STRONGER TOGETHER

COALITIONS AS A CATALYST FOR INFORMATION INTEGRITY

// TIM NIVEN

STRONGER TOGETHER
COALITIONS AS A CATALYST FOR INFORMATION INTEGRITY

CONTENTS

NED
NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM
INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

EXECUTIVE SUMMARY

Coalitions that strengthen information integrity are central to countering authoritarian efforts to manipulate the information space. Such coalitions catalyze the work of diverse prodemocracy voices across sectors—including journalists, fact checkers, narrative researchers, and strategic communicators, among others—and offer important advantages, including:

- **Strengthening the Foundation of Monitor-and-Report Strategies:** Coalitions accelerate early detection and exposure of information manipulation, before such efforts generate societal impact.

- **Creating Efficiencies:** Coalitions boost the efficiency of limited resources, reduce overlap in information integrity initiatives, and encourage knowledge-sharing.

- **Enabling Rapid Learning:** Coalitions accelerate learning and drive adaptation to novel techniques of authoritarian information manipulation that harm democracy.

- **Synergizing Diverse Perspectives and Skillsets:** Coalitions help align diverse perspectives and skillsets, while amplifying the complementary roles played by prodemocracy organizations.

- **Elevating Communication Strategies:** Coalitions provide the strategic coordination necessary for communication strategies that break through an increasingly competitive information environment.

Recent developments in Taiwan demonstrate how information integrity coalitions are critical catalysts for securing the integrity of the information space. In Taiwan, one such coalition strengthened societal resilience to information manipulation by the People's Republic of China (PRC). Key characteristics of successful information integrity coalitions include:

- A focus on shared goals and overcoming challenges to collective action.

- Organize organically and draw from bottom-up guidance from civil society.

- Evolve continuously to keep pace with authoritarian learning and new technological capabilities.

- Ensure that coalitions are *remit-bound* and minimize redundancy.

Authoritarian information manipulation is a complex but inherently solvable problem. Those who value democracy must increase their coordination by building information integrity coalitions that show promise for accelerating critical responses.

INTRODUCTION

Authoritarian powers such as Russia, China, and Iran are evolving their efforts to weaken democratic values and undermine democratic practice by exploiting open information environments. **The growing ease and cheapness of executing malign information campaigns** have **increased the speed and scale of anti-democratic messaging**.[1] Yet, there is one noteworthy trend that is helping democracies shift their efforts from a reactive to proactive footing: the development and growth of localized coalitions in support of information integrity.

Such coalitions are increasingly considered crucial by experts around the globe. **Coalitions bring together diverse skillsets to catalyze the work of prodemocracy voices**; they save costs, pool resources, and avoid the duplication of efforts. They can also **facilitate information and data-sharing** while **elevating proactive messaging and helping journalists, fact checkers, narrative researchers, and strategic communicators compete more effectively with better-resourced authoritarians** in an increasingly complex information environment. Doublethink Lab and its partners have seen that building coalitions for information integrity has strengthened societal resilience to authoritarianism in tangible and practical ways in Taiwan. Some of them are highlighted below.

This report explores the evolving nature of the challenge, using a case study of Taiwan's 2024 election information integrity coalition to highlight why such coalitions are a crucial part of a comprehensive response to information manipulation by authoritarians.

> Building coalitions for information integrity has strengthened societal resilience to authoritarianism in tangible and practical ways in Taiwan.

AUTHORITARIAN ADVANTAGES IN THE INFORMATION ENVIRONMENT

Authoritarian powers are adapting constantly to recent developments in the information environment. They are investing in an expanding infrastructure of digital outlets, influencers, personal and platform data, as well as alternative platforms that work together to amplify their preferred narratives and crowd out high-quality information. As such, **prodemocratic voices such as fact checkers, journalists, narrative researchers, and strategic communicators are grappling with the critical challenge of keeping pace with the rate of authoritarian adaptation**.

The actions social media companies have taken to reduce transparency and curtail access to critical platform data have created challenges for those seeking to bolster information integrity. Traditionally, organizations using open source intelligence have relied on platform data to attribute suspected incidents of information manipulation, since platforms have private data—such as users' IP addresses—that can help to identify the origins and tactics of online campaigns. **With the shuttering of Crowdtangle (a Facebook-owned research tool that was formally closed in August 2024), the attribution of information campaigns has become much more difficult**.[2] By removing state media labels, some platforms have increased the reach of accounts operated by authoritarian states.[3] In addition, by firing trust & safety staff en masse, some platforms

have undercut their ability to leverage civil society expertise and input, while simultaneously weakening their support to journalists and civil society organizations that often face smear campaigns by malign actors in response to their work.[4] Moreover, the rise of less transparent social media and messaging tools, such as TikTok and Telegram which have origins in authoritarian countries, further complicates investigations of information manipulation campaigns.

