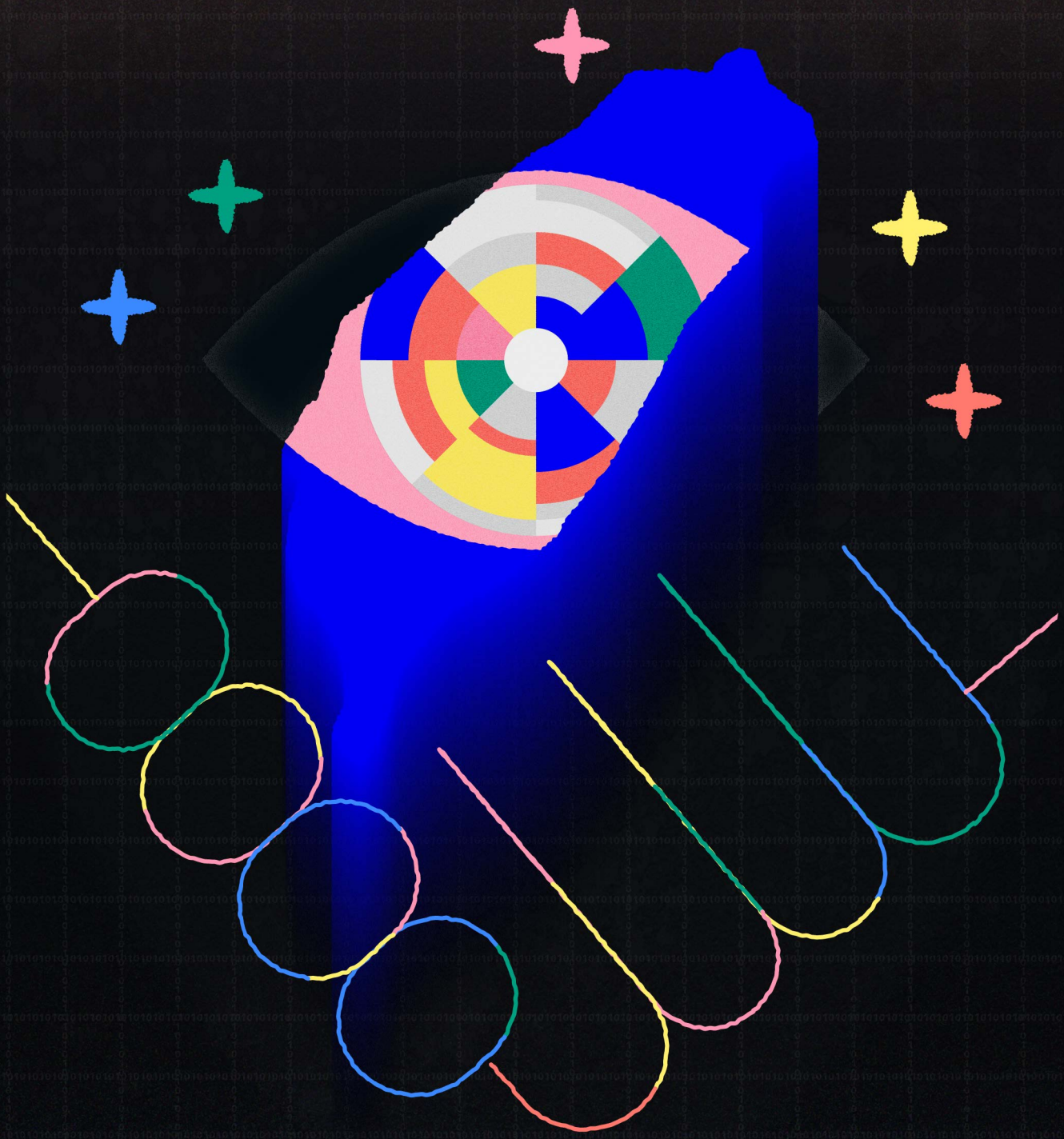


Resilience in Truth

Public-Private Collaboration in Taiwan's Response to Disinformation

Kai-Shen Huang, Muyi Chou 2025

Resilience in Truth

Public-Private Collaboration in Taiwan's Response to Disinformation

Kai-Shen Huang, Muyi Chou 2025

Research Institute for Democracy, Society, and Emerging Technology (DSET)

Research Institute for Democracy, Society and Emerging Technology (DSET) champions Taiwan's democracy as the guiding principle for its policy research. Emerging technologies are changing the global landscape, presenting both opportunities and challenges across various political and social spheres. Our mission is to develop technology governance frameworks that safeguard security and value freedom.

Democratic Governance Program

The Democratic Governance Program investigates the impact of critical technologies on democratic process and integrity, both in Taiwan and globally. Our key focus areas include artificial intelligence, information manipulation, and supply chain resilience. We explore their integration within democratic frameworks, emphasizing Taiwan's unique position within geopolitical contexts and its role in navigating the complex dynamics of global technological freedom. Our objective is to provoke critical reflection on maintaining democratic practices amid the rapid changes of technological development and international order.

Authors

Kai-Shen HUANG (D.Phil., Oxford University)

Huang is currently a research fellow at DSET, where he is the Director of the Democratic Governance Program. His research focuses on AI ethics, disinformation campaigns, and supply chain resilience. Previously, he researched AI applications in dispute resolution and public administration in Shanghai. He earned his DPhil in Anthropology from Oxford University in 2020.

Muyi CHOU (Ph.D., Humboldt University of Berlin)

Chou is a deputy director at DSET and an assistant professor at National Taiwan Ocean University. She obtained her PhD in Political Science from Humboldt University of Berlin. Her research interests include deliberative democracy, the social and solidarity economy, and social innovation, with a more recent focus on AI and social defense.

Contributors

Billy Zhe-Wei LIN (M.Sc., National Sun Yat-sen University)

Lin is currently a research fellow at DSET and leads the data team there. His work is dedicated to exploring pressing issues at the intersection of digital policy and disinformation campaigns, focusing on understanding and addressing the challenges posed by the digital age.

Y. Shane WANG (HBA, University of Toronto)

Wang is a policy analyst at DSET. He completed his HBA with distinction in Economics at UofT in 2024. His research interest spans from the sciences of antiquity to theories of the political economy to the social impacts of modern technologies.

Contributors

Pei-Chen CHENG

(PhD candidate, University at Albany, State University of New York)

Cheng is a non-resident fellow at DSET and a graduate of the Department of Sociology at SUNY Albany. Her research focuses on gender, politics, and inequality among children and youth, with particular attention to how mothers draw on their lived experiences to shape discourses and advocate for children's needs in public playground design. She is currently pursuing a doctoral degree, with a focus on childhood inequality.

Tzu-Ying HO (MA student, Tunghai University)

Ho is currently a research assistant at DSET, where she is involved in the Democratic Governance Program. Her research focuses on democratic governance and technology for teenagers. She is a graduate student in Philosophy at Tunghai University.

Renwei CHANG (PhD student, National Tsing Hua University)

Renwei Chang, Associate Researcher at DSET and a member of the Democratic Governance Program. Currently pursuing a Ph.D. at National Tsing Hua University, his research centers on the challenges and threats faced by civil society amid digital transformation.

Acknowledgements

This publication is based on a series of research projects initiated in January 2024, under the guidance of DSET's advisory board. Special thanks are also due to numerous experts and organizations, and to all the associated researchers contributing to the publication, Taiwan Pang-phuann Association of Education, FakeNewsCleaner, Taiwan FactCheck Center, MyGoPen, Cofacts, Doublethink Lab, Taiwan Information Environment Research Center, and Taiwan AI Labs.

Published in 2025 by the Research Institute for Democracy, Society and Emerging Technology (DSET).

Table of Contents

Summary

Information manipulation, operations aimed at influencing the opinions of certain people using carefully crafted deceptive narratives, is an age-old phenomenon. Many sectors of Taiwanese society have organically developed mechanisms to counter the manipulation campaigns. This report examines the impact of disinformation and information manipulation campaigns in Taiwan, focusing on how the government, digital platforms, and nongovernmental organizations have attempted to curb its impacts. This report utilizes the DISARM Blue framework to analyze existing efforts, identify the shortcomings, and offer policy recommendations.

Objectives

This report is structured around four objectives:

1. **Presenting the Taiwanese government's policy initiatives against disinformation**

   Provide a brief overview of the Taiwanese government's policy initiatives—including legislative amendments, executive decisions, public-private partnerships, and white papers—by the Executive Yuan and its subsidiary agencies to curb disinformation and mitigate its impacts.

2. **Comparing the anti-disinformation policies of cross-national and local digital platforms**

   Compare and contrast the cross-national and local digital platforms' policies, or the lack thereof, on user-generated disinformation. The platforms include LINE, Facebook/Instagram, WhatsApp, Google, YouTube, Douyin, TikTok, PTT, Dcard, and Bahamut.

3. **Introducing the Taiwanese nongovernmental organizations dedicated to countering disinformation and information manipulation**

   Highlight the works of eight media literacy advocacy, fact-checking, and anti-information manipulation organizations which have significantly bolstered Taiwan's defenses against disinformation and information manipulation, and report on the opinions of these NGOs' leaders.

4. **Analyzing the shortcomings of existing efforts and presenting policy recommendations**

   Holistically evaluate the past and present efforts by the government, digital platforms, and nongovernmental organizations against disinformation and information manipulation in Taiwan; identify their shortcomings; and propose policy recommendations using the DISARM Blue framework.

Findings

This report identifies three major findings:

1. Taiwan has developed an organic defense system through the close collaboration between government agencies, cross-national digital platforms, and nongovernmental organizations.

2. There are ways to improve upon the existing defense system, such as by strengthening government regulations and by enhancing media literacy.

3. While AI-generated disinformation has had a limited impact on Taiwan's 2024 elections, we must not ignore its ability to deepen social cleavages and undermine democratic institutions.

Policy Recommendations

This report proposes ten policy recommendations for further action:

1. Continuing Public-Private Cooperation

The government should foster collaboration among agencies, civil society, and digital platforms to continuously monitor and respond to evolving information manipulation tactics.

2. Exposing Foreign Manipulation Campaigns

Foreign actors exploit Taiwan's free speech to spread disinformation. Increased transparency about these activities is crucial to raise public awareness and support for regulations to counter foreign interference.

3. Building a Real-Time Government Response System

The Ministry of Justice Investigation Bureau may lack authority to lead a comprehensive response against disinformation. A government-wide command system is needed to coordinate responses to disinformation, including fact-checking, clarification, and legal actions.

4. Investing in the Public Media

By investing in public media, the government can create a more competitive media landscape. This will encourage private media to improve their quality and provide citizens with more reliable information, fostering a healthier democracy.

5. Expanding Media Literacy Using Digital Platforms

To improve media literacy, the government should partner with online platforms to offer free courses. These courses should teach critical evaluation skills and basic OSINT techniques to empower citizens against disinformation.

6. Creating a Platform for Information Manipulation Research

The government should encourage NGOs to collaborate using shared OpenCTI servers to pool research findings on information manipulation. Government funding for conferences and workshops will facilitate knowledge sharing and international cooperation, enhancing Taiwan's ability to combat disinformation.

7. Constructing a Legal Framework for Government-Platform Interactions

The lack of legal clarity hinders effective government-platform cooperation in addressing information manipulation. A legal framework is crucial to define communication channels and procedures, enabling coordinated responses to emerging threats.

8. Requiring Platforms to Label AI-Generated Content

Platforms should allow users to label AI-generated content and have mechanisms to address the misuse of AI. Clear legal guidelines are needed to prevent disputes between platforms and users.

9. Enhancing Platform Accountability

Platforms' algorithms can amplify disinformation and enable malicious activity. Governments must hold platforms accountable, requiring them to address fraud, protect user privacy, and ensure fair elections. The IFES guidelines provide a framework for collaboration to achieve these goals.

10. Developing an Evaluation Mechanism

Taiwan lacks a system to evaluate the effectiveness of its anti-disinformation efforts. A comprehensive evaluation mechanism, including long-term data collection, is crucial to inform future strategies and ensure these efforts effectively address societal challenges.

I. Taiwan's Defenses Against Disinformation

1. Introduction

Information manipulation goes far beyond the simplistic notion of spreading "alternative facts." It is a sophisticated operation, involving a range of strategic actions such as selecting topics, targeting specific audiences, crafting tailored messages, and choosing the right dissemination channels. It also includes follow-up tactics: prompting offline actions, evaluating the success of campaigns, and erasing the evidence of manipulation. At its core, information manipulation is a deliberate attempt to distort the information environment, often with serious political or social consequences for the target.

Taiwan has proven remarkably resilient against such tactics, thanks largely to the vigilance of its civil society. Private organizations, as noted by the Australian Strategic Policy Institute, play a pivotal role in detecting and countering disinformation in real time, often stepping in before government agencies can act.[1] The Taiwan Communication Association (臺灣傳播學會) added that this success was the result of a combined effort involving the government, civil society, and the media.[2]

The government has introduced legislative reforms, worked with digital platforms, and taken judicial action to combat disinformation. The media, for its part, has adhered to rigorous journalistic standards, avoiding the spread of unverified claims. Meanwhile, civil society groups have led extensive fact-checking and investigative efforts to root out false information.

As the tactics of information manipulation grow more sophisticated, nevertheless, Taiwan's defenses must evolve. Enhancing the technological capabilities of civil society will be essential. AI tools, for instance, can monitor unusual patterns on social media and analyze content with unprecedented speed. This report examines how Taiwan's government, civil society, and digital platforms have responded to the threat of information manipulation and outlines recommendations to strengthen their efforts further.

Figure 1 : Overview of the Actors Combating Disinformation and Information Manipulation in Taiwan

II. The Government

In the battle against rampant disinformation, the government must strike a careful balance: it should address the issue decisively without encroaching unreasonably on civil liberties. Like many countries, Taiwan encountered significant challenges with disinformation during its 2018 election cycle.[3] Since then, the government has adopted a more serious approach to tackling information manipulation.[4] In its 2018 Special Report for Preventing Disinformation (防制假訊息危害專案報告), the Executive Yuan outlined a strategy to combat disinformation. The plan included creating a legal definition for "rumors (謠言)," clarifying existing regulations, increasing penalties for spreading certain types of disinformation, promoting media literacy, and fostering collaboration with the private sector.[5] However, not all of these initiatives have been realized. For instance, the proposed Digital Intermediary Service Act (數位中介服務法) faced substantial public backlash and ultimately failed to pass into law, reflecting the challenges of balancing regulatory measures with public acceptance.

This report outlines the measures against disinformation taken by the Executive Yuan and its subsidiaries—the National Communications Committee, the Ministry of Education, the Ministry of Digital Affairs, and the Ministry of Justice Investigation Bureau.

Figure 2 : Overview of the Government Agencies

2. Executive Yuan

The Taiwanese government's framework for responding to disinformation campaigns originated with the Special Report for Preventing Disinformation, by the Executive Yuan Council on December 13, 2018. The report aimed to define disinformation and outlined a strategy centered on four core principles: identification, exposition, suppression, and penalization.[6]

Building on this approach, the Executive Yuan released a follow-up policy report in late 2019 titled Policy Overview on Countering Disinformation (2019防制假訊息政策簡介). The report defined disinformation as "information or events created, disseminated, or exploited by an individual with clear intent—whether for political, economic, national security, or other specific purposes—and with deliberate intent to spread it publicly (malice), where all or part of the information can be proven false and causes harm or actual adverse effects to individual, social, or national interests.[7]"

According to the report, the primary sources of disinformation threats are "malicious [domestic] actors" and "hostile foreign forces" leveraging emerging internet technologies and social media to create and disseminate false information.[8] This highlights the government's recognition of the critical role new technologies play in enabling information manipulation.

The 2019 report's objectives—identification, exposition, suppression, and penalization—are centered on tackling disinformation itself rather than addressing the technologies that facilitate its rapid dissemination. Identification aims to enhance citizens' ability to detect false information, while exposition focuses on providing swift and effective clarifications. Suppression emphasizes collaboration between public and private sectors to curtail the spread of disinformation, and penalization seeks to hold those who distribute false content legally accountable, thereby deterring malicious actors from engaging in information manipulation.[9]

While emerging technologies, such as generative AI and deepfake imaging, are recognized by the Executive Yuan as potential tools for spreading false information, they are treated as channels to manage disinformation rather than primary targets. For example, the government penalizes those using deepfakes to spread false information about elections, rather than the platforms that host the deepfakes. There are also legislative efforts to place greater responsibility on social media platforms to prevent information manipulation.

Acknowledging the fundamental incompatibility of governmental surveillance and freedom of speech, the Taiwanese government emphasizes a balanced approach that protects both security and human rights.[10] The Ministry of Justice has worked to clearly define punishable actions, refining relevant laws through multiple amendments to clarify definitions, rationalize accountability, and ensure that courts decide whether specific cases of alleged disinformation warrant punishment.[11]

Legislative Ammendments

Since 2019, the Legislative Yuan has passed various criminal and administrative measures, structuring the criteria for punishment around the principles of "malice, falsity, and harm."

These legal revisions stipulate that only actions meeting all three conditions—intentional malice, dissemination of specific types of false or misleading information, and harm to the public or individuals—fall within the scope of penalties.

In 2023, the Legislative Yuan significantly revised the Act on Property-Declaration by Public Servants (公職人員財產申報法) and the Presidential and Vice Presidential Election and Recall Act (總統副總統選舉罷免法).[12] Under Article 104 of the former and Article 90 of the latter, individuals who spread false information with the intent to influence election or recall outcomes, and in a manner that causes harm, are subject to penalties. The revised laws impose stricter penalties for cases involving the usage of AI deepfake technology.

Beyond election-related regulations on information manipulation, recent legislative amendments in Taiwan aim to eliminate loopholes in criminal or administrative laws across specific sectors. For instance, individuals who intentionally spread false information about agricultural products, food safety, infectious diseases, or disasters in a way that could harm others or the public may now face criminal or administrative penalties. Article 63, Paragraph 1, Item 5 of the Social Order Maintenance Act (社會秩序維護法) authorizes detention or fines for "spreading rumors that could disrupt public order."[13] This long-standing provision serves as a general fallback for penalizing disinformation. In other words, when other laws cannot be invoked to convict someone responsible for spreading disinformation, authorities can still carry out justice using the Social Order Maintenance Act.

The use of mass media or internet technologies to spread false information can lead to broader and more severe social harm. In response, the Legislative Yuan has amended relevant laws in recent years—including the Criminal Code of the Republic of China (中華民國刑法), the Criminal Code of the Armed Forces (陸海空軍刑法), and the Communicable Disease Control Act (傳染病防制法)—to impose stricter penalties on those who use these emerging technologies to disseminate disinformation.

Regulations of Media & Digital Platforms

Taiwan has been working to advance legislation that compels online platforms to assume greater responsibility and implement more robust mechanisms to curb the spread of false information. A clear example is the "Deepfake Clause,"[14] enacted on May 26, 2023. This regulation permits candidates to request law enforcement agencies to verify suspected deepfake audio or video involving them. If the content is confirmed as a deepfake, platforms are required to remove it. Regulatory authorities could impose fines on those that fail to comply.

Other capstone legislative amendments include those on the Public Officials Election and Recall Act (公職人員選舉罷免法) and the Presidential and Vice Presidential Election and Recall Act, which passed the Legislative Yuan on May 26, 2023. The amendments focused on two main objectives. The first is a "Real Name Authentication for Election Advertisements (選舉廣告實名制)," requiring all media—newspapers, magazines, broadcast television, and online platforms—to disclose the sponsor, funder, and other relevant information in any election or recall advertisements they publish or broadcast.

The second objective, "Preventing Foreign Interference in Elections (防杜境外假訊息)," mandates newspapers, magazines, broadcast media, and online service providers to verify whether the sponsors of election or recall advertisements are foreign entities. This includes individuals, corporations, groups, or institutions originating from foreign countries.[15]

If a sponsor is identified as a foreign influence, media and service providers are legally prohibited from displaying these advertisements. While these requirements are not directly targeted at disinformation campaigns, they help trace funding sources and identify malicious actors, preventing foreign entities from improperly influencing or distorting public opinion through financial intervention.

