DKI APCSS
SECURITY
NEXUS

The DKI APCSS journal for comprehensive security issues throughout the Indo-Pacific region and the world!

Security Nexus Perspective

COMPETING IN THE COGNITIVE DOMAIN: LESSONS FROM TAIWAN'S ANTI-FRAUD INITIATIVE

By Michael Kolton & Maa Shyh-Yuan

In his 2025 testimony to the U.S. Congress, the U.S. Indo-Pacific Commander Admiral Samuel Paparo, described China's pressure campaign against Taiwan as "a multi-faceted approach combining military pressure, cognitive and cyber operations, and economic coercion."[1] The U.S. Department of War likewise assesses, "Beijing almost certainly considers cognitive domain operations to be a key component of its pressure campaign against Taiwan."[2] In January 2026, Taiwan's National Security Bureau (NSB) warned that Chinese cognitive warfare aims to weaken Taiwan's *will to resist* and the international community's *will to support.* The NSB also pledged to ensure "unmanipulated public opinion." [3] But how can Taiwan counter China's cognitive warfare? Since 2024, an interagency effort in Taiwan has fought cyberfraud and now offers a blueprint for competing in the cognitive domain. [4]

Taiwan, like the rest of the world, has suffered an intensifying trend of online criminals manipulating victims to steal their assets.[5] [6] [7] In 2024 alone, online scams in Taiwan affected 3.8 million people, stealing over $7.4 billion.[8] For context, Taiwan's most destructive earthquake inflicted $26.5 billion in losses.[9] Organized crime operates in an "intelligence age" of fraud; AI tools and other information technology intensify the "volume, sophistication, frequency and success rate" of their scams.[10] Criminals exploit social engineering to manipulate victims, and integrating the latest cognitive science only supercharges their effectiveness. The same trends – data exploitation, AI-enabled personalization, and social engineering at scale – also affect 21st Century warfare.

Cognitive warfare extends beyond conventional influence operations that shape narratives and sentiments. In their political warfare campaign against Taiwan, China's cognitive domain operations seek to defeat an individual's *will to resist*, thereby achieving aggregate effects for their strategic victory. Advances in technology and neuroscience research strengthen the scale, speed, and precision of cognitive warfare and its manipulation tactics.

Online scams showcase the tactics of cognitive domain operations

Taiwan's NSB warns that China is employing private companies "to collect personal data of Taiwan's political leaders, legislators, and opinion leaders" for psychological attack; they have developed AI tools to automate data collection, video generation, and the "precise" means to deliver effects. [11] [12] Meanwhile, Chinese military researchers envision cognitive domain operations that can disrupt and even manipulate the decision-making of enemy commanders.[13] [14] [15]

Technology researcher Libby Lange similarly details China's pursuit of "algorithmic cognitive warfare" capabilities that employ sophisticated algorithms alongside near-limitless data and compute to tailor content for an "individual's cognitive terrain." [16] Chinese intelligence services and their proxies continuously harvest and process personal data, automating as many steps as possible, and generative AI tools only accelerate bespoke content creation. [17] This evolution delivers custom-built manipulation at speeds far surpassing traditional social engineering.

In Taiwan, victims of online scams are sadly too familiar with such cutting-edge manipulation. Since 2023, criminals have increasingly leveraged AI-generated content like deepfake videos and voice recordings to deceive victims.[18] Scammers especially exploit social media applications, mimicking friends, family members, and trusted organizations.[19] [20] [21] Many scams target victims via direct messaging, then use online payment platforms and cryptocurrencies to transfer funds.[22] [23]

The quality and scale of these tactics are growing in tandem with criminal access to data, compute, and generative AI tools. In February 2026, Taipei police arrested six suspects for masterminding a fake online romance that conned a woman into depositing $225,000 in a fraudulent cryptocurrency investment.[24] The growing intimacy of online fraud reveals personalized manipulations that are evermore automated and scalable. In war, China will employ cognitive domain operations that exploit these kinds of vulnerabilities to achieve political goals.

