

RESEARCH PAPER

Countering AI Disinformation: Lessons from Taiwan's 2024 Election Defense Strategies

PANEL 4

The Role of Information in Democratic Resilience



Summer Chen

Summer Chen is an experienced journalist and fact-checker specializing in OSINT (Open Source Intelligence), fact-checking, and media literacy training. She served as the Chief Editor of the Taiwan FactCheck Center from 2019 to 2024, where she led the team in debunking mis- and disinformation related to regional conflicts, cross-strait military drills, and the COVID-19 and the elections. She and her team stepped in at key moments to stop mis/disinformation and reveal how it threatened Taiwan's democracy. She also provided fact-checking and media literacy training to journalists, teachers, and communities to help build Taiwan's information resilience.

This paper is circulated for discussion and feedback. The views expressed are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, CfDS, Faculty of Social and Political Sciences UGM or any other organization. The author(s) welcome comments on this version and invite you to contact them directly with any feedback or questions.

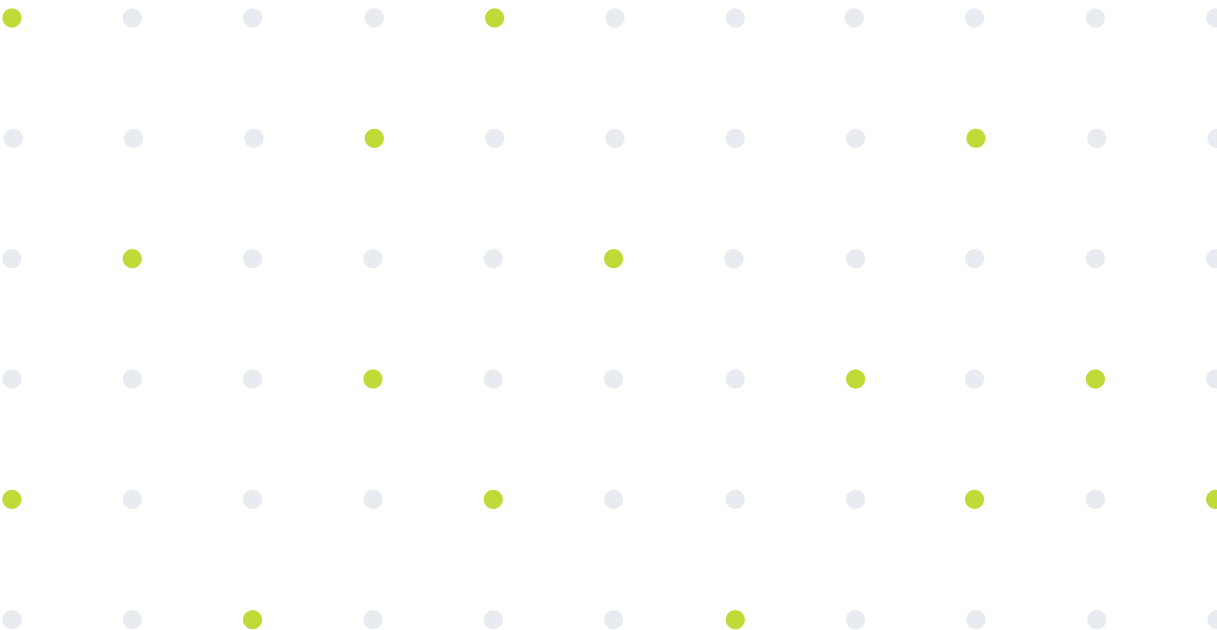


Countering AI Disinformation: Lessons from Taiwan's 2024 Election Defense Strategies

Summer Chen

This study examines the emergence and impact of AI-generated and deepfake disinformation during Taiwan's 2024 presidential and legislative elections. Although AI-generated content, deepfake, and AI-cloned audio did not become dominant tactics, they revealed evolving strategies for information manipulation. Drawing on official records, interviews, and firsthand observations, the report analyzes responses from both government and civil society—including legal amendments, law enforcement actions, and AI literacy initiatives. Law enforcement faced significant challenges, including limited AI verification tools, delayed responses from platforms, hard tracking origins and politically sensitive cases involving deepfake false denial. Civil society experimented with collaborative verification networks and public AI literacy education, achieving breakthroughs in public awareness while also encountering resource and capacity constraints. As AI-driven disinformation continues to evolve, its growing influence highlights the urgent need for proactive policies, stronger collaboration between tech experts and media professionals, and greater investment in training and AI literacy to strengthen information resilience.