Despite these regulations, Taiwan has encountered challenges in advancing additional legislation to hold platforms accountable. In 2019, the Executive Yuan proposed amendments to the Public Officials Election and Recall Act, which included an "emergency restriction order (緊急限制刊播令)" modelled after France's *LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*.[16]

This measure would allow candidates or recall targets to petition the court to, within three days, issue a ruling that restricts the publication of campaign or recall ads containing false information, requiring platforms to remove, suspend, or address the content in some other way. However, the Judicial Yuan publicly opposed the proposal on the basis that courts are not ideally suited as primary fact-checkers and that early judicial intervention could interfere with democratic processes.[17] With the Judicial Yuan's objections, this legislative proposal ultimately failed to pass.

An additional attempt to regulate online information was the Digital Intermediary Service Act, proposed by the National Communications Commission in June 2022.[18] Designed to combat the spread of disinformation, the draft legislation granted regulatory authorities the power to require intermediary service providers (platforms) to temporarily flag content as potentially false if it involved rumors or disinformation, even prior to a court ruling.

For cases where unlawful content posed an immediate and significant threat to public interest, the draft allowed authorities to seek an "emergency information restriction order," requiring the court to issue a decision within 48 hours. However, the proposal faced significant public backlash and ultimately failed to progress.[19]

This legislative approach to limiting disinformation faced widespread public criticism, however. The main concern was that the criteria for requesting an information restriction order—defined as "violating mandatory or prohibitory legal provisions"—were overly broad and unclear.

Moreover, the draft allowed regulatory authorities to compel intermediary service providers to label content as false even before a court ruling,[20] raising concerns that they would grant government agencies too much authority to censor content, potentially prompting digital platforms to preemptively

screen content for any signs of illegality or disinformation to avoid penalties—thereby overly restricting users' freedom of expression.[21]

At the time the legislation was proposed, a poll conducted by RW News (菱傳媒) revealed that nearly 60% of respondents opposed the disinformation control measures in the draft.22 In response to strong public opposition, President Tsai Ing-wen (蔡英文) and Premier Su Tseng-chang (蘇貞昌) both called for a suspension of the draft.[23]

In addition to governmental regulatory mechanisms, Taiwan's government has vigorously called for major online platforms to self-regulate to reduce the spread of disinformation, focusing on improving the timeliness, accuracy, and effectiveness of clarifying false information. The government enthusiastically collaborates with many private-sector institutions to efficiently verify and clarify disinformation, while also using legislation and platform self-regulation to strengthen the roles of media outlets and third-party fact-checking organizations in the debunking process.

Partnerships with Digital Platforms

Platforms with the resources and ability to address disinformation in real time are essential partners in the government's efforts to curb disinformation. Thus, the Executive Yuan also focuses on strengthening partnerships with digital platforms to curb the spread of disinformation. In the era of social media and generative AI, most disinformation is produced and circulated online. Social media, especially, has become a hotspot for viral disinformation due to concerted bot activities and algorithmic exploitations. By enhancing cooperation with digital platforms, the government aims to encourage these platforms and service providers to take on greater responsibility in suppressing the spread of false information.

Since 2019, the Taiwanese government has had an "immediate clarification mechanism (即時澄清機制)" that involves multiple ministries under the Executive Yuan.[24] Under this initiative, government departments actively monitor information across online platforms, broadcast media, and print sources to quickly identify and address disinformation. A press release must be issued within four hours and posted in a dedicated real-time clarification section on official websites. Moreover, executive agencies have developed the Digital Era Government Policy and Crisis Communication Reference Manual (數位時代政府政策溝通與危機溝通 作業參考手冊), offering a standardized process to guide administrative departments in effectively responding to and debunking disinformation.[25]

Government agencies have strengthened public-private partnerships to improve disinformation control. In collaboration with LINE, the most widely used social media in Taiwan, the Executive Yuan launched the "Digital Accountability Project (LINE數位當責計畫)," featuring tools like the "LINE Fact-Checking (LINE 訊息查證)" official account and the LINE TODAY "Rumor-Busting Zone (謠言破解專區)" to further clarification efforts.[26]

In 2019, the Taipei Computer Association and Taiwan's major online platforms—Facebook, Google, LINE, Yahoo Taiwan, and PTT—also introduced Industry Self-Regulation Guidelines

for Combating Disinformation (不實訊息防制業者自律實踐準則).[27] These guidelines established procedures for identifying and controlling disinformation, promoted advertisement transparency, and supported collaboration with government and third-party groups to develop tools for labelling, filtering, and controlling disinformation. They also urged the platforms to promote digital literacy and media education efforts, with regular reviews and public reporting on self-regulation outcomes.[28]

Educational Efforts

Former minister Lo Ping-cheng (羅秉成) has emphasized that relying solely on legislation to "eliminate" disinformation is unrealistic; instead, it is essential to have a combined approach of disinformation suppression and media literacy education. He advocates using AI to organize government resources for timely responses to disinformation and initiating media literacy programs, customized for different demographic and age groups, designed to strengthen citizens' ability to recognize false information.[29]

Taiwan's government has pushed for media literacy education tailored for each age group, helping all citizens build skills to assess information accuracy.[30] Rather than advancing new legislations, the government primarily uses administrative measures to achieve this goal. For example, the Civil Service Development Institute under the Executive Yuan offers courses on disinformation counter-strategies, online discourse analysis, and digital media use to improve civil servants' understanding and response to disinformation.[31]

3. National Communications Commission

The National Communications Commission (NCC) aims to improve media quality by mandating stronger internal controls in broadcast media, enforcing fact-checking and fairness principles, and offering professional training for broadcasters. Programs such as the "Implementing Fact-Checking and Fairness Principles (事實查核與公平原則)" workshop aim to enhance the skills of media professionals in these areas.

The public can report disinformation broadcasted on television directly to the NCC. If the NCC has full legal authority to tackle an incident, it would review the case to determine whether inadequate fact-checking compromised public interest or violated standards of public order and decency. The NCC would then hold a "Broadcast Advertising Advisory Meeting (廣播電視節目廣告諮詢會議)" to gather expert recommendations, after which the NCC Commission would decide whether to take legal action, issue a notice for improvement, or close the case without further action.[32]

If a public complaint falls outside the NCC's jurisdiction—for example, when the disinformation is being spread online—the NCC, with the complainant's consent, would forward the case to the relevant law-enforcement agency as instructed in the Basic Guidelines for Internet Content Management and Division of Responsibilities (網際網路內容管理基本規範及分工原則), implemented by the Executive Yuan's National Information and Communication Security Taskforce (行政院國家資通安全會報). The responsible agency then

investigates and issues a clarification through the Executive Yuan's real-time news system.[33]

The NCC provides professional training for broadcast media personnel. Its "Broadcast Media Professional Literacy and Citizen Empowerment Program (廣電媒體專業素養培訓及公民培力計畫)" offered training sessions, delivered by expert instructors, focused on strengthening self-regulation and implementing fact-checking practices.[34] Training materials were later made publicly accessible.[35]

To promote public media literacy, the NCC collaborates with community groups and schools, supporting initiatives such as the Broadcast Media Citizen Empowerment Program and online media literacy courses to enhance public understanding of media production. In 2023, the NCC partnered with the Taiwan Public Television Service (公共電視), National Taiwan Normal University (國立臺灣師範大學), Chaoyang University of Technology (朝陽科技大學), The Association of Taiwan Journalists (台灣新聞記者協會), and other non-profit institutions to host 20 media literacy events. One such event, organized by Yangmingshan Cable TV (陽明山有線電視), featured a "Recognizing Media Content and Preventing Disinformation (辨識媒體內容 防制假訊息)" course, where the FakeNewsCleaner team shared case studies and taught participants how to verify and identify disinformation.[36]

In response to its expanded role in internet communication policy, the NCC established the Office of Internet Communications (網際網路傳播辦公室) in 2023 to promote internet literacy and citizen empowerment initiatives. It released the draft of the Internet Governance White Paper (網際網路傳播政策白皮書) in July 2024 to collect public opinions.[37] The White Paper emphasizes self-regulation as the guiding principle for internet platforms, while also addressing concerns about the unintended impacts of AI algorithms, such as the amplification of extreme speech and the targeting of specific groups.

4. Ministry of Education

In May 2019, the Ministry of Education established the Media Literacy Education Promotion Committee (媒體素養教育推動會) to regularly review and plan media literacy policies. Shortly after, it introduced the 2019 Media Literacy Education Action Plan (108年媒體素養教育行動方案), outlining a framework with three focus areas, six strategies, and 23 action items to guide Taiwan's media literacy efforts. Building on this foundation, the White Paper on Media Literacy Education in the Digital Age (數位時代媒體素養教育白皮書), released in 2023, seeks to cultivate "informed, responsible, and altruistic" digital citizens who use media and technology constructively, with an emphasis on developing critical thinking skills.[38]

The Ministry of Education has integrated "technology, information, and media literacy" into elementary and middle school curricula, focusing on teacher training, curriculum resources, and lesson planning, establishing new programs while continuing to build on existing ones. It has also established media literacy institutes, acting as regional hubs to assist local educators in developing curriculum modules and obtaining educational resources.

The Ministry's efforts are not limited to helping the youth. It also funds media literacy lectures and courses at community colleges,[39] provides media literacy reources to public libraries, and incorporates media literacy topics into the National Education Radio (國立教育廣播電台) programs. In addition, the ministry partners with private organizations to promote lifelong media literacy education. In 2019, for example, the Learning to the Nth Power program (學習N次方) featured collaborations with 104 nongovernmental organizations to enhance the public's abilities to identify disinformation.[40]

5. Ministry of Digital Affairs

The Ministry of Digital Affairs (MODA) is tasked with developing Taiwan's digital policies (IT, cybersecurity, telecommunications, etc.). MODA aims to ensure national information security, promote digital transformation, and strengthen public digital resilience.[41]

MODA provides technical support, such as platforms for real-time disinformation clarification, for other agencies' anti-fraud campaigns. During elections, it would also be responsible for detecting and taking down websites that promote political fraud, such as ones using deepfakes to spread made-up campaign promises.[42]

MODA oversees the National Institute of Cyber Security, restructured in 2023 to focus on strengthening cybersecurity through research, technology development, and application. Partnering with third-party organizations like the Taiwan FactCheck Center, the institute employs AI to analyze disputed information, offering tracing and advisory services to combat disinformation.[43] The Institute also shares its analytical methods with the Ministry of Justice Investigation Bureau and the Criminal Investigation Bureau.

In February 2024, MODA's Administration for Digital Industries launched the 2024 Smart Anti-Fraud and Digital Trust Program (113年度智慧防詐與數位信任應用發展計畫), aiming to build a digital trust ecosystem through public-private partnerships focused on industry engagement, public awareness, intelligence sharing, and source-blocking.[44] As part of this program, MODA introduced the Digital Trust Field Service Field Verification Plan (數位信任場域服務實地驗證計畫), offering grants to developers of anti-fraud softwares, which popularized FIDO secure identity verification, steganography, electronic signatures, and blockchain technologies in Taiwan, strengthening digital trust and enhancing business security in the private sector.[45]

6. Ministry of Justice Investigation Bureau

On August 8, 2019, the Investigation Bureau established the Disinformation Prevention Center (假訊息防制中心) to trace and investigate disinformation sources.[46] In April 2020, this center was expanded and rebranded as the Cybersecurity Task Force (資安工作站), increasing its ability to combat cybercrime and respond to emergent threats.[47] At its opening ceremony, then-President Tsai Ing-wen gave a speech emphasizing the critical connection between cybersecurity and national security in addressing information warfare.[48] After the 2024 election, the Bureau further expanded the Cybersecurity Task Force, renaming it as the Cognitive Warfare Research Center (認知戰研究中心). At the opening ceremony, Minister

of Justice Tsai Ching-hsiang (蔡清祥) highlighted the growing scope and intensity of cognitive warfare conducted by foreign adversaries, who threaten Taiwan's national security by subtly eroding public resilience against geopolitical threats.

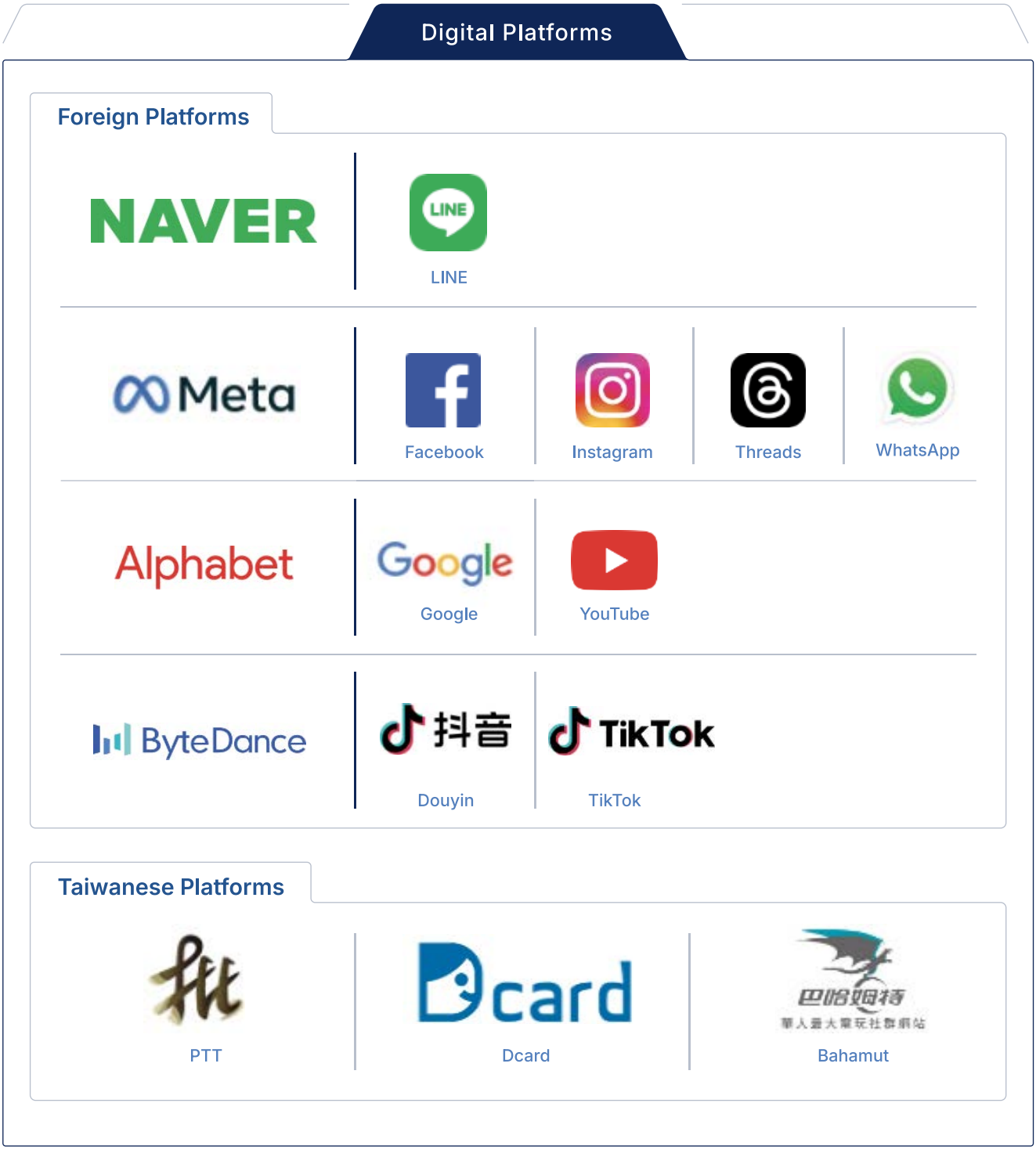
The Center, comprising three divisions—responsible for data compilation and research, analysis of cognitive warfare targeting Taiwan, and swift responses to combat fake news respectively—synergized the existing efforts of multiple agencies, combining theories, experiences, and expertise, to increase the government's capability to combat foreign manipulation efforts.[49] The Center has investigated many instances of information manipulation, such as the "Under the Foot of Yushan (玉山腳下)" videos Chinese state media used to influence Taiwan's 2020 elections, and the hundreds of fake news reports on the COVID-19 pandemic.[50]

III. Digital Platforms & Social Media

According to the 2022 Taiwan Communication Survey Project (台灣傳播調查資料庫)[51] and the 2023 Social Media Usage Behavior Survey (2023年社群媒體使用行為調查),[52] the four most widely used social media and messaging platforms in Taiwan are LINE, Facebook, Instagram, and Messenger. These platforms are used by more than half of Taiwan's population, underscoring the significant influence of LINE and Meta (the parent company of Facebook, Instagram, and Messenger) on content management and their impact on Taiwanese society. Google and its subsidiary YouTube are also key players with substantial influence due to their high website traffic.

The following sections will analyze the content manipulation policies of the most widely used digital platforms and social media in Taiwan: LINE, Meta (including Facebook, Instagram, and WhatsApp), and Google (including YouTube). We will also address the policies of Douyin (the Chinese version of TikTok), TikTok, and local platforms such as PTT, Dcard, and Bahamut due to their high traffic and name recognition.

Figure 3 : Digital Platforms by Parent Company and Country



7. LINE

LINE, one of the most widely used digital platforms in Taiwan, provides a range of services from contactless payment to emoji marketplace. This section will focus on the information manipulation challenges arising from its messaging service.

Given its extensive user base, LINE has often been criticized for the high amount of user-generated scams and disinformation,[53] making it a focal point for governance and regulation. To address this problem, LINE launched its Digital Accountability Initiative,[54] which highlights its collaboration with Taiwanese civil and governmental organizations to conduct fact-checking and debunk disinformation. During the 2024 presidential and legislative elections, the Central Election Commission utilized LINE to remind citizens not to share election-related disinformation and encouraged users to take advantage of LINE's fact-checking tools to verify reports from dubious sources.[55]

On top of establishing its own fact-checking platform and fostering cross-agency cooperation, LINE has adopted technical solutions to combat the ever-evolving nature of disinformation on the platform. These strategies, including training language models to recognize and analyze textual content, demonstrate LINE's commitment to address information manipulation challenges using technology.

8. Meta

Meta, the parent company of Facebook, Instagram, Messenger, Threads, and WhatsApp, has a significant presence in Taiwan, with Facebook and Instagram being especially popular. Following controversies like the Cambridge Analytica scandal, which highlighted its role in influencing the U.S. elections, Meta has become a focal point in global efforts to combat disinformation.[56]

Disinformation Policies and Enforcement

Meta outlines its disinformation policies at its Transparency Center, detailing policies and methods for managing misleading content. It explicitly targets content that interferes with political processes or contains highly deceptive information. Its definition of inauthentic behavior includes:

1. **Subtle Edits or Synthesis:** Videos edited or synthesized in ways imperceptible to the average viewer, beyond mere definition adjustments. These edits could let viewers incorrectly believe that the individuals depicted in the video had made certain statements.

2. **AI-Generated Content:** Material created using artificial intelligence or machine learning, such as deepfaking, blending, altering, or overlapping content to produce made-believe material.[57]

After verifying the authenticity of the content, Meta classifies it into six levels based on its factuality:

1. **True:** Verified factual information.
2. **False:** Determined to be entirely incorrect.
3. **Altered:** Edited in misleading ways.
4. **Partially False:** Inaccuracies found among mostly true statements.
5. **Satire:** Identified as humor or parody, not

meant to be misleading.
6. **Opinion:** Recognized as a subjective viewpoints, not facts.[58]

For content classified as false, altered, or partially false, Meta employs algorithmic measures to reduce its visibility and diffusibility. Monetization of such content through advertisements is also prohibited.[59]

Platform-Specific Approaches

Meta's disinformation policies extend across its many platforms, but the degree of policy transparency varies. While Facebook provides comprehensive guidelines through the Transparency Center, platforms like Instagram and Threads offer less detailed explanations of their disinformation policies.[60] WhatsApp employs a different approach, using a forwarding limit to curb viral disinformation rather than removing or demoting content.[61]

Collaborations with Fact-Checking Organizations

Meta collaborates with International Fact-Checking Network (IFCN)-certified organizations to verify content globally. In Taiwan, it partners with Taiwan FactCheck Center (TFC) and MyGoPen, the only two IFCN-certified organizations in the country. However, Meta's Transparency Center does not explicitly mention these local collaborations. WhatsApp, despite being part of the Meta ecosystem, does not appear to collaborate with any Taiwanese fact-checking organizations.[62]

9. Google

As a leading player in search engines and video platforms, Google plays a crucial role in addressing online disinformation, especially during election periods. Google Taiwan has implemented several measures to counteract misleading information and to promote digital literacy.