Meanwhile, **advancements in generative artificial intelligence (gen AI) have reduced the cost and increased the velocity of information manipulation** by providing a cheap way to create manipulative content[5] and increase capabilities to micro-target niche audiences with tailored content.[6] They have also facilitated an evolution in tactics that makes attribution to authoritarian powers difficult. For example, researchers are no longer facing waves of bot accounts posting the same copy and paste messages, but rather waves of bots posting tailored messaging under a single strategic narrative.[7] This type of content is inherently more challenging to analyze at scale than content that is simply copy and pasted, and the ability of gen AI-powered bots to adopt personas that evolve over time and engage in non-political discourse results in more realistic fake social media accounts that are harder to detect. Similarly, increasingly realistic deepfakes[8] retain the power to cause significant harm at critical moments—for instance, a deepfake of election officials questioning legitimate results—that could be decisive in inciting partisan violence during a tensely contested election.[9]

In recent years, an online influence-for-hire industry has begun serving commercial, political, and authoritarian state clients.[10] Private firms, PR agencies, and organized crime syndicates are developing cutting-edge techniques of algorithmic manipulation that game systems to boost their topics and hashtags into trending lists, user feeds, and search engines. Influence-for-hire operations add a layer of plausible deniability between their customers and the content produced on their behalf, complicating attribution. Simultaneously, journalists and other traditional gatekeepers of information are losing clout— even as online influencers,[11] who serve niche audiences and may or may not hold and espouse democratic values, have grown in influence.[12]

Authoritarian powers are investing in an expanding infrastructure of digital outlets, influencers, personal and platform data, as well as alternative platforms that work together to amplify their preferred narratives and crowd out high-quality information.

COALITIONS FOR INFORMATION INTEGRITY

Faced with the increasing scale and complexity of authoritarian information manipulation, democracies require greater cooperation at national, regional, and international levels to compete in the information space. This effort entails breaking down silos, reaching beyond the current borders of the community of organizations working toward integrity in the information space, and defining goals clearly and inclusively in ways that can win new allies.

We use the term "coalitions" to refer to this type of cooperation, which is more formal than "collaboration." Whereas collaboration can be opportunistic and fleeting, we need coalitions for information integrity that are informed by a strategic vision and a common purpose in order to build the kinds of **durable mechanisms needed to counter the persistent challenge of information manipulation by authoritarians**.

UNDERSTANDING FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

Early progress has already been made in establishing the foundations of coalitions for information integrity. For example, democratic actors have recognized that it would be difficult to collaborate on the challenge without a shared set of definitions for understanding and addressing the problem. A focus on exposing and debunking false information is too narrow, as authoritarians shift toward content that is unverifiable, such as conspiracy theories. They also frequently present true information taken out of context, which has a greater possibility of gaining traction in a crowded information space. The information integrity community has come to understand that **information manipulation that harms democracy is a challenge that encompasses but goes beyond messages that are untrue, and relies upon deceptive actors and manipulative behaviors.**[13]

Although a number of useful concepts exist, the framework of **Foreign Information Manipulation and Interference (FIMI)** is gaining broad traction.[14] The European External Action Service (EEAS) spearheaded this framework to enable systematic research and operationalize policymaking in a way that protects freedom of expression. In the two years since its formulation, it has already been used by the U.S. and U.K. governments as well as the G7, along with a vast array of civil society organizations.

The EEAS defines FIMI as **a pattern of behavior that can negatively impact democratic values, procedures, and political processes.** The actors include authoritarian states and their proxies as well as ideological allies inside democratic countries. The behaviors are not simply meant to influence but to manipulate—implying a hidden agenda—and conduct such operations in an intentional and coordinated manner. There is no mention of content in the definition, which gives the framework broad societal appeal among groups that have reasonably different views on particular narratives. This understanding can also generate political will by uniting coalitions of actors around a shared rejection of manipulative information campaigns driven by foreign powers that threaten democratic values and institutions.