Keywords: AI Disinformation, Deepfake, fact checking, AI Literacy, AI verification, information resilience




Introduction

Taiwan held its presidential and legislative elections in January 2024. During that time, deepfakes and AI-generated disinformation started to appear. Although AI technology was still developing, these types of false content had already shown up. In this election, AI was not yet the main tool used for information manipulation. However, it was clear that bad actors were testing AI to make content faster and cheaper. (Chen & Chen 2023; DoubleThink Lab 2024).

In the future, as these groups become more skilled with AI tools, disinformation will likely grow in both number and quality. This will create a bigger threat to the trustworthiness of the information environment during elections. Taiwan's experience in preparing for, responding to, and reflecting on the 2024 national election is worth reviewing. It can help Taiwan get ready for the next election and also provide lessons for the international community.

Looking back at the deep fakes and AI-generated disinformation that circulated during Taiwan's 2024 election, they can be grouped into three main types:

1. Video editing with AI voice cloning: AI was used to clone voices and alter news clips. For example, interviews with presidential candidates or U.S. lawmakers were edited with voiceovers expressing opposite views, distorting the original meaning.
2. AI-generated audio clips: Fake audio recordings using cloned voices of well-known public figures were created and widely shared on social media. These clips called on voters to support specific candidates, aiming to influence voter behavior. For example, Microsoft Threat Analysis Center, which has been closely monitoring China's information operations, detected that a pro-PRC threat actor known as Storm-1376—also referred to as Spamouflage—released an AI-generated fake audio clip of potential presidential candidate the day before the election, aiming to manipulate public opinion. (Clint Watts, 2024).
3. Fully AI-generated content: This includes items like the e-book *The Secret History of Tsai Ing-wen*, or fake stories about a specific candidate's affairs, secret children, or fabricated historical revelations. These materials often used exaggerated and sensational tone but lacked details and credible evidence. The videos were made using AI-generated visuals and AI news anchors, often incorporating photos collected from the internet. (Team T5, 2024) (DoubleThink Lab, 2024).



As for the disinformers of AI-generated disinformation, neither law enforcement nor civil society actors have directly identified the individuals or groups responsible. However, based on the content, the disinformation appears to serve two main purposes: first, to influence voters to support specific candidates; second, to discredit specific presidential candidates.


In this election, there were no malicious or threatening AI-generated videos of presidential candidates. However, examining how AI tools were used in disinformation provides insight into the current stage of technical development among disinformers. According to analyses by Taiwanese experts specializing in AI detection, one common method involved editing real news footage and combining it with AI-cloned voices to make the subjects' lip movements and facial expressions appear more natural and convincing—making such content harder for detection tools at the time to flag. Another method involved generating audio using AI and presenting it as a "leaked private recording." These AI-generated audio clips are harder to verify due to the lack of visual cues and limited available verification tools, and were mainly spread through peer-to-peer platforms like LINE. Experts also suggest that since AI-generated video still tends to show technical flaws, disinformation actors have focused primarily on these two audio-based approaches (Andy Chen & Summer Chen, 2023).

In terms of reach and influence, the three types of AI-generated disinformation had limited impact during this election. Although Team T5 noted that AI-generated rumors—such as alleged secret histories of Tsai Ing-wen or claims about candidates having affairs and illegitimate children—appeared across multiple platforms, in various languages, and had high share counts. (Team T5, 2024). These claims failed to trigger significant public reactions, and did not enter mainstream media. As a result, they have not yet meaningfully affected the overall information ecosystem.

From the perspective of impact, the spread of the three types of AI-generated disinformation mentioned above was limited. These AI-driven messages were mainly amplified by fake accounts on social media, but they did not reach mainstream media or trigger significant public reactions. As a result, they have not yet had a real impact on the broader information ecosystem in Taiwan.