Key Initiatives and Partnerships

Google has introduced features such as image search tools that help users trace the origin and history of an image, enabling them to identify potentially manipulated or false content. The company also supports Taiwanese fact-checking organizations, including Taiwan FactCheck Center (TFC) and MyGoPen, financially.[63] Through collaborations with the National Association for the Promotion of Community Universities (社團法人社區大學全國促進會), FakeNewsCleaner, and MyGoPen, Google offers community-based courses and volunteer training programs to enhance public awareness and improve the public's ability to identify disinformation.[64]

The 4R Principles

Google's strategy for managing content is guided by its 4R framework—Remove, Raise, Reduce, and Reward—which balances the reduction of disinformation with the protection of free speech:

1. **Remove:** Remove harmful content that violates its policies.
2. **Raise:** Raise the visibility of authoritative sources in search results and recommendations.

3. **Reduce:** Reduce the visibility of content that may mislead users.
4. **Reward:** Reward high-quality content creators by enhancing their visibility and monetization opportunities.[65]

Google regularly evaluates content management policies based on user feedback, refining its algorithms to ensure that reliable information ranks higher in search results. For content that doesn't meet their criteria for removal, Google reduces their visibility in search rankings to minimize their impact.[66]

Cybersecurity Efforts and Concerted Threats

Google has a dedicated cybersecurity team to monitor and respond to hacking attempts and online attacks, particularly those involving organized crime or state-sponsored activities. This proactive approach addresses not only disinformation but also broader cybersecurity challenges, setting Google apart from other major tech companies.

10. Douyin and TikTok

Douyin (抖音), the original Chinese version of TikTok, primarily serves the Mainland Chinese market. Since it is a Chinese platform, the accounts registered and content hosted on Douyin must comply with Chinese regulations.[67] Such regulations have, to an extent, prevented the spread of manipulated information. There are no known collaborations between Douyin and any Taiwanese fact-checking platforms.

In contrast, TikTok has more comprehensive policies to combat information manipulation. These policies are detailed in its community guidelines with clearly defined terms and policies for addressing disinformation.[68] While the platform does not specify the tools used to detect violations, TikTok provides "Community Guidelines Enforcement Reports", which explain enforcement methods, outline results, and classifies removed content by reason for removal.[69] TikTok also collaborates with international fact-checking organizations, though no Taiwanese fact-checking groups are listed as its partners.[70]

However, under specific circumstances, such as during election periods, TikTok would adopt localized solutions to enhance media literacy and information accuracy. For instance, it partnered with MyGoPen to launch the "2024 Election Guide (2024 年選舉指南)"[71] and collaborated with the Taiwan FactCheck Center and the Child Welfare League Foundation (兒福聯盟) to produce educational videos promoting media literacy.[72]

11. Local Platforms: PTT, Dcard & Bahamut

Compared to the aforementioned international platforms, Taiwan's local platforms have shown limited engagement in addressing disinformation. Prominent Taiwanese digital platforms, including PTT, Dcard, and Bahamut, have not publicized specific policies on manipulative content. Their actions against disinformation have primarily been limited to compliance with requests from law enforcement agencies.[73]

Among them, Dcard is the only platform that has collaborated with a nongovernmental organization (MyGoPen) to promote media

literacy.[74] These platforms largely rely on their moderators' discretion for content removal. PTT, in particular, has publicly opposed the proposed Digital Intermediary Service Act, citing its insufficient resources to manage violent, fraudulent, and manipulative content.[75]

12. Analysis and Discussion

Multinational platforms are more likely to implement policies to address information manipulation. They often publicize their countermeasures against disinformation, which frequently involve collaboration with law enforcement agencies. In contrast, Chinese and local platforms, such as Douyin (distinct from TikTok), PTT, Dcard, and Bahamut, disclose little about their approaches to combating information manipulation. Beyond general terms of agreement, these platforms provide little information on specific policies, methods, or evaluation mechanisms.

As a result, multinational platforms appear more inclined to establish self-regulatory mechanisms and form partnerships with fact-checking organizations or non-governmental entities. For policymakers, supporting cooperative domestic platforms that lack the resources to combat information manipulation effectively and regulating those unwilling to self-govern will be the critical challenges moving forward.

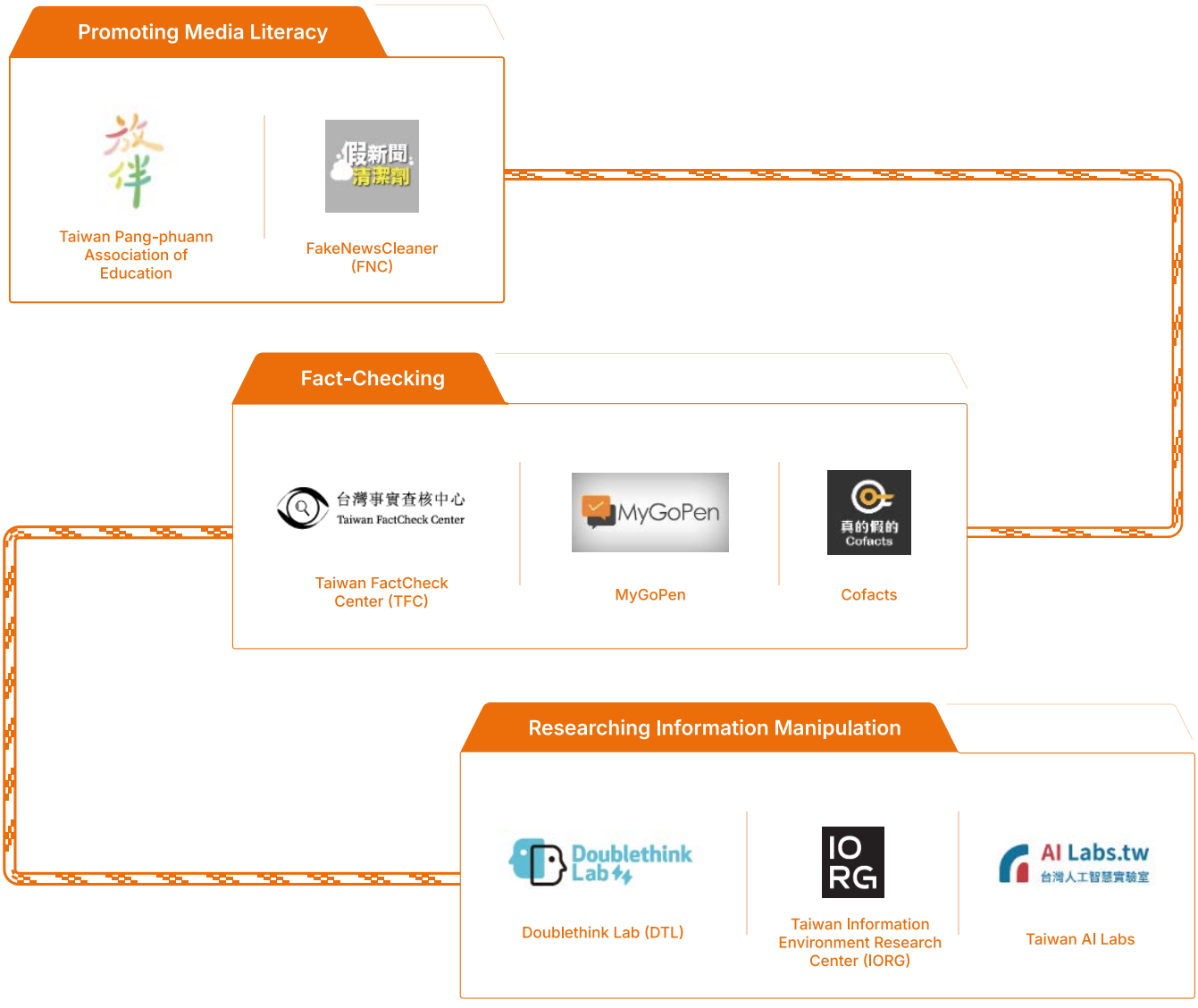
Figure 4 : Overview of the Digital Platforms

Digital Platforms	Anti-Disinformation Policy	Evaluations of Policy Enforcement	Collaborative Partners
LINE	Fact-checking services[76]	Yes[77]	MyGoPen, Cofacts, TFC
Facebook	Transparency Center[78]	Yes[79]	IFCN-certified organizations (TFC, MyGoPen)
WhatsApp	List of methods to prevent the spread of disinformation[80]	Yes[81]	Not in Taiwan[82]
Google	Transparency Center[83]	Yes[84]	IFCN-certified organizations (TFC, MyGoPen)[85]
YouTube	Yes[86]	Yes, publicizes the number of accounts removed for policy violations[87]	Not in Taiwan, only offers the Priority Flagger Program[88]
抖音	User agreement[89]	Only the punishments[90]	No
TikTok	Yes[91]	Yes[92]	MyGoPen[93]
Instagram	User agreement[94]	No	No
Dcard	User agreement[95]	Press release declaring its abidance to the law	MyGoPen
巴哈姆特	Site policies and policy protections[96]	No	No

IV. Nongovernmental Organizations

Taiwan's civil society has taken proactive steps to combat disinformation and information manipulation, including fact-checking, investigating concerted activities, and promoting media literacy and critical thinking skills. This report organizes and analyzes the actions, strategies, and perspectives of various nongovernmental organizations addressing these challenges. Unless otherwise marked with an endnote, the information presented in Section IV. is based on interviews with representatives of these NGOs and does not represent the views of DSET or the authors of this report.

Figure 5 : Primary Functions of the Nongovernmental Organizations



13. Media Literacy Advocacy Organizations

Enhancing media literacy and critical thinking skills is vital for fostering resilience against information manipulation. While fact-checking and research organizations produce reports on disinformation, the complexity of the topic often makes it inaccessible to the general public. Media literacy organizations play a crucial role in addressing this gap by equipping citizens with the tools to comprehend and critically evaluate the intricate issues covered by the media.

Two prominent media literacy organizations in Taiwan are the Taiwan Pang-phuann Association of Education and FakeNewsCleaner. The Taiwan Pang-phuann Association of Education focuses on integrating media literacy and critical thinking into school curricula, helping students understand and evaluate information effectively. FakeNewsCleaner, which began in Taichung, engages directly with the public on the streets to raise awareness about disinformation and media literacy. They have since expanded their work to community colleges, offering courses that build digital skills and encourage critical awareness of information manipulation.

The sections below addresses the following key questions regarding the organizations:

1. Who are their target audiences for media literacy outreach?
2. How are outreach strategies tailored to resonate with different groups?
3. What have these organizations observed on the recent use of GenAI in disinformation?

14. Taiwan Pang-phuann Association of Education

The Taiwan Pang-phuann Association of Education (台灣放伴教育協會, Pang-phuann) was founded in 2020 by a group of teachers and social workers who wished to integrate social issues, including media and information literacy, into school curricula.[97] Pang-phuann brings IORG's research findings into communities, providing outreach into local communities. Pang-phuann and IORG have also published A Guide to Information Literacy (資訊判讀力), a practical guide on recognizing and understanding information manipulation.[98]

The same year, Pang-phuann hosted its first issue-based workshop, which received enthusiastic feedback from the attending teachers. Positive word of mouth spread quickly, leading to widely popular workshops in subsequent sessions. Pang-phuann hopes to drive change by empowering teachers, who in turn can inspire students, fostering meaningful, long-term transformations within the school system.

Assisting Teachers to Provide Media Literacy Education

Pang-phuann had initially aimed to bring IORG's research into schools to improve the media literacy of students when they noticed a bigger problem: many NGOs struggled to introduce discussions of social issues to schools due to their inefficient methods. The 2019 curriculum reform, which increased the number of electives, mandated the teachers to develop a more diverse curriculum, thereby increasing their workload, without providing

ample assistance to the teachers. Teachers interested in developing media literacy courses often require administrative support, which adds extra workload not all are willing to take on. Some struggle to deliver such lessons, while others lack the necessary knowledge or resources.

Pang-phuann explains that although schools are required to teach media literacy, the responsibility for this course is often assigned to IT teachers, who may not necessarily possess expertise in media literacy. Although the National Academy for Educational Research (國家教育研究院) offers media literacy workshops to these teachers, the instructors at these workshops are often professors of journalism whose expertise is training journalists, not teachers. Likewise, the online media literacy resource platform, created by the Ministry of Education, offered little empirical use for teaching.

To address these deficiencies, Pang-phuann has implemented a multi-phase plan to help teachers plan their media literacy courses. The process begins with workshops and lectures that introduce foundational concepts and methodologies for teaching. These sessions aim to build teachers' understanding, increase their self-confidence, and offer them directions for lesson planning.

Once teachers resolve the administrative challenges and secure funding, they can invite Pang-phuann to help them plan their lessons. This type of collaboration typically involves three or more teachers and spans three to four planning sessions per semester, to have the course be offered in the following semester. Pang-phuann conducts over 100 workshops and lectures annually, providing assistance to more than 3,500 teachers nation-wide.

In addition, Pang-phuann assesses whether these courses genuinely impact students. For example, at the end of 2022, they conducted a "Student-Teacher Dialogue Workshop (師生對話工作坊)", where middle school teachers and students shared their opinions on the media literacy courses. While many teachers were initially skeptical of this approach, positive feedback from students shifted their perspectives, increasing their acceptance of the program.[99]

Despite these successes, Pang-phuann faces challenges when working within school environments. Political topics—information manipulation, foreign influence, and cognitive warfare—are off-limits in schools; instead, Pang-phuann focuses on non-partisan subjects like the risks of short-form videos.

Information Manipulation Undermines Democracy and Trust

Pang-phuann highlights a critical challenge in information manipulation: even factual statements or fragments can be woven into misleading narratives, making it increasingly difficult to discern truth from falsehood. This problem is compounded by the rise of GenAI, which adds layers of complexity to evaluating information credibility.

Drawing on a 2016 psychological study by Foa and Mounk, Pang-phuann notes that individuals who perceive information manipulation as widespread and lose trust in the media are more susceptible to its influence after repeated exposure.[100] This erosion of trust

can lead to disillusionment with democracy and a growing preference for authoritarian solutions. Pang-phuann warns that the real danger of information manipulation lies in its ability to make people doubt the democratic society's ability to effectively address the issue, thereby legitimizing authoritarianism as an alternative.

By helping individuals recognize problematic information and understand the need for verification, people become better equipped to use fact-checking tools effectively. For this reason, Pang-phuann's courses consistently prioritize fostering critical thinking and information literacy.

Furthermore, Pang-phuann tailors its approach to different audiences—teachers, communities, students, and seniors—by addressing topics relevant to their specific experiences and challenges. For instance, they use Taiwanese dialect and real-life examples of scams to engage seniors in discussions about digital literacy. They often start discussions with students by examining scams related to growth supplements promoted on platforms like Instagram or YouTube. This approach helps participants not only resonate with the content but also apply the knowledge they gain to their daily lives effectively.

Rebuilding the Foundations of Social Dialogue

Rebuilding social dialogue also means addressing the spread of disinformation in private chat groups, where much of it circulates unnoticed. While individuals can play a role in supporting one another, the responsibility also extends to key information producers, such as media outlets, influencers, opinion leaders, politicians, and commentators. These actors must acknowledge their responsibility in fostering a healthier information ecosystem.

In particular, Pang-phuann highlights the troubling tendency of some political figures to use manipulative or misleading information to simplify communication with voters. While this approach may seem effective in the short term, it undermines public discourse, stifles dialogue between people with opposing perspectives, and risks eroding public confidence in democratic institutions. Just as problematic is the rise of short-form videos and social media algorithms, which have led to increasingly fragmented and oversimplified information, often reducing complex issues to easily digestible slogans. This trend amplifies the impact of information manipulation and, combined with GenAI, further complicates democratic dialogue. While addressing these issues is undoubtedly challenging, it is a shared responsibility that requires collective efforts to ensure a more resilient democratic society.

15. FakeNewsCleaner (FNC)

FakeNewsCleaner (假新聞清潔劑, FNC) was founded in December 2018 by a group of committed citizens, including young professionals, engineers, and social workers. Concerned by the spread of disinformation during the elections and referendums in 2018, FNC began organizing ground campaigns in busy areas like trailheads, markets, and parks in their free time.[101] Their goal was to promote media literacy and help the public learn how to recognize and counter false information, empowering individuals to protect themselves and their families.

From Street Campaigns to Workshops and Courses

FNC began its work by organizing street campaigns to combat disinformation, using simple yet engaging methods to connect with the public. Volunteers showcased examples of disinformation messages commonly received on smartphones, using interactive displays to spark conversations. The volunteers self-funded these early efforts, spending their own money on props and giveaways to encourage participation. These activities helped people learn how to evaluate information critically and identify misleading content, empowering them to protect themselves and their families against disinformation.

As interests grew, community leaders began inviting FNC to host sessions in their neighborhoods. This inspired the organization to develop a series of workshops held at community hubs, such as community colleges, community centers, churches, and temples, to further promote media literacy. Initially funded by its volunteers, FNC gradually attracted corporate sponsorships and established the "Taiwan Information Literacy Empowerment Association (社團法人台灣資訊素養推進會)" to facilitate public fundraising. Despite these developments, FNC strictly avoids donations from political parties or politically affiliated organizations.

To ensure sustainability, FNC launched a "seed training (種子培訓)" program to train volunteers nationwide.[102] Today, the organization boasts over 180 volunteers working across various regions of Taiwan. Between late 2018 and the end of 2023, FNC held 683 events, reaching over 42,000 families.

FNC frequently collaborates with organizations like MyGoPen and Cofacts. For example, its recent "Disinformation Awards (最佳詐騙獎)" initiative invited the public to vote on the most notable scam of the year. This creative effort not only reviewed the past year's most widespread disinformation but also served as a reminder to prioritize fact-checking. FNC also partners with Google in its Taiwan Media Literacy Program (台灣媒體素養計畫), with Google providing financial support to FNC and NGOs to promote media literacy.[103]

FNC also addressed the needs of seniors, many of whom were new to using smartphones. The team designed practical courses teaching basic skills like using LINE, Facebook, and Google Maps. Media literacy is integrated into these lessons, helping participants learn to verify information while mastering digital tools. By presenting relatable, everyday scenarios, FNC made it easy for attendees to share their knowledge with family members, extending the program's impact.

Improving the Public's Information Literacy

FNC emphasizes that disinformation is bigger than the false message itself—it can lead to economic losses, health risks, and family quarrels. For instance, one widely shared false claim suggested that drinking milk mixed with sweet potato leaves could cure gout, high blood pressure, and even cancer. In reality, sweet potato leaves are high in potassium, which can worsen conditions for individuals with gout or kidney issues. Other examples include short videos of traffic accidents or school bullying. While these videos are not manipulated, sharing these videos achieves little beyond

provoking strong emotions like anger and hatred among their audiences. FNC uses these scenarios to encourage participants to rethink what types of content are appropriate to share and to highlight the dangers of disinformation—particularly in short video formats.

FNC creates teaching materials from fraudulent messages commonly shared in group chats, misleading policy statements, and scams. These examples resonate with participants' everyday experiences, fostering a deeper understanding of the importance of media literacy. FNC continually updates its materials to address the latest trends. Two pressing topics are the rise of short-form videos and the misuse of GenAI. In addition, FNC introduces fake-checking tools, such as those developed by MyGoPen and Cofacts, to help participants verify information effectively.

FNC has also incorporated knowledge of deepfake technology in its sessions, educating participants about face-swapping and other manipulative AI techniques. This knowledge helps individuals deal with scams involving deepfakes. For example, when someone gets blackmailed with a deepfake video, FNC advises them to block the perpetrator, report the incident to the police or the 165 anti-fraud hotline, and, if needed, consult MyGoPen's live support service.

To ensure ongoing support, FNC creates group chats for workshop participants, allowing them to ask questions and seek assistance after the sessions. This follow-up engagement helps participants feel supported and encourages them to continue building their information literacy skills.

The Lack of Government Efforts

FNC has observed a growing public awareness of disinformation and scams, even as these tactics continue to evolve. In 2018, when FNC first began promoting information literacy, most people were unfamiliar with the concept of fake news. Today, many individuals actively use fact-checking tools. However, a significant urban-rural divide persists. Urban communities are more likely to have the resources to host FNC workshops, while rural areas often lack access to such initiatives, leaving residents more vulnerable to disinformation and fraud. FNC emphasizes the pressing need for government investment to address this disparity.

Under the current system, citizens can report fraud by contacting the police or calling the 165 anti-fraud hotline. However, FNC has received feedback from participants that first-line responders often redirect cases between departments, leaving victims feeling frustrated and unsupported. FNC recommends that the government establish a clear and standardized process for handling fraud reports, ensuring agencies work collaboratively to provide effective assistance.