Our experience has shown that information integrity coalitions offer many advantages, including:

Strengthening the Foundation of Monitor-and-Report

A strategic approach to countering information manipulation must stand on a foundation of "monitor-and-report." Such a practice is the first step toward resilience. By monitoring the information space and reporting the activities of authoritarian powers—to government agencies, journalists, social media platforms, or the public—we build a base for responses such as communications campaigns, disruption actions (such as take-downs of inauthentic social media assets), public attribution to impose reputational costs on malign actors, and the

gradual development of more systematic, evidence-based responses from civil society and key decision makers.[15] **Early detection and exposure are also vital to catching information manipulation before it generates impact** (e.g., by breaking out of echo chambers or by crossing channels, platforms, and the online-offline barrier).[16]

While necessary, this approach is insufficient on its own. According to one member of a Philippine civil society organization, "we have to stop just doing autopsies." In other words, efforts to counter malign actors must go beyond monitoring the information environment and start engaging with the public on key topics relevant to the quality of democracy. Methods such as civil society-led strategic communications play an important role in going beyond monitoring and can drive proactive efforts to counter information manipulation and build democratic values. Such efforts may include raising awareness about Foreign Information Manipulation and Interference (see text box on previous page for more information) sources and techniques as well as pre-bunking, building context and comity around divisive topics, in addition to attempts to strengthen democratic values and resilience. Efforts such as these, which Doublethink Lab has adopted as a strategic framework, represent proactive approaches to building resilience to FIMI and must be based on a foundation of a common understanding of actors, tactics, and narratives. Through common understandings, new forms of collaboration may be forged and existing capabilities broadened.

Information-sharing enhances the benefits of research and monitoring efforts by individual organizations. Across country and regional contexts, it is the same group of actors who are frequently involved in campaigns of information manipulation, and they often use the same playbooks. Those preparing to counter FIMI during elections may find that examining a recent election on the other side of the world can be more useful than the most recent domestic election, as tactics evolve quickly in a fast-moving information environment. By pooling our observations, we can build up rich databases of incidents that can facilitate attribution of newer incidents, as coalitions of journalists, civil society organizations, and democratic governments are already doing in some contexts. We can also achieve higher-level statistical understanding of authoritarian messaging patterns and strategy, **which can help to predict future behavior and prioritize the most effective responses**. Central to such efforts is a common data object model such as DISARM,[17] an open source framework for categorizing, cataloging, and countering malign information campaigns that has been adopted widely across the European Union, United States, and Indo-Pacific.

Creating Efficiencies

Coalitions boost the efficiency of limited resources. In the modern, pay-for-play information environment, having two organizations doing the same work— so-called "strategic overlap"—can be prevented through closer collaboration and the sharing of research agendas. The fight against Russian information

We have to stop just doing "autopsies:" Efforts to counter malign actors must go beyond monitoring the information environment and start engaging with the public on key topics relevant to the quality of democracy.

operations after the full-scale invasion of Ukraine has demonstrated the advantages of such collaboration. **While some overlap is better than leaving gaps, any duplication of efforts must be coordinated rather than incidental**.[18] Similarly, broad information-sharing among like-minded partners for situational awareness creates important efficiencies for fact checkers, journalists, strategic communicators, and others who may not have dedicated resources to understand and respond to every narrative, campaign, or malign actor. Furthermore, civil society activists encounter many of the same opponents and tactics across different country contexts. Consequently, there has been a proliferation of nearly-identical attempts to design tools for collecting and storing social media data for analysis. Particularly in the civil society sector, **spending limited and competitive funding on repetitive initiatives is a recipe for strategic disaster**. Recognizing this reality (and with funding from the European Union), Doublethink Lab has been building a coalition of FIMI experts in the Indo-Pacific region working from a shared, centralized database of FIMI incidents.

Enabling Rapid Learning

As authoritarian information manipulation tactics evolve, democratic researchers and actors must also adapt; coalitions accelerate this type of learning among the democratic community. For example, based on the efforts of a biannual election monitoring coalition, Taiwanese civil society has identified a shift in PRC (People's Republic of China) tactics in the information space.[19] The PRC is currently relying less on initiating information attacks through foreign assets outside Taiwan and more on amplifying stories seeded by local influencers. Therefore, we know that **more resources are required to monitor the influencer propaganda economy**, and that **more cooperation with investigative journalists is necessary to trace offline connections which are increasingly central to the PRC's information operations targeting Taiwan**. Doublethink Lab's experience is that sharing our findings and learning helps inform best practice and contributes to faster solutions.

