21. Wahlperiode

Deutscher Bundestag
Ausschuss für Menschenrechte und humanitäre Hilfe

Ausschussdrucksache 21(17)9
vom 10. November 2025

Schriftliche Stellungnahme

Öffentliche Anhörung

„Desinformation durch autokratische Staaten mit dem Ziel der Schwächung von Demokratie und Bedrohung der Menschenrechte“

Dr. Puma Shen
Abgeordneter im taiwanischen Parlament (Yuan) für die Democratic Progressive Party

Disinformation by autocratic states with the aim of weakening democracy and threatening human rights
Digital Autocracy vs. Democratic Resilience

Puma Shen

Legislator, Legislative Yuan, Taiwan

Opening Statement

The debate over the precise definition of "disinformation" is often a conceptual dead end. From a policy and analytical perspective, the real issue is not the maliciousness of a single message, but the **information ecosystem** itself—a structural asymmetry between open and closed societies. The strategic goal of authoritarian states is to penetrate and subvert democratic discourse through systemic interference targeting the foundation of democratic deliberation.

1. The Internal Genesis: "Informational Autocracy"

Modern authoritarian governance, exemplified by figures like Vladimir Putin and Xi Jinping, has shifted from 20th-century fear-based repression to a subtler, yet effective, model termed "**informational autocracy**".[1] These regimes secure domestic legitimacy by manipulating information to lead the public to believe, rationally but incorrectly, that the rulers are competent and public-spirited. This is achieved by employing rhetoric focused on economic performance and public service, mimicking democratic leaders, and using concealed censorship rather than overt oppression. They even strategically mimic democracy by holding elections to create a façade of legitimacy.

2. External Projection and the Dilemma of Asymmetry

This internal strategy for survival serves as a foundational capability for external projection. Authoritarian governments have increasingly expanded their information control to the international arena, engaging in malign foreign influence operations. Data from V-Dem[2] on the "Government dissemination of false information abroad" shows a clear trend: from 2000 to 2024, key authoritarian powers, notably Russia and China, have significantly intensified their external information operations, as indicated by their scores increasingly shifting towards the lower end of the scale (0–1, indicating frequent dissemination).

[1] Sergei Guriev and Daniel Treisman, "Informational Autocrats." *Journal of Economic Perspectives* 33, no. 4 (2019): 100–127.

[2] Michael Coppedge et al., "V-Dem Country-Year Dataset v15" (Varieties of Democracy (V-Dem) Project, 2025). https://doi.org/10.23696/vdemds25

This transnational attack leverages two decisive structural factors that create an **asymmetric dilemma** for democracies. First, authoritarian states possess enormous, virtually unlimited **resources and channels for content amplification**, whereas democratic countries are constrained by costs and democratic checks and balances. For instance, in 2023, Google reported removing, on average, 200 YouTube channels *per day* linked to China. Second, cross-border information operations are not subject to **domestic democratic oversight**, as the governments behind the content are not accountable to the recipient country's democratic institutions. These two factors—unlimited budgets and the absence of democratic constraints—make authoritarian campaigns uniquely powerful and difficult to counter.

Question 1 - Forms, actors and aims of state disinformation

How can disinformation in (social) media be structurally recognised and what structural findings do you have on the systematic manipulation of information by autocratic states?

Answer

1. A Shift in Analytical Focus

The focus must not be limited to the content of messages but should rather be on **how information is disseminated** and the structural role of autocratic regimes in that process. The key to countering these operations is recognizing that the foundation of democracy—freedom of speech, where every individual's voice carries equal weight—is undermined when massive financial resources, especially from authoritarian states, create an unequal speech environment. Therefore, research attention should shift from what is said to whether the **methods** used violate democratic principles.

2. Disinformation Analysis Framework: The 3I Model

To address the evolving threat, a focused analytical framework is crucial for understanding the changing strategies of authoritarian states. I use the **"3I" framework** to illustrate China's specific strategies for spreading online disinformation. This model encompasses Direct Information Manipulation, Indirect Investment, and Ideology-Driven approaches.[3]

- **Direct Information Manipulation (Information Flow)**

  The first strategy used by China is Direct Information Manipulation. This approach involves three different levels of information manipulation, each varying in scale and intensity. At the high level, the Propaganda Department and other committees set key themes that are often observed through state media or officials' Twitter (X) accounts. Low-level information manipulation occurs through trolls and patriots who spread low-end fake news through social media and bot networks. Finally, the most harmful form of direct manipulation is **connected-level** information operations, which involve China-controlled content farms spreading biased reports and conspiracy theories through organic channels.[4]

[3] Puma Shen, "How China Initiates Information Operations Against Taiwan," *Taiwan Strategists*, no. 12 (2021): 20.