The FNC has consulted the Ministry of Education on the draft of the White Paper on Media Literacy Education in the Digital Age[104] and has trained teachers in workshops. Despite these efforts, teachers face significant challenges in implementing media literacy education. While media literacy has been included in the curriculum, many teachers lack the necessary background knowledge and struggle to create materials that resonate with students. To address this, FNC partnered

with MyGoPen to organize workshops that help teachers translate complex concepts into accessible, student-friendly lessons.

While the government has taken steps by integrating media literacy into the curriculum and launching anti-fraud initiatives, FNC believes more comprehensive measures are essential. Stronger support systems, better inter-agency coordination, and enhanced public communication are necessary to ensure these efforts effectively empower citizens to combat disinformation and fraud.

16. Analysis and Discussion: Media Literacy Advocacy Organizations

Pang-phuann and FNC are two Taiwanese organizations that are working to cultivate the public's media literacy and disinformation discernment skills, preparing society against disinformation and information manipulation. While the two organizations target different demographics and employ distinct approaches, both recognize the importance of teaching the public how to identify disinformation.

Pang-phuann hopes to improve education practices from within by conducting teacher training workshops and helping teachers design curriculums. In contrast, FNC offers workshops, seminars, and organized chat groups to build "mobile platforms", catering to the specific needs of local communities. They ground their work in real-world scenarios and audience-specific experiences, using pervasive scam messages and medical disinformation as examples to make their teachings more palatable. Both organizations focus on hands-on training. They teach participants how to fact-check using MyGoPen and Cofacts and how to evaluate information using IORG's research. They also keep their audiences updated on the dangers of short videos and GenAI could pose in information manipulation.

These organizations are invaluable in a society where trust is being eroded by disinformation. By empowering individuals with the skills to critically evaluate information, they help build a more informed and resilient society.

17. Fact-Checking Organizations

Disinformation has never spread at a faster speed than in today's information-driven society. Thus, fact-checking services, which clarify disinformation quickly, have been more important than ever. The widespread adoption of fact-checking services would enable public access to accurate information and curb the dissemination of false and misleading content.

The fact-checking organizations we've interviewed for this report are Taiwan FactCheck Center (TFC), MyGoPen, and Cofacts. While all three focus on fact-checking, each has unique approaches and characteristics.

Besides fact-checking, these organizations also play active roles in promoting media literacy. Cofacts and MyGoPen offer accessible fact-checking tools and volunteer training. TFC runs workshops to enhance journalists' skills, along with public lectures and a podcast to engage the general public.

The sections below answer the following questions about the fact-checking organizations:

1. How has GenAI been used to promote disinformation during this election cycle? What has the use of GenAI achieved?
2. What are their experiences dealing with digital platform's responses to disinformation?
3. What challenges does the rise of GenAI bring to their fact-checking efforts?
4. Are these organizations using GenAI in their daily operations? If so, how?
5. What challenges, in their opinion, does the rise of GenAI pose to democracy and society?

18. Taiwan FactCheck Center (TFC)

The Taiwan FactCheck Center (台灣事實查核中心, TFC) was founded by the Taiwan Media Watch Foundation and The Association for Quality Journalism in April 2018 as the first fact-checking organization in Taiwan to combat rampant fake news. TFC started publishing fact-checking reports on July 31st, 2018 and received certification from the International Fact-Checking Network (IFCN) later that year.[105] TFC notes that fact-checking is often limited—or even absent—in the current media landscape, which allows disinformation to spread more freely.[106] By focusing on fact-checking, TFC aims to make up for this deficiency of the media ecosystem and help curb the spread of false information.[107]

Methods and Limitations

A major component of TFC's work is collecting rumours. It utilizes an AI tool to go through internet sources, selecting false claims that compromise public interests for its staff to analyze.[108] TFC would share the insights they found with the public via the "Rumor Tracker" on their website.

However, TFC's reports are limited to verifying factuality and cannot address issues such as discriminatory or hateful speech. For these cases, TFC compiles expert opinions on its "Issue Watchroom (議題觀察室)"[109], arguing against discriminatory or hateful speech.

Collaborations with Platforms

TFC collaborates with many platforms to popularize its findings: it promotes its fact-check reports through LINE; Google bumps up TFC's website in its search results, as well as removes any sites which masquerades as TFC from its search results; Facebook, TFC's largest source of funding, puts problematic posts below TFC's fact-checking results, urging users to read the latter before the former.

On Facebook, disinformation is marked with a "black label," reducing its visibility and adding a prompt directing users to TFC's fact-check report. If a Facebook page is flagged this way, its reach is also reduced until the flagged content is corrected or removed.

Facebook, TFC's main funding source, requires TFC to meet a monthly quota of facts checked. Though fact-checks of public statements by political figures do not count toward its monthly quota, since Facebook wishes to maintain political neutrality. During election periods, however, political disinformation

tends to rise, posing risks to fair democratic processes. Since TFC must meet its quota for non-political content, its ability to fact-check political statements or debate content during elections would be limited.

The Necessity to Regulate Digital Platforms

TFC argues that without regulatory oversight, platforms could not be held accountable, resulting in several issues, such as the lack of transparent procedures dealing with user complaints and unexplainable algorithmic behavior. Platforms often are not held responsible for promoting harmful advertisements, despite profiting significantly from selling user data to advertisers, political campaigns, and other actors. TFC contends that digital platforms should balance their pursuit of profits with the protection of public interest and the integrity of the democratic process. It also advocates for legislation to hold platforms legally accountable, ensuring their operations contribute to societal well-being.

TFC's opinion reflects the findings of the recent disinformation surveys it had commissioned.[110] The 2023 Annual Disinformation Survey (2023 假訊息年度大調查) showed that nearly 90% of respondents support "legislation requiring social media to establish self-regulation mechanisms for disinformation," while close to 80% favor "legislation to increase algorithm transparency."[111] These findings indicate strong public support for holding platforms accountable. However, TFC believes that the National Communications Commission has not effectively pushed for digital intermediary legislation, made worse by the absence of relevant bipartisan efforts.

Furthermore, TFC has advocated for the empowerment of state-funded media. It believes that algorithm-driven echo chambers created by profit-oriented private media limit users' exposure to diverse perspectives and make dialogue across viewpoints increasingly difficult. In an age of widespread disinformation, having a powerful state-funded media could force commercial media outlets to uphold journalistic ethics or risk losing viewership. The state-funded media would also serve as a reliable source of information within the democratic society.

However, the push for a more powerful state-funded media has been met with much resistance. Many politicians, TFC believes, are wary of an unbiased media's ability to expose scandals. Moreover, many private news outlets are already struggling financially in the face of severe competition from social media platforms; the lackluster funding of traditional news outlets makes it challenging to compose high-quality articles. Taiwan's media ecosystem is further compromised by pressures and influences from China. In the face of oversized challenges, TFC remarks, it remains committed to confronting the threats posed by disinformation and information manipulation, working on the frontlines to defend Taiwan's democracy.

Enhancing Media Literacy

TFC, despite being a fact-checking organization, has emphasized the importance of media literacy. During workshops for journalists and the general public, TFC introduced AI-detection tools, shared case studies on AI-generated disinformation, and provided

guidance to improve awareness and media literacy regarding AI-manipulated content. TFC notes that many significant social changes have historically emerged from grassroots civic movements, and it sees media literacy as no different.[112] By fostering media literacy from the ground up, citizens can build the resilience needed to navigate today's complex and often overwhelming information environment.

To bring this goal to fruition, TFC collaborates with organizations like MyGoPen, FakeNewsCleaner, the National Association for the Promotion of Community Universities, the Media Literacy Lab at National Chengchi University (政治大學傳播學院媒體素養研究室), the Association for Quality Journalism (優質新聞發展協會), and the Taiwan Media Watch Foundation (財團法人台灣媒體觀察教育基金會). Together, they work on the Google-sponsored Taiwan Media Literacy Education Initiatives project, which aims to strengthen media quality and literacy across the country.[113]

AI-Generated Disinformation in the 2024 Election: Detectable but Increasingly Sophisticated

During election periods, the amount of political disinformation circulating usually would surge, and TFC's fact-checking efforts have converged on such topics. During Taiwan's 2024 presidential election, for instance, TFC has identified several themes among the disinformation circulated:

1. Political brigading;
2. Disinformation about controversial political topics, such as green energy, solar power, and vaccines;
3. Disputable narratives about Taiwan's relationship with China and the U.S.;
4. Unfounded claims of electoral fraud;
5. The revival of past controversies, including military and civil service pension reforms, education reforms, and U.S. pork imports.[114]

Throughout the election cycle, TFC encountered various AI-generated disinformation campaigns,[115] such as fabricated audio clips of Ko Wen-je (柯文哲) and edited videos of Lai Ching-te (賴清德) discussing the "KMT-TPP Coalition (藍白合)". Problematic contents often originate from anonymous accounts and are amplified by influential figures on social media, which prompted TFC's suspicion about large-scale concerted attacks.

In response, TFC collaborates with media outlets to fact-check statements by political candidates on major issues[116] and makes predictions on the themes of upcoming false narratives to prepare the public against future disinformation.[117]

TFC is also testing tools to detect AI-generated content. In a recent case, it discovered a deepfake video showing a U.S. congressman endorsing a Taiwanese political party.[118] Due to how little of the original video was edited—only the voice and the movement of the lips—most AI detection tools failed to flag the video. However, drawing on journalistic expertise, TFC found it unlikely for the official to be making such a statement. It then found the original video, confirming forgery. This case highlights the imperfection of automated tools; it is important to apply common sense and cross-reference multiple sources when fact-checking.

19. MyGoPen

The name "MyGoPen" translates to "stop lying (麥擱騙, mài koh phiàn)" in Taiwanese. Established as a fact-checking website in 2015, MyGoPen registered as a company in November 2019 and received certification from the International Fact-Checking Network (IFCN) in March 2020.[119] When encountering suspicious information, MyGoPen conducts fact-checks, consults relevant experts, and presents clear, accessible summaries with complete references to help users improve their information literacy.

To make fact-checking more accessible, MyGoPen offers a website and an official LINE account where the public can quickly access the latest reliable news. Moreover, it provides a dedicated one-to-one messaging service on LINE, allowing users to receive direct assistance in verifying information accuracy.[120]

Using GenAI to Create & Debunk Disinformation

Currently, MyGoPen focuses on verifying facts and providing evidence to support its findings. When addressing manipulative opinions, it explains how certain perspectives may mislead the public by giving thorough context and background. Although AI has not been integrated into MyGoPen's fact-checking process, the organization is exploring such possibilities given its resource limitations.

MyGoPen sees the potential of using AI to automatically transcribe videos, allowing fact-checkers to efficiently identify their key points and streamline the verification process. However, some AI tools are costly, which can be a barrier for organizations with small budgets. Moreover, the vast and diverse set of AI detection tools is prone to have disagreements among themselves, making it difficult to confirm with certainty whether the content was AI-generated.

MyGoPen has observed an increasing trend of AI-generated disinformation during recent election cycles. The widespread use of GenAI has made it easier to produce believable false content, leading to a rise in the volume of disinformation and making fact-checking more difficult. Disinformation typically comes in the form of videos or articles, such as the article on the fabricated "The Secret History of Tsai Ing-wen (蔡英文秘史)" or the video of Joe Biden speaking Mandarin.

MyGoPen has identified three purposes for using GenAI to create disinformation: entertainment, malicious manipulation, and organized attacks. For example, the Biden video was originally meant for entertainment. The case involving Tsai Ing-wen's fake "secret history", on the other hand, is an example of malicious manipulation, where AI was used to create and disperse multiple videos from the same script.

MyGoPen collaborates with other fact-checking organizations like TFC and Cofacts, sharing latest trends observed by the organizations in a LINE group chat. When encountering cases of widespread disinformation, such as "The Secret History of Tsai Ing-wen", MyGoPen shares its findings with organizations like DTL, IORG, and Taiwan AI Labs to help them further investigate the manipulation tactics involved. MyGoPen also partners with FakeNewsCleaner to promote media literacy in local communities.

As an IFCN member, MyGoPen has maintained its independence from government agencies, opting not to extensively cooperate with law enforcement agencies in combating fraud. MyGoPen believes that disinformation debunking is more effective when handled by independent third parties; government-led efforts will be perceived as politically biased, and thus will not be trusted by the public.

The Need for Platform Accountability Regulations

MyGoPen partners with platforms such as Google, Facebook, Yahoo, Dcard, and LINE. MyGoPen's fact-checking articles are shown on Yahoo News and LINE Today. LINE also promotes its official account free of charge. MyGoPen also partners with Facebook, which authorizes MyGoPen to flag verified disinformation on its platform. The "flag", which comes with a link to an article that provides additional context, would not only allow users to easily distinguish real content from problematic ones, but also prompt Facebook's algorithm to reduce its visibility. MyGoPen only has a de facto partnership with PTT, which would remove content that TFC or MyGoPen finds misleading or false. Dcard provides MyGoPen with an official account and communication channels to report suspicious content. Google provides funding for MyGoPen without interfering with its daily operations.

MyGoPen observes that because global hegemons like Facebook and Google apply the same policies against disinformation in every corner of the world, their policies would resemble generic principles more so than actionable plans. Without localized regulations, Google Taiwan would have to rely on these abstract guidelines. Although the Taipei Computer Association (台北市電腦公會) introduced the Self-Regulation Guidelines for Combating Disinformation in 2019, the Guidelines do not have the necessary authorities to make digital platforms abide by them.[121] Recognizing this problem, MyGoPen advocates for a digital intermediary law, tackling issues like fraud and child protection that have public consensus, to clarify platform accountability and build public support for further regulations.

Disinformation Fuels Division and Undermines Democracy

MyGoPen believes that everyone is vulnerable to disinformation; that we'd be inclined to believe in any information that resonates with our personal experience. In recent years, GenAI has made it easier to create and disperse disinformation; platform algorithms often create echo chambers that expose people to overwhelming amounts of chaotic information, leading to greater polarization.

When partisans become radicalized by emotionally charged disinformation, rational dialogue becomes difficult, making it more difficult for democratic societies to build consensus. This ultimately undermines democratic decision-making and weakens trust in democratic institutions.

20. Cofacts

Cofacts (真的假的) was launched in 2016 as an open-source project in response to widespread disinformation about marriage equality on social media.[122] Founded by concerned engineers, Cofacts is a collaborative

fact-checking platform that uses crowd-sourced verification and a chatbot to address suspicious information. Cofacts enables public participation in fact-checking and turns their results into a practical tool for users, promoting media literacy and critical thinking to combat disinformation. In 2023, its founders established the Taiwan Information and Fact-Checking Association to sustain Cofacts' operations, with a core team of 3—5 full-time members and over 2,000 volunteers.

Synergizing Human & AI Efforts to Fact-Check

Cofacts primarily focuses on information circulating in private settings. Users can forward suspicious messages to Cofacts' LINE account.

Cofacts' AI would then search its database to determine if the content of the message was known to be false. If no similar messages could be found in the database, the AI would then categorize the suspicious message by its topic (e.g. political propaganda, international relations, and gender equality) and relayed to a platform for volunteers specialized in that topic to verify or debunk. Cofacts also employs chatbots to guide volunteers through the fact-checking process to ensure its thoroughness. After the verification or debunking of said message, the AI would be able to automate appropriate responses when similar messages were received through Cofacts' LINE account.

By extensively fact-checking every message it receives, Cofacts hopes to encourage its users' critical thinking skills and cultivate their abilities to reflect on the sources and intent of a piece of information, moderating their knee-jerk reactions of fear and anger when encountering inflammatory media contents. Recently, Cofacts partnered with MyGoPen and FakeNewsCleaner to deliver community workshops on identifying and fact-checking false information and to enhance media literacy skills, focusing especially on the elderly in lifelong learning programs.

Limitations of Fact-Checking on LINE

A major limitation of Cofacts' fact-checking method through its LINE account is its inability to trace its origins. Since LINE messages are end-to-end encrypted, third-party organizations cannot effectively trace the routes by which the disinformation had travelled to reach one particular user. Thus they would not be able to identify the users who have bought into the disinformation and target their debunking efforts towards those users.

GenAI's Limited Impact on the 2024 Election

During Taiwan's 2024 presidential election cycle, Cofacts observed some instances of GenAI being used to create disinformation, such as a deepfake video of Xi Jinping (習近平) commenting on Taiwan's presidential candidates.[123] However, Cofacts noted that the overall impact of generative AI-generated disinformation was limited.

Cofacts suggests that, though GenAI can efficiently produce rephrased versions of the same content, increasing its volume, this efficiency does not necessarily lead to the creation of disinformation. The biggest problem with information overload is that it

makes it harder for the public to discern fact from fiction. Although foreign interference and disinformation have long influenced Taiwanese elections, whether GenAI will become a decisive factor remains a question for further research.

Cofacts emphasizes that neither GenAI nor disinformation are entirely new issues. As most current research on GenAI is technical, Cofacts believes that GenAI's social impact—such as its impacts on inequality, infringements of digital rights, and unemployment—should be more extensively studied for the effective development of societal responses. Furthermore, GenAI may widen the existing divide between the digitally savvy and the old-school people, deepening social inequality and highlighting the need for further research and solutions to address these challenges.

Disinformation's Role in Undermining Democracy

Even if AI-driven disinformation had limited impacts on Taiwan's 2024 elections, we should not overlook disinformation's broader social effects, including the polarization of public opinion and the erosion of trust in democratic institutions. In addition to offering fact-checking tools, Cofacts encourages public participation in fact-checking and online disinformation debunking. It also organizes regular editorial meet-ups and training sessions to empower citizens to not only identify suspicious information but also contribute to debunking efforts.

21. Analysis and Discussion: Fact-Checking Organizations

The three fact-checking organizations we've interviewed—two of which have adopted AI in their operations while the third is contemplating it—agree that the use of GenAI for information manipulation has made disinformation campaigns more sophisticated and lowered the cost of creating multiple versions of the same script, leading to an overall increase in the volume of disinformation. This surge in both accurate and erroneous information makes it difficult for resource-limited fact-checking organizations to keep up with the rapid spread of rumors. However, during Taiwan's 2024 presidential election, expedient fact-checking has limited the overall impact of AI-driven disinformation.

Despite that, all three organizations agree that detecting AI-generated content remains challenging. Detection tools often lack consistency and struggle to keep up with the rapid advancements in GenAI technology, which may soon outpace current detection capabilities.

All three organizations agree that platforms' responses to disinformation have been inadequate. The lack of transparency surrounding algorithms, complaint mechanisms, and content removal policies makes it difficult for nongovernmental organizations to hold platforms accountable for their dissemination of disinformation, underscoring the need for governmental regulation. TFC and MyGoPen stress the importance of extensive public dialogue during

the legislative process, while Cofacts highlights the need to address inequalities and protect digital rights. TFC further argues that a strong public media sector is vital to a healthy media ecosystem.

22. Anti-Information Manipulation Organizations

Techniques of information manipulation are just as critical as the accuracy of the information. Manipulators often employ networks of bot accounts to create "parallel realities" that mislead the public using partial truths. With the rise of AI, GenAI in particular, information manipulation has become more sophisticated—not only by generating hard-to-detect false information but also by executing more nuanced, highly coordinated operations that are increasingly difficult to uncover. The findings of these organizations could serve as building blocks of the government and platforms' responses to information manipulation.

To understand the efforts of Taiwanese NGOs on information manipulation, we have interviewed representatives from three organizations: Taiwan AI Labs, Doublethink Lab (DTL), and the Taiwan Information Environment Research Center (IORG).

Each organization focuses on different aspects of information manipulation. Taiwan AI Labs specializes in detecting unusual account behavior, concerted actions, and information dissemination patterns.[124] DTL analyzes foreign interference in Taiwan's elections, focusing on identifying the perpetrators and understanding the narrative frameworks. IORG, on the other hand, surveys Taiwan's information environment, studying the sources, narratives, and reasonings of the manipulated information and developing a credibility assessment model to help the public distinguish facts from inferences and opinions.

The sections below addresses the following key questions regarding the organizations:

1. How did the rise of GenAI make researching and detecting information manipulation more difficult for these organizations?
2. How has GenAI been used to manipulate information during Taiwan's 2024 election cycle, and what impact did it have on elections, democracy, and society?
3. What are these organizations' experiences with digital platforms? What are their observations on platforms' responses to disinformation and manipulation?
4. Are these organizations using AI or related technologies to identify or counter information manipulation? If so, how?