Synergizing Diverse Perspectives and Skillsets

Coalitions strengthen work across an ecosystem by **synergizing diverse perspectives and skillsets**, allowing **different types of stakeholders to play complementary roles**. The "MacronLeaks" campaign is case-in-point.[20] Based on lessons learned from Russian interference in earlier elections, cybersecurity experts, the French election commission, some political parties, and mainstream media outlets worked in coalition to launch a response to the "MacronLeaks" campaign, stopping its spread across French media and society. The French National Cybersecurity Agency raised awareness among partners of the hack-and-leak attack, which had been observed in previous elections elsewhere around the world. The election commission immediately issued a statement once the leaked documents were published, calling on mainstream

As authoritarian information manipulation tactics evolve, democratic researchers and actors must also adapt.

media to respect the country's blackout period before the election, a directive with which most outlets complied. Finally, Macron's team took proactive steps, such as planting false data in their systems to confuse hackers, making it difficult for these malign actors to discredit him with the stolen documents. His team also responded in a timely manner, communicating that the leaks were fabricated. Others identified Russian characters and obvious forgeries among the data.

Elevating Communication Strategies

Coalitions can provide the strategic coordination necessary for effective public communications. Due to top-down state control, **authoritarians have near-perfect message discipline across multiple actors and channels**. With Russia and the PRC now coordinating messaging more closely, this effect is even stronger.[21] **Prodemocracy actors, on the other hand, need to rely on coalition-building to achieve a similar reach**. In Ukraine, the National Democratic Institute supports a coalition that has helped local journalists, civil society, and strategic communicators collectively amplify debunks of Russian information operations related to the full-scale invasion, blunting their effectiveness. Thus, coalitions are powerful tools for elevating communications and information in an increasingly competitive information space.

TAIWAN'S ELECTION-FOCUSED INFORMATION INTEGRITY COALITION

Six months prior to Taiwan's January 2024 election, Doublethink Lab organized a coalition to counter FIMI. This was the second time such a coalition was formed—the first having been around Taiwan's 2022 local elections. This coalition brought together fact checkers, FIMI investigators, cybersecurity experts, and academics, functioning mainly as an information-sharing mechanism. Doublethink Lab connected insight to action through a line of communication with Meta, which was used for directly submitting suspected platform policy violations for review. This effort led to the takedown of an inauthentic, Cambodia-based network on Facebook that sought to undermine trust in prodemocracy politicians in the run-up to the election.[22]

Of course, some manipulative information campaigns are so expansive that even siloed researchers are likely to see notable commonalities, as was the case with the cross-platform, gen AI-powered campaign falsely accusing former Taiwanese president Tsai Ing-Wen of having a "secret history" of immoral behavior.[23] Due to proactive information-sharing within the coalition, however, at least one covert campaign was identified in which malign actors attempted to exploit cultural tensions and start an astroturf protest targeting Indian migrant workers in Taiwan with polarizing anti-Indian rhetoric.[24] **The coalition was able to catch this campaign before it broke out of echo chambers in either country and quickly spread awareness about it within Taiwan, while a media partner issued a pre-bunk to make the Indian public aware of the campaign.**[25]

The Taiwanese experience suggests that coalitions for information integrity can be powerful tools for countering FIMI when they rest on the following principles.[26] They should focus attention on shared goals to **align diverse partners**, and **overcome challenges to collective action**. They should **organize organically** and rely on **bottom-up guidance from civil society**; doing so **increases credibility and reach**, a factor that is particularly important in the context of increasing political polarization. They should **identify and leverage synergies from diverse perspectives and skillsets** to achieve *whole-of-society* **engagement**. They should also **evolve over time** to keep up with the pace of authoritarian learning. Finally, they should be *remit-bound*, meaning that each member organization focuses on contributing its expertise and minimizing redundancy.

Coalitions that hew to these principles will make far more efficient use of resources and prove more effective in the fight against authoritarian information campaigns.

Principles for Effective Information Integrity Coalitions

WHOLE-OF-SOCIETY
Taiwan's resilience is expressed across a swathe of institutions including universities, civil society organizations, media outlets, and social platforms. Initiative is diffuse rather than concentrated.

PURPOSE-DRIVEN
Strategic discipline among Taiwanese civil society organizations is facilitated not by a single organization or a shared strategic plan, but a clear sense of shared purpose.

EVOLVING
Taiwan's approach is not static, but moves in step with changes in the FIMI threat.