Methodology and Data Sources

To prevent the potential threat of AI-generated disinformation, both the Taiwanese government and civil society took independent actions and measures. Their goal was to stop misleading AI and deepfake content from causing harm to democracy during critical and



tense moments in the election, and to ensure fairness in the flow of election information. Although these defense mechanisms were not fully activated during this election, their existence highlights an urgent need to learn from the experience and strengthen future preparedness as AI-generated disinformation continues to evolve.

This study covers the period from September 2023 to January, 2024, the day of the election. It observes and documents the types and impacts of AI-generated disinformation during this time. The research focuses on how different actors—such as government agencies, legislative bodies, police and law enforcement units on the official side, and media, fact-checking organization, and research institutions on the civil society side—each took steps to build mechanisms for defending against and responding to AI-driven disinformation. The report also reflects on how these actors viewed the election process and offers policy and practical recommendations for countering AI disinformation in the future.

Sources for this study include the author's firsthand experience and observations as Chief Editor of the Taiwan FactCheck Center (2019/5–2024/2), documents provided by the Investigation Bureau and prosecutors, interviews with relevant officials and law enforcement personnel, as well as public reports from research institutions.

Dual Actors in AI Disinformation Defense

In defending against deepfake and AI-generated footage in the 2024 election, one main actor is the government's law enforcement agencies, while the other is civil society. Taiwan's law enforcement agencies and the Central Election Commission (CEC), in order to maintain neutrality, operate independently from political parties and adhere strictly to legal procedures. For fact-checking and media literacy organizations, public trust and credibility are built on their independence and non-affiliation with any political party. Consequently, while government and civil society operate through different mechanisms, they work independently but complement each other's efforts.

Amendments to Electoral Laws in Response to AI-Generated Disinformation

To address potential AI-generated and deepfake disinformation in the 2024 elections, Taiwan amended its laws on May 26, 2023. Provisions targeting AI-generated and deepfake disinformation are added to the [Presidential and Vice Presidential Election and Recall Act](#) and the [Public Officials Election and Recall Act](#).

Under the new regulations in the Presidential and Vice-Presidential Election and Recall Act and the Public Officials Election and Recall Act, creating or disseminating AI-generated and deepfake voices, images, or records with the intent to influence elections can lead to up to 7 years in prison. Additionally, tech platforms and media outlets are required to restrict or remove flagged content within two days of notification, or face fines from NT\$200,000 to NT\$10 million.

This regulation applies to the period between the official election announcement and the day before voting. Both candidates and the general public may request content verification through law enforcement or investigation agencies. Once the authorities confirm that the content is a deepfake or AI-generated disinformation, the candidate may use the official verification document to notify technology platforms and the Central Election Commission (CEC). The CEC will then coordinate with the platforms and media outlets.


Upon receiving such notice, platforms and media are required to stop broadcasting, remove the content, take down websites, or restrict access within two days. Failure to comply may result in fines ranging from NT\$200,000 to NT\$10 million. Continued non-compliance may lead to repeated fines. However, in this election, there were no reported cases in which disinformation was removed or taken down through this mechanism. (Legal Research Center, Supreme Prosecutors Office, Taiwan, 2023).

Legal Enforcement Mechanisms in the Context of the Election

To strengthen enforcement, Taiwan's Legal Research Center under the Supreme Prosecutors Office released a report titled "Case Studies on AI-Generated or Deepfake Audio, Video, Images, and Text that Undermine Electoral Integrity." The report provides legal interpretations, case analyses, and serves as a training resource for internal use by investigative and law enforcement agencies.

After the official announcement of candidate registration for the election, Taiwan has appointed dedicated prosecutors in six major cities and established a nationwide "AI-Generated and Deepfake Disinformation Case Processing Center." Three prosecutors work in shifts around the clock in the month leading up to the election. (Interviewee 1)

During the election period, the Central Election Commission (CEC) established communication channels with four major technology platforms commonly used by the Taiwanese public: Google, Meta, LINE, and TikTok (Chen, 2023). Among them, TikTok, which



does not have an office in Taiwan, communicated with the CEC through an outsourced public relations firm. After setting up the communication mechanism, the CEC and the platforms adopted a case-by-case reporting system. However, no routine mechanism or regular meetings have been established to date (Interviewee 2, 2024).