[4] Doublethink Lab, "Deafening whispers: China's information operation and Taiwan's 2020 election." (Doublethink Lab, 2020).

China has been successful in utilizing its infrastructure to disseminate content through the 50-cent party and its cyber police.[5] The Communist Youth League is also involved in inciting disinformation campaigns through cross-posting content farm articles on social media.[6] Additionally, China has established content farm channels on YouTube that utilize AI voice generators to read biased articles with traditional Chinese subtitles.[7] Understanding the relationship between the Propaganda Department, trolls, and YouTube channels is essential for combating these attacks.

Studies and digital investigations illuminate the "connected-level" operations of China-based content farms, specifically demonstrating how they gather Taiwanese user data for **microtargeting** efforts to influence democratic elections. Companies in China's Hebei province, for instance, have been found managing Facebook pages and groups, often disguised with seemingly harmless content like psychological quizzes or pornography, to compel users to share their personal information and preferences.[8] This activity essentially creates a database that enables the precise delivery of political disinformation, such as pushing specific candidates, attacking opposition parties, or promoting narratives favoring unification.[9] These methods constitute direct and sustained interference in Taiwan's electoral process.[10]

- **Indirect Investment (Money Flow)**

China's second strategy involves Indirect Investment, which entails providing financial backing to groups that can generate and disseminate disinformation. This approach includes investing in Taiwanese marketing companies, exerting economic pressure on influencers, and enticing live streamers to join the propaganda network via online donations. By separating the creation and distribution processes in this strategy, China can invest more covertly and indirectly, making it more challenging to detect their influence. This allows them to avoid direct confrontations and, instead, manipulate public opinion by spreading false information through trusted channels and influential figures. The case of one of Taiwan's most-subscribed influencers, serves as a potent example: he revealed in 2019 that he firmly rejected a multi-million NTD offer to whitewash the CCP, but his stance gradually eroded over the next six years. By 2025, the former high-

[5] Puma Shen, “The Chinese Cognitive Warfare Model: The 2020 Taiwan Election” [中國認知領域作戰模型初探：以 2020 臺灣選舉為例]. *Prospect Quarterly* 22, no.1 (January 2021): 1-65.

[6] Ibid.

[7] Puma Shen, *New Variants of COVID-19 Disinformation in Taiwan* (Washington D.C., USA: National Democratic Institute, 2022).

[8] Liberty Times Net, "臉書心理測驗藏危機？ 他追查幕後公司爆隱憂 [Facebook Personality Quizzes Hide a Crisis? Researcher Traces the Company Behind It and Reveals Hidden Concerns]." Liberty Times. November 8, 2019. https://news.ltn.com.tw/news/politics/breakingnews/2971518

[9] Austin Horng-en Wang, “色情內容可以用來統戰嗎？證據比你想像的還多 [Can Pornography Be Used for United Front Work? There's More Evidence Than You Think],” *Voicettank,* July 3, 2024. https://voicettank.org/20240703-2/

[10] Austin Horng-en Wang, “河北秦皇島公司控制香港帳號介入 2024 台灣總統大選 [Hebei Qinhuangdao Company Controlled Hong Kong Accounts to Intervene in Taiwan's 2024 Presidential Election],” *Voicettank,* June 4, 2024. https://voicettank.org/20240604-1/

profile anti-China advocate had become a united front model, frequently visiting China, identifying as Chinese, and publicly supporting cross-strait unification.[11] Another well-known case is when Chinese media directly used shell companies in Taiwan to invest in opinion polls and widely spread fake polling results during elections in an attempt to influence the outcome.[12]

- **Ideology-Driven (Human Flow)**

  The third strategy used by China is an Ideology-Driven approach, which involves establishing an "ideology market" to attract individuals who already have the incentive to criticize the government. In this approach, China manipulates information through volunteers who agree with anti-government messages and further spread disinformation in an organic way. The UFWD often shares videos or photos that can be manipulated within private messenger chat groups, where information is weaponized by citizens who voluntarily disseminate pro-China and anti-democracy messages. This volunteer-driven approach, leveraging interpersonal trust and organic dissemination, represents the most challenging form of foreign interference to detect and regulate.