23. Doublethink Lab (DTL)

Doublethink Lab (台灣民主實驗室, DTL), established in September 2019, primarily researches the influence campaigns and information warfare by authoritarian states, assesses China's global influence quantitatively, and studies the societal impact of disinformation. To achieve their goals, DTL developed several key resources: the China Index, which quantifies China's global influence;[125] the Disinfo Walkthrough (破譯假訊息新手村), an information literacy toolkit;[126] and a series of research reports on China's information warfare and related strategies.[127]

Foreign Actors in Information Manipulation

Doublethink Lab (DTL) focuses on studying concerted actions by foreign actors in Taiwan. It determines whether these organized attacks originate abroad and assesses their societal impacts. DTL also examines narratives associated with these operations, tracking changes in messaging over time. To identify foreign involvement, DTL looks for specific indicators, such as simplified-to-traditional Chinese text conversion errors, distinctively foreign terminologies, and Facebook's Page Transparency information.

DTL compares coordinated activities on platforms like Facebook and Instagram with those on Chinese platforms, including Weibo, WeChat, and TikTok, to determine if content or behaviors are driven by foreign actors. Previously, DTL found that information often originated on Chinese social media and then spread to Taiwan. More recently, however, concerted actions have taken the more effective approach of magnifying local disagreements in Taiwan.

DTL maintains regular intelligence sharing and collaboration with some of Taiwan's fact-checking organizations. Moreover, DTL has organized a regional network across the Indo-Pacific to monitor and share insights on foreign organized attacks. This network spans 11 countries and comprises 12 experts (scholars, journalists, analysts, and NGO representatives).

In the 2024 election, DTL observed that China frequently leveraged existing internal issues within Taiwanese society to exacerbate social conflicts and undermine public trust. The narratives promoted by these campaigns aimed to erode confidence in Taiwan's ruling party and reduce trust in allied nations, such as the United States and Japan. Tactics used included using half-truths and hard-to-verify claims, making disinformation more challenging to counter.

Platforms Should Proactively Address Concerted Manipulation

DTL works closely with platforms like Facebook and YouTube, identifying suspicious accounts and providing the reasonings behind their suspicions. Platforms could then conduct their own reviews, taking actions—such as removing accounts—if they find the accounts violating their policies.

DTL notes that it is often challenging to trace the origins of concerted manipulation efforts; one would need information from multiple platforms to fully understand the scope of concerted operations. While platforms have the capacity to engage in such collaboration, they are often reluctant to commit the necessary resources. Therefore DTL believes that legislative measures like Taiwan's proposed Digital Intermediary Service Act are essential to hold platforms accountable.

Currently, the Taiwanese government does not have the authority to oversee digital platforms, making it difficult to enforce standards on multinational corporations. DTL argues that Taiwan will need further government regulations to ensure that platforms take on the level of responsibility expected from society.

Information Manipulation in the 2024 Elections

As the election neared, DTL noticed an intensification of China's manipulation campaigns, brigading against the incumbent DPP (民主進步黨, Democratic Progressive Party) government and launching smear campaigns on specific candidates. Foreign disinformation campaigns have increasingly fueled partisan hatred using conspiracy theories—such as "The Secret History of Tsai Ing-wen," "Lai Ching-te's Illegitimate Child," and "Opposition to Indian Migrant Workers"—making disinformation harder to debunk and increasing the social costs of open dialogue. GenAI was used to create deepfake anchors who present disinformation as news, as well as to generate fake profile images to spread these narratives further on social media. For instance, many of the accounts involved in the case of "The Secret History of Tsai Ing-wen" had used AI-generated profile pictures. The goal of these operations in the long run, DTL emphasizes, is to cultivate Taiwanese people's distrust of their government, their international allies, and their democratic institutions while intensifying divisions between political factions.

Two major trends defined the 2024 election: the increasing influence of short videos and the widespread use of AI in disinformation. TikTok, widely used by younger generations, became a key channel for manipulated content, though some people's caution toward Chinese platforms has limited its reach. This reluctance, however, has led to fewer fact-checking efforts on TikTok.[128]

For example, in the lead-up to the election, conspiracy theories about vote rigging were heavily promoted on TikTok and similar platforms, often paired with narratives like "mainstream media can't be trusted," "both major parties control the media," and "only social media reveals the truth." Following the election, these narratives exploited certain people's disappointment with the election results to promote distrust in Taiwan's democratic process.

Who is Most Susceptible to Disinformation?

DTL notes that attackers are now leveraging AI to analyze audience interests, feeding them disinformation custom-made to suit their interests, a strategy akin to digital marketing, thus making the vulnerable even more vulnerable—a vicious cycle.

DTL's report highlighted the fact that disinformation narratives resonate most with those already dissatisfied with Taiwan's democracy.[129] Narratives such as "the Taiwanese government condones fraud," "the government provides harmful vaccines and toxic eggs," "the ruling party is corrupt and promotes cronyism," and "the Democratic Progressive Party and the Chinese Communist Party (中國共產黨, CCP) are equally repressive" often share the same audience; respondents who agreed with one of these narratives tended to believe the others as well. DTL found that those dissatisfied with Taiwan's democracy are more inclined to accept U.S.-skeptical narratives, with a higher proportion of these individuals using Chinese social media platforms like TikTok, WeChat, and REDnote (小红书).

Conversely, respondents optimistic about Lai Ching-te's presidency and confident in Taiwan's democratic system tended to be more cautious of Chinese influence and less receptive to anti-U.S. narratives.

The Future of Information Manipulation

DTL anticipates that China's disinformation tactics will increasingly blur the line between foreign interference and local discourse, increasing the difficulty of tracing and enhancing the effectiveness of disinformation. Chinese state media and operatives will continue to amplify internal conflicts within Taiwan, using local lingua, cultural references, and local agents or sympathizers to spread propaganda. Distribution tactics are also expected to evolve from copy-pasting identical messages to using GenAI to mass-produce diverse yet similarly themed content at low costs, making information diffusion more difficult to trace. All in all, GenAI has enabled decentralized production and dissemination of disinformation, allowing for more varied content and more made-believe bot accounts that effectively put their foreign creators in camouflage. It increases the difficulties of tracking concerted disinformation activities and decreases Taiwanese citizens' vigilance against them.

China's disinformation strategy is comprehensive and long-term oriented, with elections representing only one facet. DTL warns that sustained foreign disinformation campaigns could undermine public confidence in Taiwan's democratic institutions, leading to greater social division and reducing Taiwan's resilience against manipulation.

24. Taiwan Information Environment Research Center (IORG)

Founded in 2019 by media professionals, social scientists, data engineers, and social activists, the Taiwan Information Environment Research Center (台灣資訊環境研究中心, IORG) is a non-governmental research organization dedicated to analyzing Taiwan's information environment, advancing information literacy, and fostering partnerships in the information sector using data science.[130] Guided by their motto "open by default, trusted by the public (預設開放、公眾信任)," IORG makes its research, methodologies, data, and source code openly accessible, maintaining public accountability while working to foster fact-based, scientifically grounded public discourse online.[131]

IORG's ongoing publications include annual reports[132] and weekly information environment bulletins.[133] Their weekly bulletins feature credibility assessments on media content, helping readers recognize and guard against disinformation.[134] In 2022, it released A Guide to Information Literacy, transcribing its research into accessible formats for the general public.[135] To promote information literacy and media education, IORG collaborates with the Taiwan Pang-phuann Association of Education, bringing media literacy programs into schools.[136]

Narratives in Information Manipulation Reflect Collective Psychological Vulnerabilities

Taiwan's open and diverse information environment makes the public especially

vulnerable to the spread of disinformation by news outlets, social media platforms, and short video sites. This chaotic environment breeds fragmentation, polarization, and reliance on influencers. In this environment, information manipulation could easily obstruct rational public discourse, weaken social trust, and undermine public confidence in the government and democratic institutions.

IORG analyzes narratives used in information manipulation to identify underlying collective psychological states, social concerns, and common storytelling techniques. Attackers often craft content that appeals to popular sentiments in order to maximize engagement and reinforce certain beliefs. By studying these narratives, IORG could effectively picture Taiwan's collective "psychological landscape" and identify "social vulnerabilities." This insight helps NGOs and government agencies address society's weaknesses, strengthen social resilience, and improve public communication strategies.[137]

Manipulating Information to Undermine Democracy

IORG highlights that China's manipulation campaigns promote a pro-China, anti-Taiwan narrative aimed at undermining Taiwan's democracy, sovereignty, and national identity. By framing freedom and democracy as the political opinions of a "small separatist faction," these campaigns seek to delegitimize Taiwan's democratic ideals and create a parallel reality for Chinese-speaking audiences. As a result, individuals swayed by these narratives, whose worldview would become increasingly incongruent with that of democratic societies, become less likely to support Taiwan's DPP or democratic ideals.[138]

During the 2024 election cycle, IORG noticed China's persistent efforts, focused on attacking the DPP and its presidential candidate, to influence the Chinese-speaking people. Chinese state media also used platforms like TikTok to amplify anti-DPP and anti-U.S. narratives from Taiwanese commentators such as Julian Kuo (郭正亮), Dale Wen-chieh Jieh (介文汲), Lai Yueh-tchien (賴岳謙), and Alex Tsai (蔡正元). The tactic of using "Taiwanese voices to criticize Taiwan" was intended to channel the fear of war and the skepticism of the U.S. within its audience, which in turn would raise positive sentiment toward China and shape voting behavior.[139]

IORG also noted the spread of false claims on the issue of electoral fraud. As in previous elections, these claims portrayed minor irregularities in the voting process as evidence of election rigging. These fake news have spread quickly via LINE, YouTube, and TikTok, eroding public trust in the democratic process. A new tactic identified by IORG in this election cycle was the use of fake polls, orchestrated to influence public opinion. In response, IORG created a manual to help citizens critically interpret polling data.[140]

Chinese disinformation campaigns often use terms like "Democratic Progressive Party authorities" to blur the lines between Taiwan's government and its ruling party—a tactic sometimes echoed in local media. This tendency, according to IORG, reinforces an authoritarian mindset that conflates the party with the state. Thus, IORG calls for the unambiguous separation of political parties from the government. They argue that the government should remain neutral, respond to input from civil society, and exercise caution in its messaging, while political parties should

articulate clear positions and narratives on political issues. Maintaining a clear distinction between the government and the party is crucial for upholding democratic principles in Taiwan.

GenAI Raises Fact-Checking Costs

What role does AI play in information manipulation? IORG observes that AI accelerates the production of manipulated information. AI could quickly diversify both the content and format, making it harder to discern truth from falsehood. The goal of using generative AI to create false content is often not just to convince people—it's also to increase the costs of fact-checking. IORG emphasizes that while the role of GenAI in creating disinformation should be closely monitored, there is no need for panic, for now.

On the other hand, IORG considers GenAI's capabilities insufficient for its needs, citing the meager 60% accuracy for tools like ChatGPT. However, IROG does use AI tools like Whisper to convert audio to text, build its own data repositories, and experiment with open-source machine-learning models for specific applications.

IORG believes that by continuously exposing these manipulation tactics, the public can become more aware of the common patterns, thus increasing the public's resistance against information manipulation.

Limited Platform Self-Govornance

IORG argues that current regulations to enforce platform accountabilities are insufficient. Many platforms publish transparency reports detailing their data-sharing practices and collaborations with governments, but these reports often do not provide information on the accounts removed and why they were removed.

This lack of transparency leaves the public unclear on the standards platforms use to make such decisions. Thus, IORG hopes for continued debates on the implementation of laws similar to the Digital Intermediary Service Act, in order to build a strong social consensus on platform accountability mandates.
IORG calls for platforms to take on greater responsibility by giving open access to selected datasets, implementing account appeal mechanisms, and increasing transparency to allow for public oversight. Platforms should also support initiatives that strengthen the information environment and promote a healthy digital ecosystem.

IORG suggests that while formal collaborations between digital platforms, fact-checking organizations, and government agencies may not be necessary, regular and open communication among them is essential. It argues that platforms should offer consistent support to NGOs worldwide to uphold information integrity and assist with fact-checking efforts.

Collective Responsibility to Curb Information Manipulation

Disinformation campaigns often intensify during major public events. Taiwan's complex information landscape, coupled with the increasing sophistication of GenAI, presents significant challenges for fact-checking and research on information manipulation.

IORG argues that disinformation cannot be fully eradicated and instead calls for a comprehensive approach—through research, education, and dialogue—to minimize its impact on democracy.

IORG advises against framing government authorities as bearing the sole responsibility of protecting a helpless public against information manipulation. Instead, they view it as a digital rights issue: by limiting access to accurate information and diminishing the public's ability to participate in civic matters, disinformation compromises the digital rights of everyone.

In their 2023 Taiwan Information Environment Policy and Action Recommendations (防治資訊操弄，改善公共討論，強化民主韌性), IORG encouraged all parties to focus on three goals: preventing information manipulation, improving public discourse, and strengthening the information environment. It provided unique recommendations for nine key actors: the government, political parties, politicians, news media, social media platforms, research institutions, schools and educational authorities, educators, and citizens. Through a collaborative, community-based approach, IORG aims to reduce the harmful impact of information manipulation on Taiwan's democratic society.[141]

25. Taiwan AI Labs

Founded in 2018, Taiwan AI Labs is dedicated to developing trustworthy and responsible AI. AI Labs emphasizes "volume equality," asserting that only human-operated accounts should enjoy freedom of expression, and that human voices should not be drowned out by the bot accounts. To achieve this, AI Labs uses AI to analyze organized brigades on social media platforms to identify suspicious bot accounts. The organization also aims to increase public awareness of manipulation tactics, helping people become more vigilant against information manipulation.

Developing AI Tools to Uncover Information Manipulation

While current technologies are still capable of detecting traces of GenAI usage, it may not be the case for too long, due to the ongoing advancements of AI. Also, as manipulation tactics grow beyond producing disinformation, the traditional approach of fact-checking becomes less effective. In response, AI Labs recommended focusing on analyzing organized attacks and improving public digital and media literacy to strengthen public awareness of manipulation tactics.

AI Labs has a web crawler team that gathers qualitative data from news outlets and social media platforms. Its research team then dissects the data, identifying behavioral signals indicative of unusual user activity using AI algorithms developed by themselves. According to AI Labs, concerted attacks involve numerous accounts that act in harmony with each other, such as accounts that only interact with certain posts or those that comment at the same time.

These "troll accounts" can influence platform algorithms to boost the visibility of some specific content. To give the public insights into online information manipulation, AI Labs introduced Infodemic, a web page featuring visualizations of the patterns of such concerted behavior on digital platforms.[142]

AI Labs has also created Miin (迷因), an application that monitors content on social media. Miin uses AI to collect content from various media sources and to flag manipulative content. The app, aiming to reduce public exposure to misleading information, also serves the content of Infodemic.

Profit vs Social Responsibility: A Platform's Dilemma

AI Labs believes that there are many problems with the current platform-friendly regulations. Social media platforms benefit from policies like net neutrality and Section 230 of the U.S. Communications Decency Act, which shield them from liability for false or harmful content circulating on their networks.

These protections allow platforms to overlook disinformation, hate speech, and even fraud—content that often boosts their revenue. Malevolent actors, who also purchase ads, further diminish platforms' incentives to remove harmful material. As a result, users' perceptions and emotions are skewed by misleading or hostile content. This pursuit of profit has come at a steep cost: polarized public discourse, increasingly irrational debates, and, ultimately, the erosion of democratic processes.

AI Labs observes that the Taiwanese government has not allocated sufficient resources to address gaps in social media platform oversight. It cites a case of systematic account hijacking on PTT, where compromised accounts were used to post content via proxy servers. An IP check indicated that many of these posts passed through routers controlled by malicious actors.

AI Labs suggests that this issue may extend to other platforms and notes that Taiwan's law enforcement agencies currently lack the capacity to conduct such investigations. It recommends that the government undertake thorough investigations to better understand the motivations and methods involved.

Current regulations also permit platforms to enforce content censorship at their discretion. For example, Facebook's content removal standards have been inconsistent over time and have, on occasion, aligned with the demands of authoritarian governments. AI Labs notes that digital platforms hold significant power but face limited accountability. It recommends that the Taiwanese government consider adopting EU-style regulatory frameworks to more effectively address disinformation and information manipulation.

Concerted Activities to Influence the 2024 Elections

During Taiwan's 2024 election, AI Labs observed extensive organized attacks. On Infodemic, AI Labs has kept track of over 14,000 suspicious accounts, responsible for more than 730,000 posts, from January 1, 2023, to the days following the election. Nearly half of these accounts went inactive immediately after the election.[143]

AI Labs identified several patterns during the election, including:

1. The widespread use of GenAI for information manipulation
2. A few actors, most of which are foreign, steered the conversations on certain key

topics, often echoing narratives from Chinese state media
3. On TikTok, content from these actors generally portrayed Taiwan, the U.S., and Japan negatively while casting China in a favorable light
4. Content from these actors often showed support for specific candidates
5. Short videos had a notably stronger influence than in previous elections
6. A few actors appeared to be aiming to reshape the alliances between political parties
7. Some actors joined or managed non-partisan chat groups for the purpose of injecting political messages into them

During the election period, AI Labs identified bot accounts with AI-generated profile pictures engaging in activities such as content creation and amplifying specific narratives. These tactics showcased increasingly sophisticated manipulation methods, including the promotion of CCP propaganda disguised as neutral and factual information.

It is important to note that not all coordinated manipulative activities during the election period were explicitly pro-CCP or anti-DPP. AI Labs observed numerous campaigns targeting various groups, often attacking each other and further exacerbating polarization.

26. Analysis and Discussion: Anti-Information Manipulation Organizations

During Taiwan's 2024 presidential election, AI Labs, DTL, and IORG each reported instances of GenAI being deployed in information manipulation, including AI-generated videos and audio circulating across various media platforms. AI Labs and DTL observed that these AI-generated false narratives were designed to be more relatable and were distributed through increasingly decentralized channels, making them harder to trace and detect. IORG highlighted that GenAI has significantly increased the volume and diversity of disinformation, further complicating and raising the costs of fact-checking efforts.

This election cycle saw the introduction of several novel tactics, most strikingly the unprecedented use of short videos and generative AI to influence users with shorter, more fragmented, and highly targeted content. All three organizations observed correlations between a user's political affiliation, their preferred digital platforms, and their susceptibility to disinformation.

Taiwan's political divides, often rooted in deeper ideological differences, have created partisan echo chambers where individuals affiliated with the same party live in close communities and consume identical media sources. This polarization reduces opportunities for meaningful dialogue and poses a significant challenge to the health of Taiwan's democracy.

To reverse these trends, each organization has launched initiatives aimed at enhancing media literacy and critical information evaluation among Taiwan's citizens. AI Labs developed the Miin platform to streamline information collection and Infodemic to help the public recognize concerted attacks on social media. IORG produces weekly bulletins and publishes educational materials to guide citizens in

assessing information credibility. Meanwhile, DTL recruits volunteers to conduct research with scholars, equipping the public with tools to identify manipulation techniques.

To tackle the challenges posed by the increasing use of GenAI in information manipulation, DTL investigates how foreign actors employ AI technologies to distort information; AI Labs develops AI tools to automate the detection of manipulated content; and IORG leverages real-world examples to enhance public media literacy, fostering greater societal resilience against such tactics.

All three organizations agree that social media platforms must take greater responsibility for combating information manipulation. However, these platforms often act reactively and operate with limited transparency. They contend that platform self-regulation is inadequate and advocate for government intervention, given the role of malicious foreign actors and the profit-driven nature of multinational platforms that often prioritize engagement over public interest.

AI Labs specifically highlights that disinformation frequently boosts platform activity, discouraging proactive efforts to address harmful content. Moreover, the lack of transparency and public oversight in content removal processes risks infringing on user rights, emphasizing the need for legal frameworks to ensure accountability. At the same time, governments, as bodies subject to public scrutiny, must carefully balance the exercise of regulatory power with the protection of human rights—a vital but complex task in fostering a resilient democratic society.