Some AI-generated and deepfake disinformation was proactively monitored and investigated by law enforcement at the start of the rumors' circulation, such as videos falsely portraying one presidential candidate praising their opposition and the video claiming one candidate has an illegitimate child. However, law enforcement officials noted that after reporting such cases to tech platforms, their responses were often inefficient and unclear.

Enforcement Outcomes and Reflections After the Election


During the 2024 election, law enforcement agencies held press conferences and issued statements to address certain types of AI-generated and deepfake disinformation. These included fake videos showing a presidential candidate praising their rival, or falsely claiming a candidate had an illegitimate child. In these cases, the authorities acted quickly—they started monitoring the content early, launched investigations, and publicly clarified the facts through press briefings. This also helped raise public awareness about AI manipulation.

However, the law enforcement indicated that when they reported such cases to the platforms, the responses were often slow and unclear. Because of this, officials sometimes chose to debunk the claims directly through press conferences, instead of relying on the platforms to take the videos down.

In short, law enforcement still faced several limits and challenges in handling these cases, including:

- **Inefficient Platform Response:** Platforms have slow response times and low feedback rates.
- **Lack of AI Verification Tools:** AI Verification technologies remain underdeveloped.
- **Tracing Difficulties:** Rumor-mongers often use VPNs or free online forums, making it hard to trace origins.

In this election, the public did not express concern that the removal of AI-generated or deepfake disinformation would infringe on freedom of speech. However, another case highlighted the challenges of law enforcement. In this case, a politician's private videos were



leaked, and the individual publicly claimed the content was created using deepfake technology. This was later viewed as a case of deepfake false denial—where a person falsely attributes authentic content to deepfake manipulation in order to deny its authenticity. The politician filed a formal complaint and requested law enforcement to conduct forensic verification. However, because the results of such verification could significantly influence the election, law enforcement agencies found themselves in a difficult position. They had to carefully balance the need for transparency, political neutrality, and the protection of personal privacy. As a result, verification outcomes could not be released in a timely manner—or, in some cases, were ultimately withheld. The decision not to disclose the results also brought intense political controversy and pressure.

The Challenge of Deepfake False Denial in Law Enforcement

In this election, the public did not express concern that the removal of AI-generated or deepfake disinformation would infringe on freedom of speech. However, another case highlighted the challenges of law enforcement. In this case, a politician's private videos, photos and recordings were leaked, and the individual publicly claimed the content was created using deepfake technology. They requested law enforcement to conduct forensic verification. However, because the results of such verification could significantly influence the election, law enforcement agencies found themselves in a difficult position. The forensic results from law enforcement were never made public, which led to criticism from political opponents and the media.

This case illustrates the complex challenge posed by deepfake false denial. When individuals claim that genuine content is fabricated using AI, law enforcement agencies face immense pressure. They face the challenge to carefully balance the need for transparency, political neutrality, and the protection of personal privacy. As a result, verification outcomes could not be released in a timely manner—or, in some cases, are ultimately withheld. The decision not to disclose the results leads to political controversy and intense scrutiny from both rival politicians and the media.

Civil Society's Response to AI Disinformation: Verification and Education in Action


During the election period, another key force in countering AI-generated disinformation was a civil defense network formed by fact-checking organizations, media literacy groups, and institutions researching media and information warfare. Within this network, the media played a crucial “gatekeeping” role. When reporting or rewriting viral topics or rumors from social media, media outlets lacking verification capacity could easily become distribution nodes exploited by disinformation actors—allowing false claims to be laundered into seemingly credible news reports.

To strengthen AI literacy among media professionals and fact-checking journalists, the Taiwan FactCheck Center (TFC) collaborated with Software Technology Institute of the Institute for Information Industry in 2023 to connect with Taiwanese scholars and experts who are developing AI forensics tools and technologies. They compiled a list of AI detection and verification experts in areas such as image, audio, and text analysis. They gathered information on each expert's research focus and asked whether they would be willing to assist journalists and fact-checkers in identifying AI-generated content during critical election events. As a result, TFC established a working network of AI specialists open to collaboration with the media and gained access to a broader tech community capable of supporting AI verification efforts.

