obama and Angela Merkel spending a day at the beach on Instagram\(^8\) (2023).
Distinguishing between the real and the fake

An upcoming study conducted by the Center for Strategic and International Studies indicates that we have reached the inflection point where humans are unable to meaningfully distinguish between AI-generated versus human-created digital content.

Surveying more than 12,000 people across North America, the research found that participants were able to accurately discern between machine versus human-made media items around 51% of the time, on average. These results remained relatively consistent when detecting synthetic imagery, audio, silent video, and audiovisual media items. While text was not included in this study, other research has demonstrated that human detection of AI-generated text is equally, if not more challenging.

---

**Synthetic vs Authentic Media Identification**

*Figure source: Cooke et al. 2023*
Distinguishing between the real and the fake

That we can no longer rely on our eyes and ears to identify AI-generated content is likely of little surprise to many. Experts have been closely tracking the increasing realism of synthetic media since the first generative AI models were able to produce images in 2014. However, it was the release of publicly available models in 2022, such as ChatGPT and the text-to-image generator Stable Diffusion, which displayed not only how far this technology has advanced, but how easy it is for anyone to use. Since then, the volume of synthetic media has exploded, with researchers finding three times as many synthetic videos and eight times as many synthetic audio clips online now compared to 2022.

New and increasingly realistic synthetic media has also gone viral at a steady pace – from the humorous Balenciaga Pope photos to the more concerning Pentagon explosion tweet, which briefly affected the stock market.

Weighing the current benefits and risks to society of generative AI is a complex task. It has been employed in healthcare disability services, including giving back the voices of those who have lost them to medical conditions or helping the visually impaired navigate their environments more easily. It has also been used to raise awareness and educate others on atrocities, such as masking the identities of LGBTQ Chechens in a documentary on the persecutions they faced in their home country, and has enabled Holocaust survivors to preserve their stories and continue sharing them. More recently, discussions on generative AI have focused on how this technology could significantly enhance productivity, turbocharging the global economy.
Distinguishing between the real and the fake

There are numerous ways in which AI-generated content has been weaponised by actors seeking to perpetrate harm. This includes non-consensual pornography, which in 2019 accounted for 96% of all deepfake videos online. Today, many experts believe the number of victims of non-consensual pornography to be in the millions. Increasingly, investigations are uncovering the use of AI-generated child sexual abuse materials, while financial fraudsters and cybercriminals are employing generative AI to bolster social engineering attacks, phishing emails, extortion, and more.

This is underpinned by the supply of services dedicated to these illegal activities, from pornographic video apps to voice cloning products. Synthetic media is also being increasingly leveraged in espionage operations and even as part of ongoing conflicts, such as the viral 2022 synthetic video of Ukrainian President Volodmyr Zelenskyy calling for his troops to surrender, or the June 2023 fake TV and radio emergency broadcasts of Russian President Putin declaring martial law due to invasion by Ukrainian forces. As generative AI models continue to improve at pace, so too will the capability for generating convincing synthetic media, for better or worse.

A recording of the AI-generated emergency announcements of President Putin implementing martial law broadcasted by cyberhackers on Russian TV and radio stations, 2023.
Election threats

With the growing number of reported incidents of AI-generated content being used to interfere with political elections, the threat posed by synthetic media is shifting from theory to reality. Increasingly accessible commercial or open-source generative AI applications have made it easier, cheaper, and faster to create duplicitous content than ever before, as well as discrediting authentic digital content.

Disinformation

Generative AI tools can enhance disinformation efforts by enabling malicious actors to rapidly create large amounts of customisable synthetic media, across messages, images and audio. Experts worry about how this could be combined with other technology, like automated chatbots, to make fake accounts or websites publishing or promoting specific narratives which are more convincing to online users due to their lifelike nature. While not targeting political elections directly, numerous state-sponsored disinformation campaigns, including ones originating from China, Russia, and Venezuela have been discovered using synthetic media to bolster the credibility of their messages to foreign and domestic audiences, with some more convincing than others. Already, the number of AI-generated news websites has been found to be growing exponentially.
In addition, due to their public profile, politicians have long been a favoured target for AI-generated content. Some of this has been produced for educational or comedic purposes, such as the 2018 synthetic video of Barack Obama, or a series of photorealistic fake images of Obama and Angela Merkel on a seaside retreat together. But there is now a seeming trend of this content becoming less innocuous and more purposefully deceptive, as showcased by US President Biden being the subject of numerous duplicitous synthetic videos.