Figure 6 : Overview of the Nongovernmental Organizations

	Function of Organization	Structure of Organization	Time of Founding	Date of Interview
Media Literacy Advocacy Organizations				
放伴	Promoting media literacy & information literacy Training of education personnel	Nonprofit	2020	Mar 28th 2024
假新聞清潔劑	Promoting media literacy & information literacy	Nonprofit	Dec 2018	Apr 9th 2024
Fact-Checking Organizations				
台灣事實查核中心 Taiwan FactCheck Center	Fact-checking Issue-focused analysis	Nonprofit	Jul 2018	Mar 29th 2024
MyGoPen	Fact-checking	Company	2015	Jan 24th 2024
真的假的 Cofacts	Fact-checking Promoting media literacy & information literacy	Nonprofit	Dec 2016	Jan 18th 2024
Anti-Information Manipulation Organizations				
Doublethink Lab	Researching information manipulation & foreign intervention	Nonprofit	Sep 2019	Jan 31st 2024
IORG	Researching information manipulation & foreign intervention	Company	2019	Feb 16th 2024
AI Labs.tw 台灣人工智慧實驗室	Researching information manipulation	Company	2017	Jan 30th 2024

V. DISARM

The DISARM framework was created by the Credibility Coalition's misinformation working group.[144] In 2019, this working group, referencing the ATT&CK framework (Adversarial Tactics, Techniques & Common Knowledge) developed by the U.S. non-profit organization MITRE, compiled 63 international information manipulation cases from 2012 to 2018, proposing the AMITT framework (Adversarial Misinformation Influence Tactics & Techniques). In 2020, MITRE and Florida International University modified the AMITT framework into the SP!CE framework (The Structured Process for Information Campaign Enhancement).[145] In 2021, the DISARM Foundation was established, and in 2022, it merged the AMITT and SP!CE frameworks into the DISARM framework, which it maintains and promotes.[146] Currently, the European Union's External Action Service and MITRE both adopt the DISARM framework, which is also included in the information manipulation-related data-sharing system established by the U.S. and EU governments.

27. DISARM Blue Framework

The DISARM Foundation, established in 2021, focuses on identifying patterns of information manipulation and devising effective countermeasures.[147] This initiative stems from the Credibility Coalition's misinformation working group, which compiled 63 international cases of information manipulation from 2012 to 2018.[148] These cases were initially analyzed in reference to the ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) framework developed by MITRE, a U.S. non-profit organization specializing in cybersecurity that was established in 2013. This led to the creation of the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework.

In 2020, MITRE, in collaboration with Florida International University, adapted the AMITT framework to develop the Structured Process for Information Campaign Enhancement (SP!CE). A year later, the DISARM Foundation was formed to oversee and further develop what is now known as the DISARM framework.[149] By 2022, both the AMITT and SP!CE frameworks were integrated into DISARM, which quickly gained traction, being adopted by the European External Action Service (EEAS) and MITRE for cybersecurity applications. Presently, the data-sharing systems related to information manipulation that are used by U.S. and EU authorities incorporate the DISARM framework.[150]

The DISARM framework is rooted in the field of information security and builds on the foundational ATT&CK framework developed by MITRE. The ATT&CK framework draws on military concepts, specifically, tactics, techniques, and procedures (TTPs). It explains the tactics that define the objectives of attackers; the techniques they employ; and the procedures they execute to achieve these goals.
The ATT&CK framework integrates TTPs along with essential knowledge and technologies needed to execute information security attacks. It includes principles such as firewall utilization and the psychological underpinnings

of human deception. This comprehensive approach enables a broader understanding of the entire attack lifecycle. The creators of the DISARM framework draw parallels between information security and information manipulation, noting that, while information security attacks focus on computers and network systems, information manipulation targets individual minds and social networks. This similarity underscores the analytical approaches common to both domains, emphasizing the strategic targeting of systems, whether technological or human.[151]

The DISARM adopts a structured approach similar to the ATT&CK framework, segmenting the process of information manipulation into four distinct phases: planning, preparation, execution, and evaluation. At each stage, attackers have specific tactical objectives that are achieved through various methods. For example, during the preparation phase, a tactical goal might be "establishing the legitimacy of the attacker," which could involve creating a fake news website. For an attack to be successful, all actions within the so-called kill chain must be flawlessly executed. Consequently, implementing defensive strategies at multiple points in the kill chain, for example, "reducing the credibility of the fake news website" significantly lowers the likelihood of an attacker's success.

To describe the framework's four stages in more detail: the planning stage focuses on strategic planning, objective setting, and analyzing the target audience; the preparation stage involves developing narrative angles, creating content, establishing legitimacy, building foundational assets within social networks, targeting the audience, and selecting appropriate channels for information dissemination; the execution stage is designed to test the initial dissemination, spread content, proliferate extreme content, create online trauma, and instigate offline activities; and finally, the evaluation stage centers on assessing the effectiveness of the campaign.

The DISARM framework details 244 techniques across its 16 tactical objectives, drawing a parallel to the ATT&CK framework, which differentiates techniques based on their use by "red teams" (attackers) and "blue teams" (defenders). This structured approach not only delineates potential threats but also strategizes proactive defense mechanisms. Therefore, this categorization helps equip a democratic country such as Taiwan, which acts primarily in a defensive role, to effectively identify and implement countermeasures against information manipulation attacks.[152]

For instance, in the context of AI-generated false information—for example, the development of AI-generated images and videos classified as deepfakes (T0086.002 and T0087.001)—proactive measures like "Prebunking" (C00125) can significantly raise public awareness about AI-generated disinformation. In addition, disinformation campaigns often seek to exploit traditional media to broaden their influence (T0117: Attract traditional media). In response, enhancing media literacy (C00073: Inoculate populations through media literacy training) and urging media outlets to avoid disseminating false information (C00154: Ask media not to report false information) can serve as effective countermeasures to curb the spread and impact of such manipulative practices.

The European External Action Service has successfully implemented the DISARM framework, utilizing it to detect, analyze, and document instances of information manipulation. This system aids in identifying threats and formulating appropriate responses.[153] In addition, the department has developed a specialized response framework specifically designed to combat foreign information manipulation and interference (FIMI).[154]

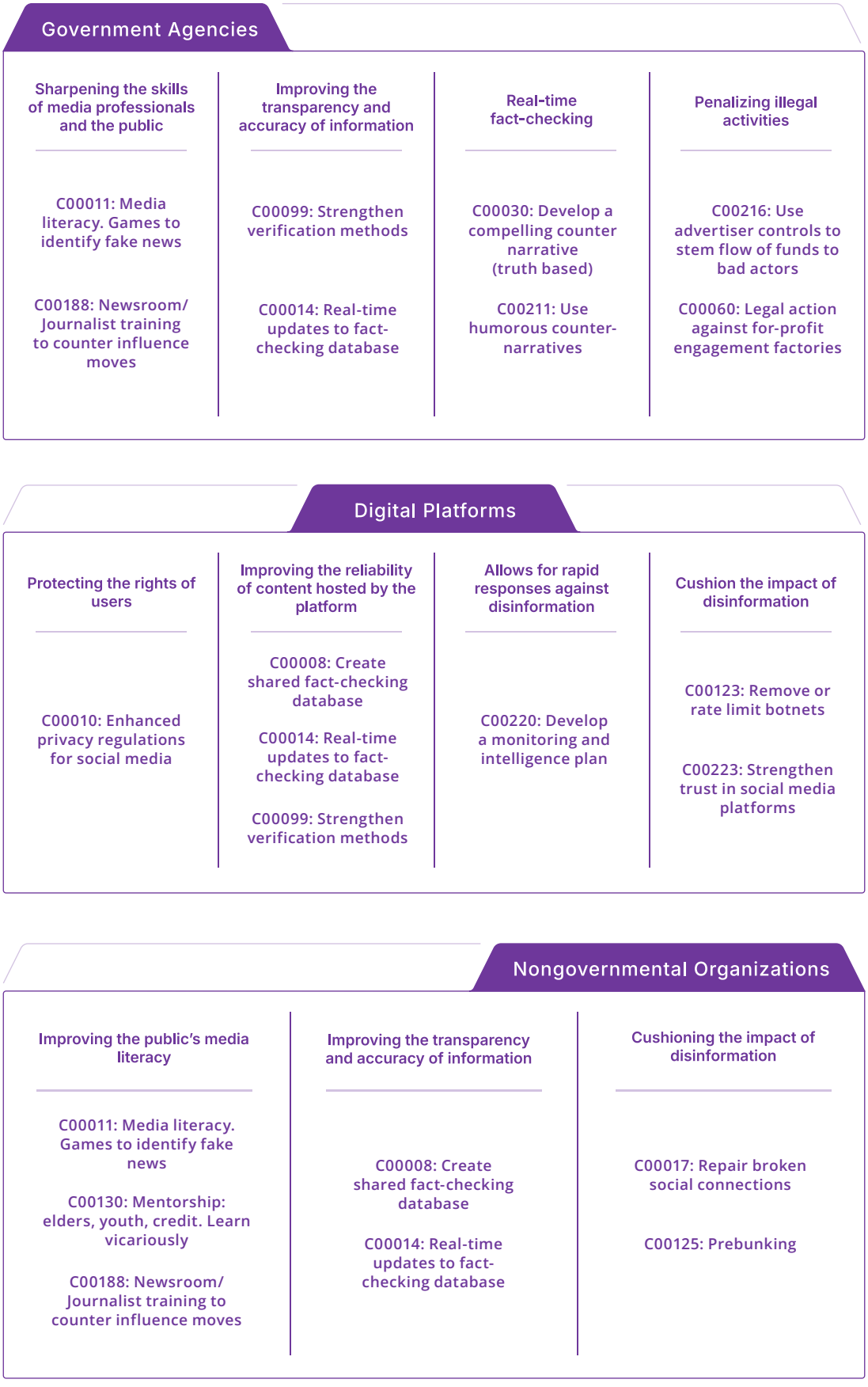
This report adopts the DISARM Blue Framework (DISARM for disinformation countermeasures and mitigation behaviors) to categorize the countermeasures against information manipulation taken by the Taiwanese government, Taiwanese civil society groups, and various digital platforms. This will help us understand the respective responsibilities of the government, nongovernmental organizations, and platforms. It will also allow us to identify areas of weakness and explore possibilities of collaborations between existing actors to address these challenges.

28. Applying the DISARM Blue Framework to Existing Efforts

The government, platforms, and NGOs have taken diverse and composite measures against disinformation and information manipulation. Below is the summary of their measures, presented using the DISARM Blue Framework.

Taiwan has developed an organic defense system that resembles the DISARM Blue Framework through the close collaboration between government agencies, cross-national digital platforms, and nongovernmental organizations. Yet there is much to be done, such as strengthening government regulations and addressing the challenges brought by emerging technologies. As important as taking down disinformation is the ongoing effort to enhance public media literacy. In the long run, the lack of effective mechanisms to evaluate the aforementioned efforts could undermine sustained collaboration between the government, NGOs, and platforms, making it a key area for improvement moving forward.

Figure 7 : Analysis of the government, platforms, and NGOs' efforts against disinformation using the DISARM Blue Framework



VI. Discussion & Recommendations

29. Shortcomings of Current Efforts

AI-Driven Disinformation in Taiwan's 2024 Elections

GenAI has become a powerful tool in information manipulation, with its (mis) use reaching a new height in Taiwan's 2024 elections. Since Gen AI lowers the barriers to disinformation, a fact agreed upon by organizations like MyGoPen, IORG, DTL, TFC, and AI Labs, its adoption allows for disinformation production at a larger scale, pace, and variation, making fact-checking increasingly difficult. However, as noted by TFC and AI Labs, Gen AI is still in its early stages, often producing content with detectable flaws or logical inconsistencies.

Despite the availability of AI tools to combat information manipulation, their adoption remains relatively limited. So far, they have been used to automate fact-checking (Cofacts), analyze qualitative data (AI Labs), and produce tools like Miin and Infodemic to raise public awareness (AI Labs). Reasons against wider adoptions include issues with accuracy and consistency (IORG) and cost (MyGoPen).

While the influence of AI-driven disinformation and information manipulation on Taiwan's 2024 presidential election has been limited, its long-term effects on society and democracy are deeply concerning. Much existing research by nongovernmental organizations and think tanks has established the correlation between information manipulation and the polarization of public opinion, the fuelling of hatred, and the undermining of trust within societies and across nations. This fosters polarized public opinion, undermines the dialogue necessary for democratic societies, and makes consensus-building increasingly difficult. As the space for dialogue and negotiation between groups shrinks and hostility intensifies, public trust in democratic institutions falters, leading to broader disillusionment with democracy. A causal relationship between information manipulation and voting patterns seems nothing more than its corollary.

However, as IORG had remarked, existing research could not identify the segments of the population that are exposed to manipulated information or their inclination to accept such narratives as truths. While correlations have been identified, causal relationships between information manipulation and factors that influence election outcomes (e.g. false narratives about a certain candidate) remain unproven. Further research should be conducted to address this deficiency.

It is one thing to prove the danger, it's another to mitigate its threat. To address the consequential real-life challenges of combating information manipulation, nearly all the organizations we have interviewed emphasized the importance of exposing manipulation tactics and methods to the general public. Anticipating vigorous disinformation campaigns in the 2024 election cycle, TFC released "2024 Election Rumor Playbook Revealed: Learn the Tricks Before They Appear (2024年選務謠言劇本

大公開 一起事先掌握謠言套路),"[155] a collection of fake news and impartial truths from previous elections which serve as examples of what not to believe. This proactive effort to raise awareness and enhance public vigilance has proven to be an effective measure against information manipulation.

Please refer to our first report of this series, *GenAI and Democracy: AI-Driven Disinformation in Taiwan's 2024 Presidential Election and Lessons for the World*, for more details on the effect of GenAI and disinformation on Taiwan's 2024 Presidential Election.[156]

Disinformation and Civil Society

For many people, politics takes up only a minute part of their lives, far from being their top priority. Consequently, while elections are hotbeds for information manipulation, we should not ignore the effects of information manipulation on the non-electoral aspects of civil society.

Research conducted by civil organizations and think tanks suggests that false or manipulated information primarily serves to polarize public opinion, intensifying antagonism and replacing solidarity and mutual care with a divisive "us versus them" mentality. It also reduces individuals' willingness to engage in dialogues and compromises. The interplay of anger, confusion, and disillusionment—both in the physical world and online environments—erodes public trust in democratic systems. As AI-generated disinformation exacerbates social divisions, it is crucial to build trust within communities. It's less about technical knowledge and more about creating spaces where people can discuss concerns with trusted peers.

The greatest danger of a chaotic information environment, as Dr. Tzu-Wei Hung (洪子偉) remarked, is not necessarily its effect on voter behavior, but rather its capacity to undermine trust in democracy. This erosion of trust can prompt people to choose authoritarianism over democracy.[157]

As Pang-phuann points out, fighting disinformation requires more than just raising public awareness; there must be a concerted effort by all members of our society to rebuild trust and understanding between individuals. IORG's identification of various social roles and their potential contributions could offer a valuable framework for such collaborative efforts. [158]

It is worth noting that most young people consume short-form videos. Not only do the viewers of short-form videos struggle to discern fact from fiction, they also lack exposure to diverse perspectives. To address this issue, we need to foster spaces for meaningful political dialogue, both in face-to-face settings and moderated online forums. By popularizing meaningful discussions, our society can better resist the spread of disinformation. Furthermore, it's worth examining how Taiwanese people respond to fake news. Current investigations into information manipulation focus on the reach and content of fake news and largely ignore its effectiveness. This raises interesting questions regarding why certain people might encounter fake news without being convinced.

As disinformation continues to tear the fabric of society, we must explore how social cohesion can be strengthened as a countermeasure. Are existing mechanisms,

such as traditional family values, capable of reinforcing such cohesion? Is social trust being undermined by manipulation? If trust between and engagement among individuals remain strong, would disinformation campaigns become less effective? The impact of information manipulation on social cohesion is a critical area for further research, especially the role cohesive mechanisms might play in resisting manipulation and division.

Nevertheless, there are good reasons for hope. Taiwanese people tend to avoid discussing politics with strangers and can maintain intimate relationships despite differences in political opinions. This suggests that there are underlying common values and concerns that transcend political cleavages. This highlights the core value of a democratic society: recognizing shared values while respecting diverse perspectives.

Media Literacy

The 2023 "White Paper on Media Literacy Education in the Digital Age" aims to cultivate "informed, responsible, and altruistic" digital citizens.[159] However, the ongoing efforts are still deficient in several areas:

1. **Limited Outreach of Lifelong Learning Programs:** Lifelong learning programs often fail to reach a majority of those who struggle to identify and respond to rapidly evolving disinformation.
2. **Inadequate Response to Online Media:** Government agencies have not outlined their philosophy on regulations of emerging media platforms, such as TikTok and YouTube. Education policies have inadequately addressed the rising influence of online media on today's youths.
3. **Insufficient Inter-Agency Coordination:** Government agencies have not effectively coordinated their efforts in media literacy education. Efforts targeting marginalized groups such as new immigrants and migrant workers have not been holistically planned.
4. **Regional Disparities and Inadequate Teacher Training:** Media literacy education varies across different regions of Taiwan. Teachers often lack the necessary training and resources to effectively deliver relevant messages to students.
5. **Lack of Fundamental Solutions:** The White Paper fails to address fundamental issues such as resource allocation, regulatory frameworks, and performance evaluation.

While the 108 Curriculum has attempted to improve the students' media literacy, its supposed effectiveness often fails to transliterate from the bureaucracy to the classrooms. The burden of teaching media literacy is often placed on individual teachers, who may struggle to find suitable teaching materials and methods. Organizations like Pang-phuann and FakeNewsCleaner have recognized this challenge and have been providing workshops and support to teachers. However, a more comprehensive and sustainable support system is needed.

Universities and the National Science and Technology Council can also play a significant role in promoting media literacy. Universities with relevant expertise can collaborate with local schools to develop innovative and engaging media literacy programs. These programs can foster cross-generational, interdisciplinary learning and create supportive communities.

Of course, we must improve the media literacy of not just those still in school. Several Taiwanese NGOs have developed tools to help the public analyze information critically and strengthen media literacy, such as AI Labs' Miin platform, IORG's A Guide to Information Literacy and its weekly reports, and DTL's periodic publications. These resources are designed to keep the public informed about emerging trends in information manipulation and to foster awareness and resilience.

However, there are relatively few organizations dedicated to engaging the broader public in this effort. A leader of such efforts is FNC, which has created chat groups for its workshop participants, giving them a safe space for consultation and mutual support, building trust within these communities. However, it recognizes that many remain unreached, highlighting the need to expand outreach efforts further. As disinformation and information manipulation—accelerated by generative AI—further polarize and divide society, the trust cultivated within these groups could become a key defense against the spread of disinformation and manipulation.

Platform Self-Regulation

Organizations such as TFC, DTL, IORG, and AI Labs observe that platforms' responses to disinformation remain largely superficial, focusing on public relations and reputation management rather than substantive action. They contend that platforms have the capability to do much more. For example, TFC, AI Labs, and IORG point to the lack of transparency surrounding platform algorithms, account deletion standards, operational mechanisms, and appeals processes, which has undermined public trust in platforms' self-regulation efforts.

As a result, MyGoPen, TFC, DTL, AI Labs, and IORG advocate for the reintroduction of the Digital Intermediary Act to enforce accountability on platforms. AI Labs further stated that many hacked accounts are exploited to spread disinformation, urging the government to proactively investigate these cases, address cybersecurity vulnerabilities, and hold the responsible parties accountable.

In June 2019, the Taipei Computer Association, in partnership with five domestic and international online platforms and advertisers—including Google, Facebook, LINE, Yahoo, and PTT—introduced the "Code of Practice on Self-Regulation for Combating Disinformation." This initiative aimed to address disinformation on their platforms through voluntary measures. However, the NGO representatives interviewed for this report revealed that many organizations, including MyGoPen, TFC, DTL, and IORG, were unfamiliar with the code, indicating its limited reach and effectiveness.

30. Policy Recommendations

Taiwan's government, digital platforms, and nongovernmental organizations have each introduced measures to address information manipulation, creating a broad defense system. However, these organic efforts, largely driven by the looming threat of Chinese military aggression and fears over the erosion of Taiwan's democracy, lack systematic planning and coordination. They are neither comprehensive nor fully optimized, leaving room for improvement. The following

section contains policy recommendations to strengthen existing efforts against information manipulation.

Continuing Public-Private Cooperation

Given the ever-evolving nature of information manipulation, the government should foster ongoing dialogue between its agencies, civil society, and digital platforms. By regularly assessing the latest trends, these organizations can develop more effective strategies to combat disinformation.