At the same time, the National Institute of Cyber Security provided technical support and AI detection knowledge and tools. Together with TFC, they helped develop AI verification methods and AI literacy materials, combining technological expertise with fact-checking methodologies.

TFC launched two major AI literacy initiatives. For media professionals, TFC organized two workshops: one for editors-in-chief focused on raising awareness about the threats posed by AI disinformation and introducing verification guidelines, and another hands-on training session for 40 journalists and fact-checkers on how to verify AI-generated content. For students, educators, and local communities, TFC promoted AI literacy through explanatory articles, interactive online quizzes, public talks, and community workshops—helping the public improve their ability to recognize deepfakes and AI-generated content during the election.

In addition, Taiwan Media Watch trained volunteers and teachers to guide students in playing Election Wind Direction, an educational board game simulating the manipulation of



information and public opinion during an election. Through gameplay, participants practiced identifying and countering disinformation and influence tactics in a hands-on, engaging way.

This section presents key observations and feedback on AI literacy initiatives, as well as developments in the fact-checking and media literacy fields during the election. The following points summarize the main findings:

1. Fact-checking organizations are still developing their AI detection capabilities.


In some cases involving AI-generated footage, law enforcement agencies issued clarifications before fact-checking organizations released any fact checks or explanatory articles. This is because fact-checkers are still in the early stages of developing the methodology and technical skills and experience needed to verify AI-generated visuals. Their work in areas such as social media monitoring, verification methods, and the use of relevant tools is just beginning.

As AI technologies evolve rapidly, fact-checkers and media professionals must collaborate with AI detection experts to build a community or network. The community can help analyze manipulation tactics, share knowledge, invent AI detection tools and promote the use of open-source tools. Such collaboration is essential to keep pace with the fast-changing nature of AI-driven information operations.

2. It is important for the media to build AI verification capacity and publish AI-verifying guidelines both for their reporters and audience.

Interviews with media professionals show that most newsrooms in Taiwan are not fully prepared to verify disinformation or AI-generated content, and often rely on partnerships with fact-checking organizations (Hung et al., 2024). In contrast, the Taiwan FactCheck Center built a network of AI experts, developing knowledge, techniques, and methodologies for AI verification, and organizing workshops to train both journalists and fact-checkers. TFC also made AI literacy among the public. These efforts help strengthen the media's gatekeeping role and raise public awareness of AI-related risks.

However, these efforts remain at a very early stage. Currently, fact-checking organizations and media outlets still lag far behind the rapid development of AI-generated image and audio technologies in terms of verification capacity. Both newsrooms and fact-checking organizations must continue to invest in resources and training to effectively respond to this fast-evolving challenge.



Going forward, media and fact-checking organizations can take several key actions: first, strengthen the visual verification skills of journalists and editors, especially in the areas of image and audio authentication. Second, develop and publicly share newsroom guidelines for detecting AI-generated disinformation to establish transparent verification processes and enhance public trust. Third, expand public-facing AI literacy efforts by producing accessible educational content that teaches people how to recognize and interpret AI-generated visuals. These measures can help raise the overall information literacy of society and reduce the potential threats AI disinformation poses to democratic systems.

3. Law enforcement and civil society have different but complementary roles in countering disinformation

Law enforcement agencies and civil society operate independently, and their approaches to countering disinformation are not the same. When law enforcement agencies take legal action or issue official statements and press releases to punish both the disinformers and disseminators of disinformation. They are often perceived as representatives of the government or the ruling party, and their motives may be subject to public skepticism. In contrast, civil society organizations—such as fact-checking groups and media literacy initiatives—generally operate independently from political parties and are more likely to be seen by the public as neutral and trustworthy third parties. As a result, they often hold greater credibility when addressing politically sensitive disinformation.

Fact-checking and media literacy organizations in Taiwan have earned a significant level of public trust. According to the 2024 Annual Disinformation Survey conducted by the department of Journalism at National Taiwan University, 74% of respondents were aware of Taiwan's major fact-checking organizations—such as the Taiwan FactCheck Center (TFC), MyGoPen, and CoFacts. More than 70% of respondents had used these services, and over 70% said they trusted these civil society fact-checking organizations when it came to addressing sensitive social issues (Hung et al., 2025).