3. Case Study: Taiwan's 2018 Local Elections

The 2018 nationwide local elections in Taiwan provided significant evidence of these covert transnational tactics. Information operations were executed through a hybrid model combining offshore resource manipulation with domestic dissemination. Early anomalies included the artificial inflation of a specific candidate's Google search traffic, with data routed through third-country nodes (e.g., Russia, Malaysia) to mimic organic interest and drive search engine optimization (SEO) for coordinated content farm articles.[13] This manufactured visibility drove the proliferation of content from obscure, overseas-operated platforms like **Mission (密訊)**, a site run by Chinese nationals in Malaysia with editorial input from pro-China actors.[14] At its peak, this single foreign platform became the most frequently shared website by Taiwanese Facebook users in a single week in 2019, making Kuomintang (KMT) supporters, who shared this content most frequently, the direct target of foreign influence.[15]

Crucially, the rapid diffusion relied on dedicated, multi-channel structures beyond content production. These included: **(a)** the direct purchase of existing Taiwanese Facebook fan pages to gain immediate

[11] Liberty Times Net, “價碼曝光！館長遭「統戰」 嘆挺國民黨時「錢很好賺」 [Price Revealed! 'Holocaust' Khan 'United Front' Sighs That 'Money Was Easy to Make' When Supporting the KMT].” Liberty Times. December 4, 2019. https://news.ltn.com.tw/news/politics/breakingnews/2997885

[12] Zhuang Jing et al., "深度報告｜中共外宣在台灣之一：台檢以《反滲透法》訴大選假民調當事人，一審因何失利？[In-Depth Report | CCP Propaganda in Taiwan, Part 1: Why Did the Taiwan Prosecutor Fail in the First Trial of the Fake Poll Suspect under the Anti-Infiltration Act?]," Radio Free Asia, December 12, 2024, https://www.rfa.org/cantonese/news/factcheck/china-taiwan-united-front-work-anti-infiltration-act-12122024120412.html.

[13] Liberty Times Net, "誰最愛 Google 韓國瑜？去年台灣排 16 這國第一名 [Who loves Googling Han Kuo-yu the most? Taiwan ranks 16th last year; this country takes first place]." Liberty Times. December 4, 2019. https://news.ltn.com.tw/news/politics/breakingnews/2998826

[14] Jason Liu, "How do content farms operate in the Asia–Pacific?" *Influence for hire: The Asia–Pacific's online shadow economy*. (Canberra: Australian Strategic Policy Institute, 2020), 27–29.

[15] See note 4.

algorithmic access to domestic audiences; **(b)** the leveraging of proxy actors, such as a Taiwanese businessman serving as a political advisor to Beijing's Chinese People's Political Consultative Conference (CPPCC), to administer major domestic political groups; and **(c)** the mobilization of troll armies to amplify divisive topics, such as the sudden, disproportionate online attention given to air pollution in 2018. Subsequent adaptations included expanding operations to **YouTube** using AI-generated video clips and exploiting the closed, interpersonal trust networks of messaging apps like **LINE**, where disinformation videos seeded on YouTube were redistributed, often bypassing platform verification.

4. Conclusion and Recommendations

The fundamental threat of autocratic information operations is rooted not in content veracity, but in the structural distortion created by asymmetric amplification. These campaigns, which often leverage state resources to deploy mechanisms like content farms and microtargeting, effectively mimic genuine domestic discourse, substituting authentic democratic voices with foreign influence. Social media functions as a "distorted mirror," where a minuscule fraction of actors (e.g., 3% of accounts generate 33% of posts; 1% of online communities are responsible for 74% of online conflict; 0.1% of users driving 80% of disinformation)[16] generates an illusion of consensus or extreme polarization, thereby degrading the civic space and reducing moderate engagement.[17] Therefore, the strategic response must pivot from content verification to the detection and neutralization of these methods of mass amplification. Policy must focus on dismantling the structural architecture of foreign interference and promoting media literacy that encourages citizens to benchmark online narratives against offline, real-world complexity and focus on primary and nuanced information.