Our recommendations correspond to the following DISARM Blue Counters:

- C00161: Coalition building with stakeholders and third-party indecements
- C00176: Improve coordination amongst stakeholders: public and private
- C00190: Open engagement with civil society
- C00205: Strong dialogue between the [central] government and private sector to encourage better reporting

Exposing Foreign Manipulation Campaigns

Many of the most active agents manipulating information for the Taiwanese audience are abroad. These agents, abusing Taiwan's freedom of speech, are polluting Taiwanese people's views and understandings of Taiwan's freedom and democracy. While it may not be necessary for the government to hunt these individuals down, it should publicize the actions of these individuals, bringing their gray area maneuvers under the sunlight, raising public awareness of foreign disinformation campaigns, and building a public consensus for further regulations.

Our recommendations correspond to the following DISARM Blue Counters:

- C00081: Highlight flooding and noise, and explain motivations
- C00113: Debunk and defuse a fake expert / credentials
- C00115: Expose actor and intentions
- C00184: Media exposure
- C00203: Stop offering press credentials to propaganda outlets

Building a Real-Time Government Response System

While the government has taken steps to strengthen regulations addressing disinformation, a comprehensive and coordinated system is still lacking. It remains unclear whether the Cognitive Warfare Research Center (a subsidiary of the Ministry of Justice Investigation Bureau) has the authority to coordinate the different government agencies to initiate a forceful and timely response. Therefore, a government-wide command system should be established such that when a potentially dishonest message gets reported, the commander can coordinate relevant agencies to discern the truthfulness of the message, issue timely clarifications, and take legal actions against the perpetrators.

Our recommendations correspond to the following DISARM Blue Counters:

- C00030: Develop a compelling counter narrative (truth based)
- C00080: Create competing narrative
- C00126: Social media amber alert
- C00156: Better tell your country or organization story

- C00159: Have a disinformation response plan
- C00220: Develop a monitoring and intelligence plan

Investing in the Public Media

The government could play a significant role in improving the quality of the media outlets, as having high-quality media outlets—ones that deliver articulated facts and ideas on events and issues, as opposed to ones that only parrot partisan opinions—is crucial for a well-functioning democracy. While the government should not over-regulate private media, it could invest in public media outlets, creating something comparable to the BBC or NHK, thereby pressuring private outlets to improve their quality.

Our recommendations correspond to the following DISARM Blue Counters:

- C00024: Promote healthy narratives
- C00030: Develop a compelling counter narrative [truth based]
- C00073: Inoculate populations through media literacy training
- C00080: Create competing narrative
- C00156: Better tell your country or organization story
- C00174: Create a healthier news environment
- C00188: Newsroom/Journalist training to counter influence moves

Expanding Media Literacy Using Digital Platforms

While Taiwan has made strides in promoting media literacy in schools, there is a need to reach a wider audience; existing measures could only reach the student population. The government should partner with online platforms to offer free, accessible media literacy courses, the feasibility of which is affirmed by the success of then Vice President Chen's "National Epidemic Prevention Knowledge (全民防疫通識課：陳建仁副總統來開講)"[160] course during the pandemic. These courses should teach people how to verify information and introduce them to basic open-source intelligence (OSINT) techniques. By empowering individuals to critically evaluate information, we can better protect our society against the spread of disinformation.

Our recommendations correspond to the following DISARM Blue Counters:

- C00011: Media literacy. Games to identify fake news
- C00051: Counter social engineering training
- C00073: Inoculate populations through media literacy training
- C00125: Prebunking
- C00160: Find and train influencers

Creating a Platform for Information Manipulation Research

While many NGOs are researching information manipulation, their findings have not been effectively synthesized. An OpenCTI server to pool different organizations' findings is a good start. The government should fund conferences and workshops for researchers to share localized experiences and learn from experts around the world. This will not only strengthen Taiwan's capabilities in combating disinformation but also foster international cooperation.

Our recommendations correspond to the following DISARM Blue Counters:

- C00008: Create shared fact-checking database
- C00014: Real-time updates to fact-checking database
- C00113: Debunk and defuse a fake expert / credentials.
- C00115: Expose actor and intentions
- C00126: Social media amber alert
- C00159: Have a disinformation response plan
- C00161: Coalition building with stakeholders and third-party inducements
- C00190: Open engagement with civil society

A Legal Framework for Government-Platform Interactions

There is an absence of clear legal guidelines on the conduct between digital platforms and the government. This can lead to needless legal disputes when addressing issues such as information manipulation. Thus, we need a legal framework to define the communication channels, procedures, and scopes of cooperation between specific government agencies and platform operators, allowing for more authoritative and less chaotic responses to emerging threats.

Our recommendations correspond to the following DISARM Blue Counters:

- C00012: Platform regulation
- C00034: Create more friction at account creation
- C00070: Block access to disinformation resources
- C00117: Downgrade / de-amplify so message is seen by fewer people
- C00120: Open dialogue about design of platforms to produce different outcomes
- C00121: Tool transparency and literacy for channels people follow
- C00142: Platform adds warning label and decision point when sharing content
- C00161: Coalition building with stakeholders and third-party inducements
- C00172: Social media source removal
- C00189: Ensure that platforms are taking down flagged accounts
- C00190: Open engagement with civil society
- C00205: Strong dialogue between the [central] government and private sector to encourage better reporting

Requiring Platforms to Label AI-Generated Content

Platforms like Google and Meta should be required to enable users to flag their own content as AI-generated and to create mechanisms to suppress inappropriate AI-generated content (such as deepfake pornography). Clear legal guidelines for AI-content labelling should be introduced to prevent disputes between platforms and users.

Our recommendations correspond to the following DISARM Blue Counters:

- C00012: Platform regulation
- C00142: Platform adds warning label and decision point when sharing content
- C00219: Add metadata to content that's out of the control of disinformation creators

Enhancing Platform Accountability

Platform operators have been using advanced algorithms to feed specific material to users,

often to increase engagement. However, this practice often unintentionally intensifies targeted disinformation or scams made by malicious abusers of the advertisement system. Thus, the government should hold platforms responsible for cracking down on fraudulent activities, bot accounts, and brigading campaigns. Moreover, the government should require platforms to enhance privacy protections and establish transparent channels for user complaints.

In March 2024, the International Foundation for Electoral Systems established guidelines which provide a framework for cooperation between governments and platforms, outlining how platforms can support fair elections. By adopting these guidelines, platforms can play a more constructive role in securing the democratic process in Taiwan.

Our recommendations correspond to the following DISARM Blue Counters:

- **External Regulations:**
  - C00010: Enhanced privacy regulation for social media
  - C00012: Platform regulation
  - C00189: Ensure that platforms are taking down flagged accounts
  - C00205: Strong dialogue between the [central] government and private sector to encourage better reporting

- **Platform Self-discipline:**
  - C00034: Create more friction at account creation
  - C00070: Block access to disinformation resources
  - C00071: Block source of pollution
  - C00078: Change search algorithms for disinformation content
  - C00085: Mute content
  - C00093: Influencer code of conduct
  - C00107: Content moderation
  - C00117: Downgrade / de-amplify so message is seen by fewer people
  - C00120: Open dialogue about design of platforms to produce different outcomes
  - C00121: Tool transparency and literacy for channels people follow
  - C00172: Social media source removal
  - C00195: Redirect searches away from disinformation or extremist content
  - C00197: Remove suspicious accounts
  - C00223: Strengthen trust in social media platforms

Developing an Evaluation Mechanism

While Taiwan has made non-trivial efforts in addressing information manipulation, it is unclear how such efforts could be quantified or evaluated. There should be a comprehensive mechanism, likely using long-running questionnaires and interviews, to assess the success of the different approaches against information manipulation. Future development of such approaches should be guided by these evaluations. It should also be noted that no mechanism is perfect; the approaches should be developed to address societal issues, not to score the highest on the evaluations.

Our recommendations correspond to the following DISARM Blue Counters:

- C00013: Rating framework for news
- C00159: Have a disinformation response plan
- C00212: Build public resilience by making civil society more vibrant

31. The Path Ahead

With all that being said, false and manipulated information is just the symptom of a more serious disease: the erosion of trust in modern civil society. Would disinformation campaigns be as rampant if there were greater trust between individuals? Would information manipulation be as effective after we amended the cleavages in our society? Would having more solidary communities moderate the politicization of the bread and butter issues? Further research should be conducted to facilitate our understanding of information manipulation's impact on democracy and society.

References

1. Zhang, A. (January 18, 2024). "As Taiwan Voted, Beijing Spammed AI Avatars, Faked Paternity Tests and 'Leaked' Documents." ASPI. https://www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-fakedpaternitytests-and-leaked-fake-documents (accessed January 2, 2025).
2. Hung, C., Fu, W., Liu, C., & Tsai, H. (April 12, 2024). "AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election." Taiwan Communication Association. https://www.thomsonfoundation.org/latest/ai-and-disinformation-in-taiwan-s-2024-election/ (accessed January 2, 2025)
3. 乾隆來，(November 7, 2018)，〈不是台灣獨有 大選假新聞成全球流行病〉，今周刊，https://www.businesstoday.com.tw/article/category/80398/post/201811070021/ (accessed January 2, 2025).
4. 陳鈺馥，(December 10, 2018)，〈嚴懲假訊息 國安法列第二波修法〉，自由時報，https://news.ltn.com.tw/news/politics/paper/1252931 (accessed January 2, 2025).
5. 行政院，(December 13, 2018)，〈防制假訊息危害因應作為〉，行政院，https://www.ey.gov.tw/Page/448DE008087A1971/c38a3843-aaf7-45dd-aa4a-91f913c91559 (accessed January 2, 2025).
6. Id.
7. 行政院，(December 20, 2019)，〈2019防制假訊息政策簡介〉，行政院，https://www.ey.gov.tw/Page/5B2FC62D288F4DB7/58fc25c7-125f-4631-8314-73b82c8c62b7 (accessed January 2, 2025).
8. Id.
9. Id.
10. Id.
11. Id.
12. 法務部，(June 6, 2023)，〈總統副總統選舉罷免法〉，全國法規資料庫，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=D0020053 (accessed January 2, 2025).
13. 法務部，(May 26, 2021)，〈社會秩序維護法〉，全國法規資料庫，https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=D0080067 (accessed January 2, 2025).
14. 法務部，(June 9, 2023)，〈公職人員選舉罷免法〉，全國法規資料庫，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=D0020010 (accessed January 2, 2025).
15. Includes Mainland China, Hong Kong, and Macau.
16. Légifrance. (December 23, 2018). France's LOI n° 2018-1202 Du 22 Décembre 2018 Relative à La Lutte Contre la Manipulation de l'Information. Légifrance. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559 (accessed January 2, 2025).
17. 民事廳，(May 17, 2019)，〈不實選罷廣告之刊播限制，不宜由法院擔任第一線審核機關新聞稿〉，司法院，https://jirs.judicial.gov.tw/GNNWS/NNWSS002.asp?id=459197 (accessed January 2, 2025).
18. 國家通訊傳播委員會，(June 29, 2022)，〈數位中介服務法草案總說明〉，國家通訊傳播委員會，https://www.ncc.gov.tw/chinese/files/22081/5542_47882_220811_1.pdf (accessed January 2, 2025).
19. Id.
20. 周冠汝，(August 29, 2022)，〈數位中介服務法草案主要優缺點，你看懂了嗎？〉，台灣人權促進會網站，https://www.tahr.org.tw/news/3235 (accessed January 2, 2025).
21. 陳俐蓉，(November 4, 2023)，〈數位中介服務法草案爭議問題〉，台灣人工智慧行動網，https://ai.iias.sinica.edu.tw/controversial-draft-digital-intermediary-service-act (accessed January 2, 2025).

22. 菱傳媒，(October 7, 2022)，〈數位中介法民調／57.1%不支持　6成不同意NCC另設專責機構〉，菱傳媒，https://rwnews.tw/article.php?news=4988 (accessed January 2, 2025).
23. 陳煜，(August 23, 2022)，〈《中介法》正式出局了！蘇貞昌認了「沒共識」：不會支持繼續推動〉風傳媒，https://www.storm.mg/article/4485072 (accessed January 2, 2025).；陳昀，(August 24, 2022)，〈首度回應數位中介法 蔡英文：歸零思考、加強溝通〉，自由時報網站，https://news.ltn.com.tw/news/politics/breakingnews/4035788 (accessed January 2, 2025).
24. 行政院，supra note 7.
25. 國家發展委員會，(June 2021)，〈數位時代政府政策溝通與危機溝通作業參考手冊〉，國家發展委員會，https://www.ndc.gov.tw/nc_708_35589 (accessed January 2, 2025).
26. 「LINE訊息查證」平台上線 邀全民齊力抗假 同步舉辦媒體識讀教育 由內而外啟發新思維. (July 22, 2019). LINE. https://linecorp.com/tw/pr/news/tw/2019/2791 (accessed January 2, 2025).
27. 台北市電腦公會，(June 21, 2019)，〈自律先行 本會與四大平台業者攜手防制不實訊息〉，台北市電腦公會，https://www.tca.org.tw/tca_news1.php?n=1411 (accessed January 2, 2025).
28. Id.
29. 張家瑜、陳柏樺，(September 26, 2022)，〈不實訊息引發國安危機？羅秉成：若未努力提高警覺，假訊息將隨時反撲，吃掉我們的國家與民主制度〉，台灣事實查核中心，https://tfc-taiwan.org.tw/articles/8213 (accessed January 2, 2025).
30. 行政院，supra note 7.
31. Id.
32. 國家通訊傳播委員會，(May 10, 2024)，〈受理「廣播電視假訊息」申訴案件作業流程圖〉，國家通訊傳播委員會，https://www.ncc.gov.tw/chinese/files/21091/5448_46589_210910_1.png (accessed January 2, 2025).
33. 國家通訊傳播委員會，(May 10, 2024)，〈受理「網路假訊息」申訴案件作業流程圖〉，國家通訊傳播委員會，https://www.ncc.gov.tw/chinese/files/21091/5448_46591_210910_1.png (accessed January 2, 2025).
34. 國家通訊傳播委員會，(February 14, 2024)，〈推動媒體素養課程，強化廣電業者及社會大眾媒體素養〉，國家通訊傳播委員會，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&is_history=0&pages=0&sn_f=49865 (accessed January 2, 2025).
35. Please see 國家通訊傳播委員會，(May 10, 2024)，〈媒體素養教材 ──以年度分類〉，國家通訊傳播委員會，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=5045&sn_f=49537 (accessed January 2, 2025).
36. 國家通訊傳播委員會，supra note 34.
37. 國家通訊傳播委員會，(July 17, 2024)，〈網際網路傳播政策白皮書專區〉，國家通訊傳播委員會，https://www.ncc.gov.tw/chinese/news.aspx?site_content_sn=5705 (accessed January 2, 2025).
38. 終身教育司，(March 30, 2023)，〈面向未來關鍵能力，深化媒體素養教育—教育部發布數位時代媒體素養教育白皮書〉，教育部，https://depart.moe.edu.tw/ed2400/News_Content.aspx?n=15388506A60ACB81&sms=87137EA6056ADFD1&s=D8DDE34F0A469662 (accessed January 2, 2025).
39. Community colleges and universities refer to educational facilities for local residents, not American post-secondary institutions.
40. 終身教育司，(April 25, 2019)，〈學習N次方 跨域豐世代 108年度教育基金會終身學習圈啟動記者會〉，教育部，https://depart.moe.edu.tw/ed2400/News_Content.aspx?n=15388506A60ACB81&sms=87137EA6056ADFD1&s=FD3F3411073814CB (accessed January 2, 2025).
41. 數位發展部，(September 16, 2024)，〈施政說明〉，數位發展部， https://moda.gov.tw/major-policies/policy-elucidation/1305 (accessed January 2, 2025).

42. 徐子苓，(October 20, 2023)，〈數位部出招打假訊息 唐鳳：讓偽冒網站斷開連結〉，自由時報，https://news.ltn.com.tw/news/politics/breakingnews/4464120 (accessed January 2, 2025).；自由追新聞，(October 20, 2023)，〈台版「星鏈計畫」？阻戰時通訊中斷！數位部到底在做什麼？TikTok入侵選戰怎還擊？！唐鳳直球回應｜【官我什麼事】〉，YouTube，https://www.youtube.com/watch?v=RV0cBY7Jo7E (accessed January 2, 2025).

43. 潘姿羽，(February 17, 2024)，〈遭批打假訊息不力 數位部：積極督導資安院加碼防詐〉，中央通訊社，https://www.cna.com.tw/news/aipl/202402170098.aspx (accessed January 2, 2025).

44. 芮家楨，(October 2023)，〈數位發展部主管113年度單位預算評估報告〉，立法院全球資訊網，https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=46546&pid=233945；曹悅華，(February 17, 2024)，〈數位部砸3億推智慧防詐 四面向策略曝光〉，工商時報，https://www.ctee.com.tw/news/20240217700629-430104 (accessed January 2, 2025).

45. 蘇思云，(April 13, 2024)，〈數位部鎖定4大技術驗證 打造數位信任生態系〉，經濟日報，https://money.udn.com/money/story/5612/7896142 (accessed January 2, 2025).

46. 劉世怡，(August 16, 2019)，〈調查局成立假訊息防制中心 執行溯源偵辦〉，中央社，https://www.cna.com.tw/news/asoc/201908160202.aspx (accessed January 2, 2025).

47. 蘇仲泓，(April 24, 2020)，〈調查局「資安工作站」揭牌　蔡英文：查緝網路犯罪就是維護台灣民主自由〉，風傳媒，https://www.storm.mg/article/2560013 (accessed January 2, 2025).

48. Id.

49. 法務部調查局，(January 18, 2024)，〈調查局「認知戰研究中心」揭牌 整合多元能量 齊力反制認知作戰〉，法務部調查局，https://www.mjib.gov.tw/news/Details/1/964 (accessed January 2, 2025).

50. 陳佳鑫、彭耀祖，(October 22, 2019)，〈網路影片散播假訊息 中國官媒記者主持〉，公視新聞網，https://news.pts.org.tw/article/451454 (accessed January 2, 2025); 歐陽夢萍，(April 8, 2020)，〈調查局成立資安工作站 偵辦假訊息、電腦犯罪案件〉，中央廣播電台，https://www.rti.org.tw/news/view/id/2058901 (accessed January 2, 2025).

51. Ching-Ching Chang. (2023). The 2022 Taiwan Communication Survey (Phase Three, Year One): Communication and Civil Society — Citizen and Political Communication (D00240_1) [data file]. Available from Survey Research Data Archive, Academia Sinica. https://doi.org/10.6141/TW-SRDA-D00240_1-1 (accessed January 2, 2025).

52. Kemp, Simon. (February 23, 2024). Digital 2024: Taiwan. DataReportal. https://datareportal.com/reports/digital-2024-taiwan (accessed January 2, 2025).

53. 林芷圓，(May 31, 2023)，〈投資詐騙太狂妄，臉書跟LINE做了什麼？一張圖看懂為何難追查〉，數位時代，https://www.bnext.com.tw/article/75360/financial-fraud-marketing (accessed January 2, 2025).

54. LINE，(April 6, 2022).〈LINE數位當責計畫抗假三年有成首度揭露「影響力報告」〉，LINE新 https://linecorp.com/tw/pr/news/tw/2022/4188 (accessed January 2, 2025).

55. 張乃宣，(December 15, 2023)，〈轉傳假訊息恐觸法 中選會籲加入LINE訊息查證工具〉，華視新聞，https://news.cts.com.tw/cts/general/202312/202312152264227.html (accessed January 2, 2025).

56. 劉致昕，(January 6, 2020)，〈專訪前『劍橋分析』業務總監：只要臉書的生意繼續，民主就有危機〉，報導者，https://www.twreporter.org/a/information-warfare-business-interview-cambridge-analytica-brittany-kaiser (accessed January 2, 2025).

57. Meta. Transparency Center. Meta. Retrieved August 1, 2024, from https://transparency.meta.com/en-us/policies/community-standards/misinformation (accessed January 2, 2025).

58. Meta. (May 10, 2024). Content ratings fact-checkers use. https://transparency.fb.com/en-gb/features/content-ratings-fact-checkers-use (accessed January 2, 2025).