Conclusion and Recommendation


In summary, the main findings of this research are as follows:

1. Deepfake and AI-generated disinformation emerged during Taiwan's 2024 election, although they did not become the primary tactics of information operations at the time. These disinformation cases can be grouped into three types: AI-cloned audio

files, edited videos combined with AI-generated voices, and fully AI-generated fabricated content. However, there were no confirmed cases of fully AI-generated videos of candidates being used to influence the election. This reflects the stage at which disinformation actors were using AI technology at the time.

2. [Taiwan's law enforcement agencies and civil society have proactively prepared defenses against AI-generated and deepfake disinformation.](#) Law enforcement actively monitors and investigates, while civil society promotes AI literacy, preventing this misinformation from gaining influence. Government agencies and civil fact-checking organizations operate independently but effectively complement each other.
3. [Taiwan amended its laws to impose up to seven years in prison for deepfake and AI-generated disinformation intended to influence elections, requiring tech platforms and media outlets to remove verified content or face fines ranging from NT\\$200,000 to NT\\$10 million in May 2023.](#) During the election period, dedicated prosecutors were appointed in six cities, and an "AI-Generated or Deepfake Disinformation Case Processing Center" was established one month before the voting day. In practice, the Central Election Commission (CEC) interacts with tech platforms on a case-by-case basis, with no routine meetings in place.
4. Despite the establishment of legal frameworks and dedicated units, law enforcement agencies continue to face significant challenges in countering AI-generated disinformation. [One major issue is the inefficient response from tech platforms—responses are often slow and inefficient.](#) Tracing the origins of disinformation is also extremely difficult, as rumor-mongers frequently rely on VPNs, disposable accounts, and anonymous forums to conceal their identities. These combined challenges have created critical enforcement gaps.
5. Civil society actors, including fact-checking organizations and media, enhance public awareness of AI disinformation through fact checks and AI literacy.


Given the rapid advancement of AI-driven disinformation, building a collaborative AI verification community among media professionals, fact-checkers, and technology experts is a key strategy to strengthen the media's gatekeeping function. By bridging the gap between journalism and AI verifying technology, this collaborative approach helps ensure that newsrooms are better equipped to identify and respond to emerging AI threats.



Based on the experience from Taiwan's 2024 election, the following recommendations are proposed to maintain a healthy information ecosystem amid rapid AI development, ensuring election integrity and defending democracy:

1. **Legislation and Policy for AI:** Enact regulations requiring AI products to be publicly trustworthy technologies. Legislation should mandate that AI products include watermarks, original source data, or similar measures, to prevent AI technology from being exploited for fraud, scam and disinformation.
2. **Independent Mechanisms for Law Enforcement and Civil Society:** During elections, law enforcement and civil society should handle AI-generated and deepfake disinformation on their own mechanisms. Law enforcement should investigate autonomously to uphold electoral integrity through judicial independence, while civil society, serving as a government watchdog without ties to political parties or figures, should focus on debunking rumors and promoting AI literacy. This independent role enables public trust and allows civil society to act as a guardian of truth in politically turbulent times.
3. **Establish an AI Verification and Detection Expert Community:** Create a community of stakeholders with high demand for AI verification and detection technology, including AI experts, law enforcement, journalists, fact-checkers, and AI tools developers. Through collaborative effort, this community can learn AI techniques, develop tools, and refine verification methods for AI-generated contents.
4. **Capacity Building for Law Enforcement:** At the onset of elections, enhance the capabilities of verifying personnel in law enforcement and facilitate knowledge exchange with other countries to learn the latest verification techniques. During the election period, establish a standard enforcement process for handling AI-generated and deepfake disinformation, with internal training for relevant law enforcement personnel.
5. **Enhance AI Literacy:** Invest resources in training and upskilling media professionals and fact checkers in AI literacy. For the public, extend long-established media and digital literacy programs to include AI literacy, helping people understand AI technology, recognize the potential risks of AI-generated disinformation, and develop skills to filter and find the credible resource of information.