ORGANIC
Taiwan's resilience is primarily driven from the bottom-up. Government plays a role as a funding body and in providing overarching directions regarding the significance and nature of the threat, but action is decentralized.

REMIT-BOUND
Different organizations focus primarily on their own areas of expertise without seeking to duplicate the labors of others, maximizing collective efficiency.

Adapted and reprinted with permission of Doublethink Lab.

Despite massive investment, **the PRC has been unable to sell Taiwan's voters on the "positive" aspects of giving up their democracy and sovereignty, due at least in part to the work of our coalition for information integrity**. Still, polling shows that efforts which amplify polarization within Taiwan's society undermine trust in government and institutions, and sow conspiracy theories that have flourished among a large segment of the voting public.[27]

To better understand how our future individual and coalition efforts must evolve, Doublethink Lab conducted a representative poll in Taiwan in the last week of the election campaign. This poll asked voters if they changed their vote, for whom they were voting, and why they decided to change their vote. The reason most commonly cited by voters who changed their vote and did not vote for the governing party was a **conspiracy theory that government corruption delivered unsafe vaccines to the population**. Similar to many effective FIMI campaigns, this campaign involved a mixture of domestic and foreign efforts, with the PRC playing a significant role in amplifying domestically-seeded stories.[28]

The Taiwanese experience suggests that coalitions for information integrity can be powerful tools for countering FIMI.

PRINCIPLES FOR SUCCESSFUL COALITIONS

The problems Taiwan faces are not unique, with similar stories of decreasing trust, increasing polarization, and democratic backsliding emerging around the world. What can civil society elsewhere learn from Taiwan about how information integrity coalitions help to better confront FIMI? We offer three core principles outlined below that we believe are critical for information integrity to thrive across various contexts.

⊙ Articulate a Long-Term Vision for Information Integrity

Participation in coalitions can be costly. Such an effort often falls outside of remunerated project work and building the necessary political will can be challenging. **It is critical that local civil society takes the lead in articulating a vision of a healthy information environment, or at the very least of an information environment in which citizens are more resilient to FIMI.** Only under such a vision can a shared purpose take hold among diverse prodemocratic organizations—many of whom may be political competitors. The development of such an innovation must include an appropriate range of stakeholders, extending beyond civil society to include locally-relevant combinations of actors from other fields including: academia, the legal community, and democratic governments, among others. Finally, those involved in crafting new coalitions should consider how they might exist beyond a given election cycle.

Bolster Information-Sharing Mechanisms for Monitor-and-Report Efforts
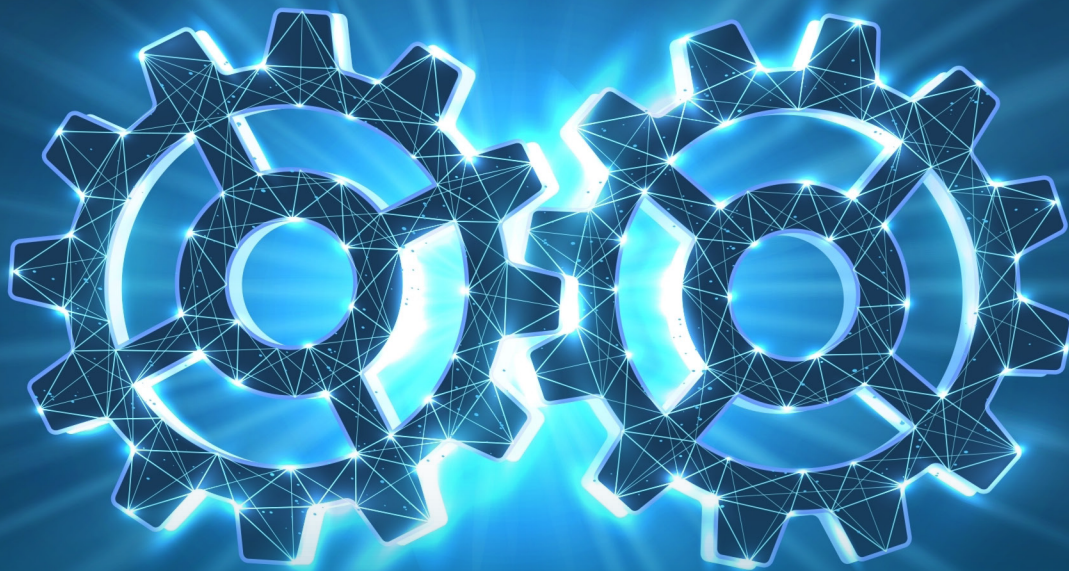
Identifying potential FIMI incidents early is the foundation for timely responses—such as communications campaigns, fact-checks, pre-bunking, or disruptions—and can be achieved by deepening information-sharing mechanisms. A leading example of information-sharing across diverse partners comes from Ukraine, where preparedness, the use of new technologies (including artificial intelligence), and close cooperation among democratic partners have helped in the fight against Russian FIMI about the ongoing full scale-invasion.[29]