The 2023 presidential election in Turkey offers some recent insights into the impact of generative AI-enabled disinformation. One candidate, Muharrem Ince, withdrew from the race due to the publication and rapid circulation of a purported AI-generated sex tape depicting him. Throughout the campaign, fact-checking organisations have reported the growing visibility of fake news circulating during the Turkish elections, including both conventionally manipulated as well as AI-generated disinformation. Indian state elections have also already encountered numerous instances of political candidates being maliciously targeted with AI-generated content while campaigning.

Although still in the early stages, the 2024 US presidential election is seeing signs that synthetic media will be a key feature of campaigns. Some have been labelled as AI-generated, like the fictitious livestream debate of Donald Trump versus President Biden in July, or the earlier Republican National Committee political ad showing catastrophic scenarios which could occur if President Biden was re-elected. Others have not: one candidate’s campaign, Ron DeSantis, was discovered falsely portraying synthetic images of Donald Trump hugging former US Chief Medical Advisor Anthony Fauci as authentic, while Trump later retaliated with his own AI-generated video depicting DeSantis. Many anticipate that synthetic media will be leveraged by domestic parties with greater frequency as the campaign continues to progress, as well as any hostile state-based interference that may occur.
The second concern is how improvements in AI-generated content and the public’s growing awareness of this capability reduce trust in all digital content, which malicious actors could leverage by strategically discrediting real digital content for their own advantage. This has been termed ‘the Liar’s Dividend’. As the volume of synthetic media has grown, so too have accusations of authentic content being fake. In 2019, there was widespread belief that a video of the President of Gabon released by the government was AI-generated. Sowing confusion and unrest, the video helped fuel rumours that the government was hiding critical information about the president’s health, and later contributed to sparking a military coup.

In 2021, many dismissed a video published by Myanmar’s new leadership of a political prisoner confessing to the previous government leader’s crimes as being created using AI technology. In both cases, investigators did not find convincing evidence of these videos being synthetic. Earlier this year an audio clip in a post by the social media account of Sudanese military commander, Mohamed Hamdan Dagalo, was thought by many to be AI-generated despite the fact that analysis pointed to it being authentic, helping fuel the popular rumour that he was dead. As generative AI continues to improve, so does the public’s scepticism of digital content in general, enabling governments and political figures around the world to discredit genuine content as fake.
Election threats

Extortion and deception

The third fear is how candidates, policymakers, civil servants, election officials, and other parties playing a pivotal role in elections may be directly targeted to achieve specific political outcomes, such as through extortion or acts of deception. Individuals could be targeted with embarrassing but realistic synthetic media of themselves or tricked by a malicious actor impersonating a trusted ally. For instance, last summer, ‘live’ AI-generated software was discovered to have been used by an unknown imposter who was pretending to be the Kyiv Mayor Vitali Klitschko during a private video call with other European Mayors. Incidents like these are already occurring in the growing field of generative AI-enabled crime, where perpetrators have stolen millions of dollars from targets by pretending to be someone else using synthetic audio or text.

Regardless of the method, these developments collectively accentuate public uncertainty in being able to distinguish between real and fake, thereby undermining societal trust in electoral processes. This will threaten the stability of democratic systems which prioritise the free flow of information and access to alternative viewpoints.
The deceivers

It is also important to note that the scope of those who might leverage synthetic media to interfere with elections has grown, due not only to the increased accessibility of the technology but also because of evolving political landscapes.