To address the potential spread of AI-generated disinformation and deepfakes during elections, both law enforcement and civil society must take preventive measures in advance.



Governments should establish clear response procedures and verification mechanisms, strengthen inter-agency coordination, and enhance enforcement capacity. Civil society can contribute by promoting AI literacy, building AI-verification communities, and developing tools and educational resources to help the public recognize manipulated content. Taiwan's experience during the 2024 national election shows that even though AI disinformation did not cause large-scale disruption, early preparations—through legal, technical, and educational strategies—played an important role in reducing risks. This approach offers valuable lessons for other democratic societies.

References

- Andy Chen & Summer Chen (2023/11/29), [Rumor Tracker] Did Lai Ching-te Say the KMT–TPP Alliance Is the Right Combination? AI-Altered Video Emerges in Taiwan’s Presidential Election, Taiwan FactCheck Center. Retrieved from: https://tfc-taiwan.org.tw/migration_article_105106_9949/
- Clint Watts (2024), China Tests US Voter Fault Lines and Ramps AI Content to Boots Its Geopolitical Interests-Microsoft on the Issues.
- Chen-Ling Hung, Wen-Cheng Fu, Chang-Ce Liu, Hui-Ju Tsai, AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election (2024), Thomson Foundation. Retrieved from: https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf
- Chen-Ling Hung, Ji-lung Hsieh, Chih-hsin Sheen, Yu-tzung Chan (2025) 2024 Survey on Media Literacy and Misinformation, National Taiwan University.
- Chao-Chien Chen (2023/12/14) Countdown to the Election! CEC Establishes Task Force to Combat Disinformation. Indigenous Television (TITV 16). Retrieved from: <https://www.ipcf.org.tw/zh-tw/News/Detail?newsId=23121420492006371>
- DoubleThink Lab (2024), 2024 Taiwan Election: The Increasing Polarization of Taiwanese Politics — Reinforcement of Conspiracy Narratives and Cognitive Biases. Retrieved from: <https://reurl.cc/YYx8aL>
- Taiwan’s Legal Research Center under the Supreme Prosecutors Office (2023), Case Studies on AI-Generated or Deepfake Audio, Video, Images, and Text that Undermine Electoral Integrity. Retrieved from: <https://reurl.cc/eMrXpK>
- Taiwan FactCheck Center (2024), 2023 Impact Report of TFC.
- Team T5 (2024), Cyber Threats against Taiwan’s 2024 Presidential Election.

Interview Participant Information

The following table lists the interview participants cited in this study. For confidentiality and clarity, each participant has been assigned a code (e.g., Interviewee 1, Interviewee 2). Their professional status and the date of the interview are also provided.

Participant	Status	Interview date
Interviewee 1	Prosecutor	2024-10-3
Interviewee 2	Central Election Commission official	2024-10-17

Appendix: Legal Amendments

Presidential and Vice Presidential Election and Recall Act

Article 90, Paragraph 2

Whoever commits any offense in the preceding paragraph by disseminating, broadcasting or distributing by any other means deep-fake voice, image, or electronic recordings of candidates in the election, the primary persons who propose a recall, or persons subject to recall shall be sentenced to a fixed term of imprisonment of not more than seven years.

Presidential and Vice Presidential Election and Recall Act

Article 47-3 第四十七條之三

From the date public notice of an election is issued or an established recall campaign is declared until the day before election day, if a prospective candidate, candidate, person subject to recall, or the primary person who proposed a recall is aware that there is a deepfake of their own voice or likeness that has been broadcast on television or published on the internet they may request an investigation by submitting a completed application form and paying the required fee.

The term deepfake that is used in the preceding paragraph refers to the use of digital composites or other technological methods used to create a form that convincingly performs speech and actions that are not those of the actual person.

If a prospective candidate, candidate, person subject to recall, or the primary person who proposed a recall requests the police investigated detailed in Paragraph 1 and the voice or likeness are found to be a deepfake, they should submit the investigation dossier along with a written request to the broadcasting businesses, internet platform provider, or internet application service provider so that they may address, in accordance with

Paragraph 4, the broadcast or published of the speech or likeness, and inform the Central Election Commission.