There is work to be done in fleshing out exactly how information-sharing mechanisms should work, particularly at the interface between government and civil society. **It is helpful to have a designated organization that is accepted by all participants as an unbiased voice that can manage coordination, facilitate communication, and ensure smooth operations within the coalition**. In Taiwan, it would be helpful to designate such an interlocutor that could then help civil society to aggregate and channel requests and correspondence. The government would then need to deal with only one organization instead of many. From the perspective of civil society organizations, one extra degree of separation between themselves and the government may help to de-fang potential charges of government influence. **Governments committed to democracy may prove powerful allies if engaged in appropriate ways to address information manipulation behaviors** through policy, increasing societal resilience through media literacy programs in education systems and tackling organized criminal groups that engage in information manipulation with greater frequency. As mentioned above, any information-sharing mechanism will need common language and a common data model, such as the OASIS STIX model, which has been borrowed from cybersecurity and is gaining traction in the information integrity community.

Strengthen the Strategic Communications Capacity of Emerging Coalitions

Fact-checks, pre-bunking, and communications need to be **directed at key audiences using effective strategic communications practices that are driven by data and audience understanding**. The findings of Doublethink Lab's election survey in Taiwan suggest we are not reaching key audiences with reliable information about FIMI. A "spray and pray" approach in our communications is inadequate. Simply "putting the facts out there" in our own echo chambers is not a sufficient response. **A more proactive, strategic response requires understanding the vulnerabilities and media consumption habits of crucial audiences**. The precise contours of such coalition-oriented responses is a work in progress, but there are already promising efforts taking shape in places such as in the Philippines and Kenya, where organizations are building networks of like-minded content creators to amplify fact-checks, share high-quality information, and build democratic values.[30]

COLLABORATION TO MEET A NEW MOMENT

Faced with the challenge of coordinated and adaptive authoritarian adversaries in an increasingly complex and fragmented information environment, **those who value democracy must increase their coordination by building information integrity coalitions**. By strengthening the foundations of monitoring and reporting, creating efficiencies and synergies, and increasing our own rate of learning and information-sharing, we can close the gap.

Although many stakeholders agree that coalition-building is desirable, sustained and effective systematic cooperation still faces challenges. We can start by crafting a shared strategic vision in which monitoring and reporting work goes beyond mere "autopsies." **This effort should inform broad civil society-driven information campaigns to reach key audiences proactively, elevate high-quality information, promote democratic values, and encourage action from industry and government**. Information manipulation by authoritarians is a complex but inherently solvable problem. We must roll up our sleeves and get to it, together.

ENDNOTES

1   Beatriz Saab, *Manufacturing Deceit: How Generative AI Supercharges Information Manipulation*, National Endowment for Democracy, June 2024, www.ned.org/manufacturing-deceit-how-generative-ai-supercharges-information-manipulation/.

2   Barbara Ortutay, "Meta Kills off Misinformation Tracking Tool CrowdTangle Despite Pleas from Researchers, Journalists," AP News, 14 August 2024, https://apnews.com/article/meta-crowdtangle-research-misinformation-shutdown-facebook-977ece074b99adddb4887bf719f2112a.

3   McKenzie Sadeghi, Jack Brewster, and Macrina Wang, "X's Unchecked Propaganda: Engagement Soared by 70 Percent for Russian, Chinese, and Iranian Disinformation Sources Following a Change by Elon Musk," NewsGuard, 26 September 2023, www.newsguardtech.com/misinformation-monitor/september-2023/.

4   Ben Goggin, "Big Tech Companies Reveal Trust and Safety Cuts in Disclosures to Senate Judiciary Committee," NBC News, 29 March 2024, www.nbcnews.com/tech/tech-news/big-tech-companies-reveal-trust-safety-cuts-disclosures-senate-judicia-rcna145435.