59. Meta. (November 12, 2024). Penalties for sharing fact-checked content. https://transparency.fb.com/en-gb/enforcement/taking-action/penalties-for-sharing-fact-checked-content (accessed January 2, 2025).
60. Meta，〈Instagram如何處理不實資訊〉，Facebook，Retrieved August 1, 2024, from https://zh-tw.facebook.com/help/instagram/2109682462659451 (accessed January 2, 2025).
61. OCF Lab，(August 12, 2020)，〈數位公民雙週報：通訊軟體假消息流竄，WhatsApp曝最新防堵機制〉，https://lab.ocf.tw/2020/08/12/【數位公民雙週報】通訊軟體假消息流竄，-whatsapp-曝最 (accessed January 2, 2025).
62. WhatsApp. IFCN fact-checking organizations on WhatsApp. Retrieved August 1, 2024, from https://faq.whatsapp.com/5059120540855664?helpref=faq_content&cms_id=5059120540855664&draft=false (accessed January 2, 2025).
63. 陳幼臻，(April 2, 2024)，〈2024年國際事實查核日－在台灣打擊不實資訊的四種作法〉，Google台灣官方部落格，https://taiwan.googleblog.com/2024/04/international-fact-checking-day.html (accessed January 2, 2025).
64. 吳家豪，(April 2, 2024)，〈媒體識讀9／國際事實查核日Google在台4招打擊不實資訊〉，中央社，https://www.cna.com.tw/news/ahel/202404020066.aspx (accessed January 2, 2025).
65. 王薇、陳柏樺，(November 23, 2022)，〈選戰期間Google如何防止虛假訊息破壞選舉公平？高瑋均：4R原則減少使用者接觸低品質訊息並兼顧言論自由〉，台灣事實查核中心，https://tfc-taiwan.org.tw/articles/8472 (accessed January 2, 2025).
66. Google. Google Transparency Report. Google. Retrieved August 1, 2024, from https://transparencyreport.google.com/?hl=en (accessed January 2, 2025).
67. 抖音，(August 22, 2024)，〈“抖音”用户服务协议〉，抖音，https://www.douyin.com/draft/douyin_agreement/douyin_agreement_user.html (accessed January 2, 2025).
68. TikTok. (April 17, 2024). Community Guidelines. TikTok. Retrieved August 1, 2024, from https://www.tiktok.com/community-guidelines/en/ (accessed January 2, 2025).
69. TikTok. (December 18, 2024). Community Guidelines Enforcement Report. TikTok Transparency Center. Retrieved December 25, 2024, from https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2024-3 (accessed January 2, 2025).
70. Safety Partners. (November 8, 2024). TikTok. https://www.tiktok.com/safety/en/safety-partners (accessed January 2, 2025).
71. TikTok，(December 24, 2023)，〈TikTok 攜手 MyGoPen 推出《2024 年選舉指南》〉，TikTok，https://newsroom.tiktok.com/zh-tw/tw-election-hub (accessed January 2, 2025).
72. TikTok，(December 1, 2023)，〈TikTok 與台灣事實查核中心、兒福聯盟齊推 #TikTok安全大揭秘 提升數位素養更有力！〉，TikTok，https://newsroom.tiktok.com/zh-tw/digital-literacy-campaign-2023 (accessed January 2, 2025).
73. 溫于德，(January 5, 2021)，〈盜IP貼文恐嚇血染跨年夜 宅男家屬無法辦保先收押〉，自由時報，https://news.ltn.com.tw/news/society/breakingnews/3401263 (accessed January 2, 2025).
74. MyGoPen，(April 2, 2024)，〈第四屆「謠言惑眾獎」開跑！〉，Dcard，https://www.dcard.tw/f/persona_mygopen/p/255148953 (accessed January 2, 2025).
75. 陳彥宇，(August 19, 2022)，〈現行法令已能「打假」設專責機構不如委託民間NCC推《數位中介服務法》難有實質效益〉，今周刊，https://www.businesstoday.com.tw/article/category/183027/post/202207130023 (accessed January 2, 2025).
76. LINE，〈訊息查證介面〉，LINE，Retrieved August 1, 2024, from https://fact-checker.line.me (accessed January 2, 2025).
77. LINE has released an evaluation report on the outcome of its anti-disinformation efforts in 2022, as well as an educational page on information verification. LINE，(2022)，〈LINE數位當責計畫影響力報告〉，LINE，https://line-tw-official.weblog.to/archives/cat_223326.html (accessed January 2, 2025).

78. Meta Transparency Center. (April 2, 2024). How Fact-Checking Works. https://transparency.fb.com/en-gb/features/how-fact-checking-works (accessed January 2, 2025).
79. Meta Transparency Center. Community Standards Enforcement Report. Meta. Retrieved August 1, 2024, from https://transparency.meta.com/reports/community-standards-enforcement (accessed January 2, 2025).
80. WhatsApp. How to Prevent the Spread of Misinformation. WhatsApp. Retrieved August 1, 2024, from https://faq.whatsapp.com/431498999157251 (accessed January 2, 2025).
81. WhatsApp has limitations on how much a message can be forwarded, effectively reducing the spread of rumours, fake news, and viruses. WhatsApp. About forwarding limits. WhatsApp. Retrieved August 1, 2024, from https://faq.whatsapp.com/1053543185312573/ (accessed January 2, 2025).
82. WhatsApp has partnered with many international IFCN organizations, but none in Taiwan. WhatsApp., supra note 62.
83. Google. Google Transparency Report. Google. Retrieved August 1, 2024, from https://transparencyreport.google.com/?hl=en (accessed January 2, 2025).
84. Google presents its evaluations of policy enforcements on the same page as its reports on government mandated account removals. Google. Government Requests to Remove Content. Google. Retrieved August 1, 2024, from https://transparencyreport.google.com/government-removals/overview?hl=en (accessed January 2, 2025).
85. Google funds fact-checking organizations and activities in Taiwan. 陳幼臻，(March 31, 2023)，〈歡慶 2023 年國際事實查核日－持續在台灣打擊不實資訊動〉，Google台灣官方部落格，https://taiwan.googleblog.com/2023/03/international-fact-checking-day.html (accessed January 2, 2025).
86. YouTube. Misinformation Policies. YouTube. Retrieved August 1, from https://support.google.com/youtube/answer/10834785?hl=en (accessed January 2, 2025).
87. YouTube. YouTube Community Guidelines Enforcement. Google Transparency Report. Retrieved August 1, from https://support.google.com/youtube/answer/10834785?hl=en (accessed January 2, 2025).
88. YouTube. About the YouTube Priority Flagger Program. YouTube Help. Retrieved August 1, from https://support.google.com/youtube/answer/7554338?hl=en (accessed January 2, 2025).
89. 抖音，(May 31, 2021)，〈“抖音”用户服务协议〉，抖音，https://www.douyin.com/agreements/?id=6763083657356773389 (accessed January 2, 2025).
90. Douyin's user agreement only outlines the punishments for rule violations without presenting a definition of disinformation:「7.1针对您违反本协议或其他服务条款的行为，公司有权独立判断并视情况采取预先警示、拒绝发布、立即停止传输信息、删除内容或评论、短期禁止发布内容或评论、限制帐号部分或者全部功能直至终止提供服务、永久关闭帐号等措施，对于因此而造成您无法正常使用帐号及相关服务、无法正常获取您帐号内资产或其他权益等后果，公司不承担任何责任。公司有权公告处理结果，且有权根据实际情况决定是否恢复相关帐号的使用。对涉嫌违反法律法规、涉嫌违法犯罪的行为，公司将保存有关记录，并有权依法向有关主管部门报告、配合有关主管部门调查、向公安机关报案等。对已删除内容公司有权不予恢复。」. 抖音，(May 31, 2021)，〈“抖音”用户服务协议〉，抖音，supra note 88.
91. TikTok. (April 17, 2024). Integrity and Authenticity. TikTok. Retrieved August 1, from https://www.tiktok.com/community-guidelines/en/integrity-authenticity/?cgversion=2023 (accessed January 2, 2025).
92. TikTok provides a community guidelines enforcement report, which contains content removal statistics organized by topic. TikTok. (March 19, 2024). Community Guidelines Enforcement Report. TikTok Transparency Center. Retrieved August 1, from https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2023-4 (accessed January 2, 2025).

93. TikTok. supra note 69; TikTok, MyGoPen, Taiwan FactCheck Center, and the Child Welfare League Foundation collaborated on the Guide to the 2024 Elections. TikTok，(December 24, 2023)，〈TikTok 攜手 MyGoPen 推出 〈2024 年選舉指南〉〉，TikTok，https://newsroom.tiktok.com/zh-tw/tw-election-hub (accessed January 2, 2025).
94. 批踢踢實業坊，〈使用者條款 2.0.1〉，批踢踢實業坊，Retrieved August 1, 2024，https://www.ptt.cc/index.ua.html (accessed January 3, 2025).
95. Dcard，(June 1, 2023)，〈用戶使用協議〉，Retrieved August 1, 2024，https://www.dcard.tw/terms (accessed January 2, 2025).
96. 巴哈姆特，〈巴哈姆特會員規範 v.20130315〉，巴哈姆特，Retrieved August 1, 2024，https://user.gamer.com.tw/help/detail.php?sn=294 (accessed January 2, 2025)；巴哈姆特，〈巴哈姆特站規〉，巴哈姆特，Retrieved August 1, 2024，https://user.gamer.com.tw/help/rule.php (accessed January 2, 2025)；巴哈姆特，〈巴哈姆特隱私權政策 v.20200703〉，巴哈姆特，Retrieved August 1, 2024，https://user.gamer.com.tw/help/detail.php?sn=144 (accessed January 2, 2025)
97. 台灣放伴教育協會，〈關於放伴〉，台灣放伴教育協會，Retrieved August 1, 2024, from https://pangphuann.tw/about (accessed January 3, 2025).
98. A Guide to Information Literacy. (May 18, 2022). IORG. https://iorg.tw/_en/book (accessed January 2, 2025).
99. 〈【未來大人物放伴專文】首創師生對話工作坊，放伴教育協會：介入第三方角色學生較敢說出真心話，直球對決老師「學習單可以拿掉嗎？」〉，(August 29, 2023)，The News Lens， https://www.thenewslens.com/article/191051 (accessed January 2, 2025).
100. According to a 2016 research by Foa and Mounk, the citizens of wealthy, established democracies become markedly less satisfied with their form of government and surprisingly open to nondemocratic alternatives. In other words, information manipulation could erode the stability of seemingly consolidated democracies by letting the people lose faith in the belief that "democracy is the only game in town." See Foa, R. S., & Mounk, Y. (2016). The danger of deconsolidation: The democratic disconnect. Journal of democracy, 27(3), 5-17; Linz, J. J. (1990). Transitions to democracy. Washington Quarterly, 13(3), 143-164.
101. 假新聞清潔劑，Retrieved August 1, 2024, from https://www.fakenewscleaner.tw (accessed January 2, 2024).
102. 郭琇真，(January 9, 2021)，〈「假新聞清潔劑」教長輩查證偽訊息 逢凶化吉〉，聯合報願景工程，https://visionproject.org.tw/story/5920 (accessed January 3, 2025).
103. Taiwan FactCheck Center. (April 29, 2022). "Taiwan Media Literacy Education Initiatives" Launched with Google's US$1 Million Funding. Taiwan FactCheck Center. https://tfc-taiwan.org.tw/articles/7275 (accessed January 3, 2025).
104. 終身教育司，supra note 38.
105. 財團法人台灣媒體觀察教育基金會，(April 20, 2018)，〈台灣首個事實查核中心成立　重建社會對媒體的信任〉，財團法人台灣媒體觀察教育基金會，https://www.mediawatch.org.tw/news/9752 (accessed January 2, 2024).
106. 台灣媒體觀察教育基金會，(April 23, 2018)，〈台灣事實查核中心募資影片〉，YouTube，https://www.youtube.com/watch?v=n15x4Y1nXGY (accessed January 2, 2024).
107. 財團法人台灣媒體觀察教育基金會，supra note 105.
108. 台灣事實查核中心，〈查核準則〉，台灣事實查核中心，Retrieved August 1, 2024, from https://tfc-taiwan.org.tw/about/principle (accessed January 2, 2024).
109. 〈議題觀察室〉，台灣事實查核中心，https://tfc-taiwan.org.tw/articles/category/22/1217 (accessed January 2, 2024).
110. The survey was conducted in partnership with the College of Social Sciences at National Taiwan University.
111. 洪貞玲、張佑宗、謝吉隆，(August 2023)，《2023假訊息年度大調查》（初版），頁14。Taiwan FactCheck Center，https://drive.google.com/file/d/10RQsn4UwUDtwvp-KAyZWzytQu_SaZH9o/view (accessed January 3, 2025).
112. It is unclear how grassroot civic movements, such as the Taiwanese pro-democracy movements in the 1980s and the American anti-draft movements in the 1960s, which aimed to invoke policy changes (i.e. to invoke top-down changes), are comparable to TFC's media literacy campaign, which does not involve public actors.

113. Taiwan FactCheck Center., supra note 103.
114. 陳洧農，(June 19, 2024)，〈民間團體：防治假訊息的活躍戰力〉，卓越新聞獎基金會，https://feja.org.tw/75979/ (accessed January 3, 2025).
115. 台灣事實查核中心，〈2024總統大選不實訊息〉，台灣事實查核中心，Retrieved August 1, 2024, from https://tfc-taiwan.org.tw/topic/9640 (accessed January 3, 2025).
116. 台灣事實查核中心，〈2024總統大選：辯論會查核〉台灣事實查核中心，Retrieved August 1, 2024, from https://tfc-taiwan.org.tw/topic/10036 (accessed January 3, 2025).
117. 陳璽安，〈【謠言風向球】2024年選務謠言劇本大公開 一起事先掌握謠言套路〉台灣事實查核中心，Retrieved December 12, 2023, from https://tfc-taiwan.org.tw/articles/8349 (accessed January 3, 2025).
118. 台灣事實查核中心，(December 30, 2023)，〈【影音變造】網傳影片「美國聯邦眾議員軍事委員會副主席魏特曼12月29日受訪公開為台灣某黨總統候選人拉票」?〉，台灣事實查核中心，https://tfc-taiwan.org.tw/articles/10066 (accessed January 3, 2025).
119. MyGoPen. Retrieved August 1, 2024, from https://www.mygopen.com/ (accessed January 3, 2025).
120. MyGoPen，〈事實查證｜真實資訊〉，MyGoPen，Retrieved August 1, 2024, from https://www.mygopen.com/p/17-httpsnews.html (accessed January 3, 2025).
121. 台北市電腦公會，supra note 27.
122. Cofacts, Retrieved August 1, 2024, from https://cofacts.tw (accessed January 3, 2025).
123. Mygopen. (December 15, 2023). 【錯誤】習近平對台灣大選指明方向的影片？AI置換嘴型及語音！實為2018年會議畫面. MyGoPen. https://www.mygopen.com/2023/12/xi-deepfake.html
124. Infodemic. Retrieved August 1, 2024, from https://infodemic.cc/zh-hant (accessed January 3, 2025).
125. China Index 2022. Retrieved August 1, 2024, from https://china-index.io/ (accessed January 3, 2025).
126. Doublethink Lab. Escape the Mist: Disinfo Walkthrough. Doublethink Lab. Retrieved August 1, 2024, from https://fight-dis.info/ (accessed January 3, 2025).
127. Doublethink Lab. Doublethink Lab—Global. Medium. Retrieved August 1, 2024, from https://medium.com/doublethinklab (accessed January 3, 2025).
128. It is unclear whether there is a causal relationship between the reluctance of some to use TikTok and the lack of fact-checking efforts on the platform.
129. Doublethink Lab. (April 8, 2024). 2024 Taiwan Election: The Increasing Polarization of Taiwanese Politics — Reinforcement of Conspiracy Narratives and Cognitive Biases. Medium. https://medium.com/doublethinklab/2024-taiwan-election-the-increasing-polarization-of-taiwanese-politics-reinforcement-of-2e0e503d2fe2 (accessed January 3, 2025).
130. IORG. (July 3, 2020). About IORG. IORG. https://iorg.tw/_en/about (accessed January 3, 2025).
131. IORG. (February 28, 2021). Open IORG. IORG. https://iorg.tw/_en/open (accessed January 3, 2025).
132. Please refer to the research by IORG at: https://iorg.tw/_en/r (accessed January 2, 2025).
133. IORG Weekly Reports are available at: https://iorg.tw/da (accessed January 2, 2025).
134. IORG，(April 12, 2024)，〈資訊環境雙週報第 3 期 — 保母虐童、電價調漲〉，IORG，https://iorg.tw/da/73 (accessed January 2, 2025).
135. A Guide to Information Literacy. (May 18, 2022). IORG. https://iorg.tw/_en/book (accessed January 2, 2025).
136. IORG., supra note 130.
137. Yu, C. (August 8, 2023). US Skepticism Narratives and Where They Come From. IORG. https://iorg.tw/_en/a/us-skepticism-238 (accessed January 2, 2025).

138. IORG. (January 19, 2024). 2023 總體研究成果. IORG. https://iorg.tw/r/2023 (accessed January 2, 2025).
139. IORG. (December 26, 2023). Top Taiwanese Commentator Featured in PRC State Media Douyin Videos 2023Q3. IORG. https://iorg.tw/_en/da/57 (accessed January 2, 2025).
140. IORG，(July 19, 2023)，〈3 步驟判讀民調可信度：透明度、研究設計、推論過程〉，IORG，https://iorg.tw/a/opinion-poll-credibility (accessed January 2, 2025).
141. IORG. (February 23, 2023). Reduce Information Manipulation, Improve Public Discourse, Strengthen Democratic Resilience. IORG. https://iorg.tw/_ua/a/policy-action-recom-2023 (accessed January 2, 2025).
142. 吳家豪，(January 20, 2023)，〈假訊息認知作戰氾濫 杜奕瑾：民眾將可利用AI工具判讀【專訪】〉，中央社，https://www.cna.com.tw/news/ait/202301200012.aspx (accessed January 2, 2025).
143. 2024 Taiwan Presidential Election Information Manipulation AI Observation Report. (January 31, 2024). Taiwan AI Labs. https://www.ailabs.tw/uncategorized/2024-taiwan-presidential-election-information-manipulation-ai-observation-report/
144. Terp, S. J., & Breuer, P. (June 06-10, 2022). Disarm: a framework for analysis of disinformation campaigns. [Conference presentation]. 2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA). Salerno, Italy. (pp. 1-8). https://doi.org/10.1109/CogSIMA54611.2022.9830669 (accessed January 3, 2025).
145. DISARM Foundation. (February 17, 2024). DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework. GitHub. https://github.com/DISARMFoundation/DISARMframeworks (accessed May 7, 2024).
146. Disarm. "A Brief History of DISARM". DISARM Foundation. Retrieved August 1, 2025, from https://www.disarm.foundation/brief-history-of-disarm (accessed January 3, 2025).
147. Id.
148. Terp, S. J., & Breuer, P., supra note 144.
149. DISARM Foundation., supra note 145.
150. DISARM Foundation., supra note 145.
151. Credibility Coalition: Misinfosec Working Group. (August 27, 2019). "Building Standards for Misinfosec. Applying Information Security Principles to Misinformation Response." GitHub. https://github.com/DISARMFoundation/DISARMframeworks/blob/main/DISARM_DOCUMENTATION/DISARM_HISTORY/2019-08-27_MisinfosecWG-2019-1.pdf (accessed January 2, 2025).
152. Each step of an attack corresponds to a tactic. To achieve this tactic, various techniques are employed, each consisting of a series of operational procedures.
153. Strategic Communications. (February 7, 2023). "1st EEAS Report on Foreign Information Manipulation and Interference Threats." European External Action. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en (accessed January 2, 2025).
154. Strategic Communications. (January 23, 2024). "2nd EEAS Report on Foreign Information Manipulation and Interference Threats." European External Action. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (accessed January 2, 2025).
155. 陳璽安，supra note 117.
156. Huang, K., Chou, M., Chen, W., & Kuo, K. Y. (October 25, 2024). GenAI and Democracy. DSET. https://dset.tw/en/research/genai-and-democracy/ (accessed January 2, 2025).
157. Tzu-Chieh Hung, Tzu-Wei Hung, How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars, Journal of Global Security Studies, Volume 7, Issue 4, December 2022, ogac016, https://doi.org/10.1093/jogss/ogac016

158. IORG, supra note 141.

159. 終身教育司，supra note 38.

160. 陳建仁，(April 7, 2020)，〈全民防疫通識課：陳建仁副總統來開講〉，Hahow，
https://hahow.in/courses/5e8d70a52aa77e6f34d6fded (accessed January 2, 2025).

Resilience in Truth

Public-Private Collaboration in Taiwan's Response to Disinformation

Kai-Shen Huang, Muyi Chou 2025

Research Institute for **Democracy**, **Society**, and **Emerging Technology**