Within two days from the date of receipt of the request detailed in the preceding paragraph, the television station, internet hosting service or internet application service provider shall comply with the following provisions:

1. Broadcast television stations shall stop broadcasting the voice and likeness.
2. Internet hosting services and internet application service providers shall restrict browsing and remove or take down the voice and likeness.

Broadcast television stations, Internet hosting services and internet application service providers shall, within six months from the date of receipt of the request referenced in Paragraph 3, retain the electronic records or webpage data of the voice or likeness that was broadcast or published, as well as the data of the entrusted broadcaster or publisher and their internet usage record data; in the event of litigation, the retention shall be extended to three months after the judgment is finalized.

Regulations governing the request for investigation referenced in Paragraph 1 and related matters, including eligibility, procedures, forms, the format of video and audio files, fees, the content that shall be included in the investigation dossier issued by the police shall be determined by the Ministry of the Interior.

Presidential and Vice Presidential Election and Recall Act

Article 96, Paragraph 5

Whoever violates Paragraph 4 of Article 47-3 and who fails to stop broadcasting, restrict browsing, or remove or take down a website shall be imposed a fine of not less than NT\$200,000 and not more than NT\$10 million and shall be ordered to rectify the situation within a certain period of time. If the situation is not rectified within the specified period, the penalty shall be successively imposed.

Public officials Election and Recall Act

Article 104, Paragraph 2

Whoever commits any offense in the preceding paragraph by disseminating, broadcasting or distributing by any other means deep-fake voice, image, or electronic recordings of

candidates in the election, the primary persons who propose a recall, or persons subject to recall shall be sentenced to a fixed term of imprisonment of not more than seven years.

Public Officials Election and Recall Act

Article 51-3, Paragraph 2

From the date public notice of an election is issued or an established recall campaign is declared until the day before election day, if a prospective candidate, candidate, person subject to recall, or the primary person who proposed a recall is aware that there is a deepfake of their own voice or likeness that has been broadcast on television or published on the internet they may request an investigation by submitting a completed application form and paying the required fee.

The term deepfake that is used in the preceding paragraph refers to the use of digital composites or other technological methods used to create a form that convincingly performs speech and actions that are not those of the actual person.

If a prospective candidate, candidate, person subject to recall, or the primary person who proposed a recall requests the police investigated detailed in Paragraph 1 and the voice or likeness are found to be a deepfake, they should submit the investigation dossier along with a written request to the broadcasting businesses, internet platform provider, or internet application service provider so that they may address, in accordance with Paragraph 4, the broadcast or published of the speech or likeness, and inform the Central Election Commission.

Within two days from the date of receipt of the request detailed in the preceding paragraph, the television station, internet hosting service or internet application service provider shall comply with the following provisions:

1. Broadcast television stations shall stop broadcasting the voice and likeness.
2. Internet hosting services and internet application service providers shall restrict browsing and remove or take down the voice and likeness.

Broadcast television stations, Internet hosting services and internet application service providers shall, within six months from the date of receipt of the request referenced in Paragraph 3, retain the electronic records or webpage data of the voice or likeness that was broadcast or published, as well as the data of the entrusted broadcaster or publisher

and their internet usage record data; in the event of litigation, the retention shall be extended to three months after the judgment is finalized.

Regulations governing the request for investigation referenced in Paragraph 1 and related matters, including eligibility, procedures, forms, the format of video and audio files, fees, the content that shall be included in the investigation dossier issued by the police shall be determined by the Ministry of the Interior.

Public Officials Election and Recall Act

Article 110-5

Whoever violates Paragraph 4 of Article 51-3 and who fails to stop broadcasting, restrict browsing, or remove or take down a website shall be imposed a fine of not less than NT\$200,000 and not more than NT\$10 million and shall be ordered to rectify the situation within a certain period of time. If the situation is not rectified within the specified period, the penalty shall be successively imposed.

Disclosure: This report used ChatGPT to assist with English language editing. However, all content and analysis are the result of the author's original research and writing.



INFORMATION RESILIENCE & INTEGRITY SYMPOSIUM

Generative AI and Information Resilience
in the Asia-Pacific: Actions and Adaptations

Faculty of Social and Political Sciences
Universitas Gadjah Mada

21 August 2025