5   "Artificial Multiverse: Foreign Information Manipulation and Interference in Taiwan's 2024 National Elections," published by Doublethink Lab, Medium, 13 August 2024, https://medium.com/doublethinklab/artificial-multiverse-foreign-information-manipulation-and-interference-in-taiwans-2024-national-f3e22ac95fe7.

6   Gundars Bergmanis-Korāts, Tetiana Haiduchyk, and Artur Shevtsov, "AI in Precision Persuasion. Unveiling Tactics and Risks on Social Media," the NATO Strategic Communications Centre of Excellence (NATO StratCom COE), 20 August 2024, https://stratcomcoe.org/publications/ai-in-precision-persuasion-unveiling-tactics-and-risks-on-social-media/309.

7   "Virtual Manipulation Brief 2024/1: Hijacking reality: the increased role of generative AI in Russian propaganda," NATO StratCom COE, 4 June 2024, https://stratcomcoe.org/publications/virtual-manipulation-brief-20241-hijacking-reality-the-increased-role-of-generative-ai-in-russian-propaganda/307.

8   "Same targets, New Playbooks: East Asia Threat Actors Employ Unique Methods," Microsoft Threat Intelligence, April 2024, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf.

9   Morgan Meaker, "Slovakia's Election Deepfakes Show AI Is a Danger to Democracy," *WIRED*, 3 October 2023, www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/.

10 Gaute Friis et al., "Countering China's Use of Private Firms in Covert Information Operations," Stanford University, Freeman Spogli Institute for International Studies, 21 June 2024, https://stacks.stanford.edu/file/druid:fg865kf5598/countering_prc_use_of_private_firms%20in_IO_gordian_knot_center_ver.pdf.

11 Renée DiResta, "The New Media Goliaths," *Noema,* 1 June 2023, www.noemamag.com/the-new-media-goliaths/.

12 "Artificial Multiverse."

13 Camille François, "Actors, Behavior, Content: A Disinformation ABC," Institut voor Informatierecht, 20 September 2019, www.ivir.nl/publicaties/download/ABC_Framework_2019_Sept_2019.pdf.

14 For more information, please consult the European Union External Action Service (EEAS) webpage the defines FIMI: www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

15 Ben Nimmo and Eric Hutchins, *Phase-Based Tactical Analysis of Online Operations,* Carnegie Endowment for International Peace, 16 March 2023, https://carnegieendowment.org/research/2023/03/phase-based-tactical-analysis-of-online-operations?lang=en.

16 Ben Nimmo, *The Breakout Scale: Measuring the Impact of Influence Operations*, the Brookings Institution, September 2020, www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations/.

17 For more information, please consult DISARM's webpage: https://www.disarm.foundation/framework.

18 Jakub Kalenský and Roman Osadchuk, "How Ukraine Fights Russian Disinformation: Beehive vs Mammoth," the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), January 2024, www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf.

19 Tim Niven, "The Evolution of China's Interference in Taiwan," *the Diplomat*, 1 December 2023, https://thediplomat.com/2023/12/the-evolution-of-chinas-interference-in-taiwan/.

20 Boris Toucas, "The Macron Leaks: The Defeat of Informational Warfare," Center for Strategic and International Studies (CSIS), 30 May 2017, www.csis.org/analysis/macron-leaks-defeat-informational-warfare.

21   Maria Isabel Puerta Riera, "Amplification among Allies: Russian and PRC Information Operations in Latin America," *Power 3.0 blog*, 13 November 2023, www.power3point0.org/2023/11/13/amplification-among-allies-russian-and-prc-information-operations-in-latin-america/.

22   "Close, Imported Products Counterfeiting Local Public Opinion: Analysis of Facebook's Overseas Fans' Methods of Intervening in Taiwan's Election Methods," published by Doublethink Lab, Medium, 11 January 2024, https://medium.com/doublethinklab-tw/%E5%81%87%E5%86%92%E5%9C%A8%E5%9C%B0%E6%B0%91%E6%84%8F%E7%9A%84%E8%88%B6%E4%BE%86%E5%93%81-%E8%87%89%E6%9B%B8%E5%A2%83%E5%A4%96%E7%B2%89%E5%B0%88%E4%BB%8B%E5%85%A5%E5%8F%B0%E7%81%A3%E9%81%B8%E8%88%89%E6%89%8B%E6%B3%95%E8%A7%A3%E6%9E%90-f90176ec14b8. (Original source material in Mandarin Chinese.)