Question 2 - Political, legislative and societal counter-strategies

How do state structures in Taiwan on the one hand and civil society and the public on the other react to systematic disinformation and manipulation of information by autocratic states and what recommendations do you have based on this for German politics and society in dealing with manipulated information and, for example, fake profiles on social media?

Answer

Taiwan has developed a pioneering and multi-layered model for countering disinformation, which has demonstrated resilience and adaptive capacity. The nation's approach to combating disinformation encompasses three distinct strategies: legislation, government task force, and civil society.

1. Legal Frameworks and Regulatory Adaptation

In 2019, Taiwan passed the **Anti-Infiltration Act**, prohibiting political donations, illegal funds, and espionage from foreign entities. However, the law has limitations as its provisions focus mainly on the conduct of political parties during elections, leaving a loophole for the online spread of disinformation. The law has also been criticized as being a "punishment" kind of law, which is difficult to enforce

[16] Claire E. Robertson, “Inside the funhouse mirror factory: How social media distorts perceptions of norms”, *Current Opinion in Psychology* (2024)

[17] Chris Bail, *Breaking the Social Media Prism: How to Make Our Platforms Less Polarizing* (Princeton: Princeton University Press, 2021)

against covert information operations. Experts have suggested implementing a **registration act** to require individuals and organizations engaged in political activities to disclose their funding sources, thus increasing transparency and accountability.

The inherent difficulty lies in the threat's multi-vector nature, encapsulated by the 3I Model: Ideology-Driven (Human Flow), Indirect Investment (Money Flow), and Direct Information Manipulation (Information Flow). The existing Anti-Infiltration Act primarily targets the human element, aiming to block foreign directives and covert human influence. Crucially, this legislation is ill-equipped to counter the rapid, anonymous spread of content and the financial backbone of online disinformation campaigns. This gap fueled the pursuit of targeted legislation: the Anti-Fraud Special Act, passed in 2024, was developed to disrupt the financial flows (Money Flow). Conversely, the proposed Digital Intermediary Services Act, drafted in 2022 and partly inspired by the EU's Digital Services Act (DSA) to manage platform accountability and Information Flow, failed to gain traction due to public concern over potential restrictions on freedom of speech, illustrating the complexities of legislating against the full spectrum of the 3I threat.

2. Governmental Structure: Inter-Ministerial Collaboration

The **Government Task Force**, established by the Executive Yuan in 2018, is a resilient, multi-agency effort that coordinates monitoring and source investigation. Crucially, it employs a **"triple-criteria" test**—malicious intent, falsification, and public harm—to justify legal intervention while safeguarding freedom of expression. This framework is reinforced by three institutional guarantees: legislative approval, judicial oversight, and state liability for restrictive actions. While effective at debunking fake news, the task force faces difficulties in addressing complex conspiracy theories.

For this task force to be truly successful and scalable, a robust, comprehensive **legal framework** is essential to legitimize and enforce its actions. Furthermore, effectiveness hinges on speed: **rapid response capability** is the key defense against the exponential spread of false or misleading information. The Task Force must achieve near real-time reaction to information operations to proactively halt viral dissemination before the messages can consolidate influence and cause widespread public harm.

3. Civil Society Resilience and the Fact-Checking Network

Taiwan's civil society forms the critical third layer, operating with vital independence from the government to maintain public trust and credibility. This necessary **distance from the state** is paramount, as close alignment would undermine their long-term effectiveness by allowing them to be viewed as government propaganda.Organizations like Doublethink Lab and the AI Lab use artificial intelligence to analyze patterns, identify sources, and document foreign information operation tactics. Concurrently, groups such as the Taiwan FactCheck Center, MyGoPen, Kuma Academy, and Cofacts actively promote public media literacy and critical thinking. Their efforts include developing school curricula, offering online courses, and establishing fact-checking platforms that use technology, like bots in chat apps, to automatically debunk false information. This response has led to the successful removal of content farm materials and the takedown of state-operated accounts. However, these successes were contingent upon the willingness of **social media companies** to cooperate in moderation efforts. Sustained pressure and incentives are therefore essential to ensure platforms continue to collaborate with government and civil society to mitigate harm effectively.