Originally, activities such as these were largely the preserve of foreign nations seeking to undermine a target state’s political discourse. Yet the willingness of domestic parties to leverage disinformation to gain a political advantage in elections has been found to be a growing trend in numerous regions, from the Polish government’s troll farm\(^{62}\) to Nigerian politicians secretly paying\(^{63}\) social media influencers to spread falsehoods about opponents. Political campaigns are also increasingly amplifying\(^{64}\) misleading or manipulated content produced by others to drive desired narratives, further blurring the line between domestic political campaigning and adversarial influence. Coupled with the booming\(^{65}\) ‘disinformation for hire’ industry, which produced companies like Cambridge Analytica and the more recently exposed ‘Team Jorge’,\(^{66}\) these developments raise significant concerns about who is perpetuating AI-generated disinformation to gain a political edge.

![Synthetic video\(^{67}\) of Putin taking photos circulating on TikTok, 2023](image)
Recommendations

Research shows it has become increasingly challenging, potentially even impossible, to reliably discern between authentic and synthetic media.

In addition to this, barriers to using generative AI continue to lower. Combining these two factors poses concerns for how AI-generated content may be used to destabilise political elections in what is already an uncertain environment. Synthetic media has already been deployed repeatedly to interfere with various elections worldwide, and this trend is expected to continue. Governments, online platforms, and the AI practitioner community must act collectively to combat the growing threat of weaponised synthetic media. While the AI practitioner community and online platforms can each move to directly control synthetic media production and publication via regulation and industry standards, governments can implement key legislation to encourage and require widespread compliance. In particular, the following measures should be prioritised:

1. **Facilitate the development and establishment of generative AI content security guardrails**
   
   A robust safeguarding infrastructure implemented across generative AI tools is critical for preventing the manufacturing of illegal digital content and minimising the creation of other harmful media before they reach a wide audience.

2. **Fund and promote the improvement of digital authentication technology**
   
   Technologies such as machine detection models, and techniques like watermarking and content provenance have been vastly neglected when compared to investment in generative AI tools. More attention and resources need to be dedicated to these endeavours to make synthetic media easier to identify and track once published.

3. **Establish a synthetic media labelling system**
   
   A comprehensive apparatus to label AI-generated content would reduce the effectiveness of duplicitous synthetic media masquerading as genuine. AI-generated images, video, and audio labelling conventions will likely need to be different to text-labelling conventions, as the former category is better suited to embedding information while the latter is comparatively harder to detect.
Advancements in generative AI have now made it easier than ever to create convincing yet fake digital content, heightening the dangers posed by disinformation to political elections worldwide. There have already been several instances where synthetic media has been weaponised with the aim of interfering with electoral processes, and as the technology continues to improve it is expected the frequency of such incidents will also grow. Defending against this threat to election integrity will require a combination of interventions ranging from regulatory to technical initiatives, with governments, online platforms and the AI practitioner community working together to collectively raise the barriers to using synthetic media for nefarious purposes.

**About the Authors**

*Di Cooke* is an open philanthropy technology policy fellow in the International Security Program at the Center for Strategic and International Studies. Her areas of expertise include emerging technology policy within a defence and intelligence context, AI governance and risk, open-source intelligence (OSINT), and deception and counter-deception efforts in the digital space. Di has worked on policy-relevant research and activities at the intersection of technology and security across academia, government, and industry.
References


10. Di Cooke et al., [forthcoming] “AI-generated images, audio, and audiovisual content is close to indistinguishable from real content when presented in social media environmental conditions,” ArXiv (August 2023).

References


References


Synthetic Media and Election Integrity: Defending our Democracies
References


39. BuzzFeedVideo, “You Won’t Believe What Obama Says In This Video! 😂,” YouTube video, April 17, 2018, https://www.youtube.com/watch?v=cQ54GDm1eL0.


42. The Patriot Oasis (@ThePatriotOasis), “BREAKING: Biden calls for a national draft. Men and women are to be selected to fight in Ukraine [sic]…” Twitter post, February 27, 2023, https://twitter.com/thepatriotoasis/status/1630299734958112770.
References


References


56. Mohamed Suliman (@MuhammedKambal), “the detailed analysis shows that the recent voice recording for the RSF militia leader in #Sudan is authentic with 98% confidence...” Twitter post, May 24, 2023, https://twitter.com/MuhammedKambal/status/1661355761836908544.


References