23   Albert Zhang, "As Taiwan Voted, Beijing Spammed AI Avatars, Faked Paternity Tests and 'Leaked' Documents," Australian Strategic Policy Institute (ASPI), 18 January 2024, www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-faked-paternity-tests-and-leaked-fake-documents/.

24   "2024 Taiwan Elections: Foreign Influence Observation—Preliminary Statement," published by Doublethink Lab, Medium, 27 February 2024, https://medium.com/doublethinklab/2024-taiwan-elections-foreign-influence-observation-preliminary-statement-caeeccb5b88e.

25   Dr. Sriparna Pathak, "Opinion: Racism, Disinformation Cast Shadow On India-Taiwan Cooperation," New Dehli Television (NDTV), 16 November 2023, www.ndtv.com/opinion/racism-disinformation-cast-shadow-on-india-taiwan-cooperation-4579209.

26   "Taiwan POWER: A Model for Foreign Information Manipulation & Interference Resilience," published by Doublethink Lab, Medium, 9 August 2024, https://medium.com/doublethinklab/taiwan-power-a-model-for-resilience-to-foreign-information-manipulation-interference-70ea81f859b7.

27   "2024 Taiwan Election: The Increasing Polarization of Taiwanese Politics—Reinforcement of Conspiracy Narratives and Cognitive Biases," published by Doublethink Lab, Medium, 8 April 2024, https://medium.com/doublethinklab/2024-taiwan-election-the-increasing-polarization-of-taiwanese-politics-reinforcement-of-2e0e503d2fe2.

28   Dr. Puma Shen, *New Variants of COVID-19 Disinformation in Taiwan,* National Democratic Institute, May 2022, www.ndi.org/sites/default/files/%28English%29%20NDI%20May%202022%20Report_New%20Variants%20of%20COVID-19%20Disinformation%20in%20Taiwan.pdf.

29   Adam Fivenson et al., *Shielding Democracy: Civil Society Adaptations to Kremlin Disinformation about Ukraine,* National Endowment for Democracy, February 2023, www.ned.org/shielding-democracy-civil-society-adaptations-kremlin-disinformation-ukraine/.

30   Omkar Poojari, "Why Some Indian Journalists Are Trading Newsrooms for YouTube," *the Christian Science Monitor*, 30 May 2024, www.csmonitor.com/World/Asia-South-Central/2024/0530/Why-some-Indian-journalists-are-trading-newsrooms-for-YouTube.

ABOUT THE AUTHOR

Tim Niven is Research Lead at Doublethink Lab, a civil society organization headquartered in Taiwan. His work at Doublethink Lab has been of vital importance to the organization's efforts to work with Taiwan-based and international networks of experts to conduct research into the PRC's malign influence and interference in multiple domains (including the information space) and to develop corresponding policy recommendations to increase democratic resilience. Tim completed an honors degree in philosophy at Victoria University in Wellington, New Zealand, and is undertaking a PhD in computer science at National Cheng Kung University in Tainan, Taiwan.

ACKNOWLEDGMENTS

PHOTO CREDITS

FORUM
INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

The International Forum for Democratic Studies at the National Endowment for Democracy (NED) is a leading center for analysis and discussion of the theory and practice of democracy around the world. The Forum complements NED's core mission—assisting civil society groups abroad in their efforts to foster and strengthen democracy—by linking the academic community with activists from across the globe. Through its multifaceted activities, the Forum responds to challenges facing countries around the world by analyzing opportunities for democratic transition, reform, and consolidation. The Forum pursues its goals through several interrelated initiatives: publishing the *Journal of Democracy*, the world's leading publication on the theory and practice of democracy; hosting fellowship programs for international democracy activists, journalists, and scholars; coordinating a global network of think tanks; and undertaking a diverse range of analytical initiatives to explore critical themes relating to democratic development.

NED
NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

The National Endowment for Democracy (NED) is a private, nonprofit foundation dedicated to the growth and strengthening of democratic institutions around the world. Each year, NED makes more than 1,700 grants to support the projects of nongovernmental groups abroad who are working for democratic goals in more than 90 countries. Since its founding in 1983, the Endowment has remained on the leading edge of democratic struggles everywhere, while evolving into a multifaceted institution that is a hub of activity, resources, and intellectual exchange for activists, practitioners, and scholars of democracy the world over.

1201 Pennsylvania Avenue, NW
Suite 1100
Washington, DC 20004
(202) 378-9700
ned.org

𝕏 **@thinkdemocracy**

f **ThinkDemocracy**

in **International Forum for Democratic Studies**