Taiwan's Anti-Fraud Initiative as a Road Map

In 2024, Taiwan launched the interagency Anti-Fraud Initiative to fight organized crime in a seemingly lawless cognitive landscape. In its first 12 months, Taiwan's Anti-Fraud Initiative achieved measurable success. Financial losses from online scams fell by 50%, a reduction of nearly US$700 million in losses per month.[25] After deploying AI-enabled detection tools, suspicious bank accounts plummeted from a peak of 150,000 in 2024 to fewer than 1,000 accounts by mid-2025.[26] A new platform for the public to report scam ads helped the Ministry of Digital Affairs (MODA) remove over 180,000 violations. MODA's automated detection tool helped reduce scam ads from a weekly rate of 77,000 down to below 900.[27]

The Anti-Fraud Initiative's success countering cyberfraud rested on five pillars relevant to competing against China in the cognitive domain: integrating interagency authorities, collaborating with the private sector, building legislative trust, maintaining transparent metrics, and managing inevitable friction between public and private interests. These pillars underwrite both Taiwan's fight against cyberfraud and its broader effort to build a resilient society that can safeguard democracy across physical and cognitive domains.

Integrating authorities and activities

In 2024, Taiwan's executive branch launched a task force with interagency convening powers to lead the Anti-Fraud Initiative. Under the command of the deputy Minister of Interior (MOI), this task force evolved into a permanent, 10-person office called the Anti-Fraud Coordination Center (AFCC).[28] The AFCC and its interagency partners consulted private industry and designed a framework to align disparate anti-fraud activities. It rejected centralizing control of these efforts under a single office and instead embraced an ethos of synchronizing a whole-of-government mosaic.

The Center became a clearinghouse for policy and an interlocutor for the private sector. In a cognitive warfare scenario, Taiwan, like any democracy, faces a fragmented landscape that includes the military contesting its information environment, intelligence services tracking Chinese malign activities, and the rest of society managing essential services. The AFCC model demonstrates that synchronization, not centralization, is a viable path for competing in the cognitive domain.

Collaborating with the private sector

During a conflict, social media platforms and telecoms will be key conduits for both Chinese cognitive attacks and Taiwan's crisis communications. The relationships and mechanisms built through anti-fraud cooperation offer a foundation for resilience during war.

The AFCC relies on numerous channels to engage social media platforms, telecoms, financial firms, and other corporations. One example is the national-level Fraud Early Warning Center (FEWC), which the Ministry of Justice (MOJ) launched in 2024. In just 12 months, the FEWC blocked US$24 million in illicit transactions after flagging suspicious bank accounts.[29] MOJ subsequently established local FEWCs like the one in Hsinchu, the epicenter of Taiwan's semiconductor industry, which the MOJ describes as the "cornerstone of national defense." The Hsinchu FEWC coordinates with technology firms to counter tactics that include "fake investments, AI face-swapping, impersonating law enforcement, and cross-border scams."[30] The FEWC exemplifies how routine collaboration with technology firms, shared detection platforms, and mutual expectations built the trusted coordination channels needed for defending against cognitive attacks.

At first glance, financial regulators and law enforcement play a limited role during war, but cybercriminals perennially exploit conflicts. Immediately after the October 7th Hamas attacks on Israel, malicious actors launched hundreds of fraudulent charity sites.[31] After Russia invaded Ukraine, cyberfraud cases more than tripled as criminals collected personal data and exploited social media to promote fraudulent financial schemes, often preying upon displaced Ukrainians desperate for loans.[32] In war, China could even encourage syndicates to wreak havoc on Taiwan's population to erode their faith in the government.[33] [34] The systems built under the Anti-Fraud Initiative will help maintain a sense of order in the cognitive realm, fortifying people's confidence.

Building trust with the legislative branch

In 2024, Taiwan's legislature passed the Fraud Crime Hazard Prevention Act (FCHPA), the foundation for the Anti-Fraud Initiative. The new law affected financial firms, telecoms, online advertisers, E-commerce sites, online gaming, and payment services. FCHPA mandated that businesses prevent misuse of their services, authenticate users, share fraud prevention information with the public, and cooperate with law enforcement on fraud investigations. For example, FCHPA required online advertisers to designate a compliance officer, develop fraud prevention plans, and share annual fraud reports with the public.[35] In 2025, lawmakers passed an FCHPA amendment that unlocked more authorities for prosecutors and regulators. This amendment directly resulted from AFCC recommendations and relied on consistent dialogue between officials, legislators, and their staff. This trust enabled reforms at a pace commensurate with rapidly adaptive threats.

Transparent metrics create a common operating picture

Within the first month of the Anti-Fraud Initiative, MOI and its subordinate Criminal Investigative Bureau (CIB) launched a publicly accessible "165 Dashboard" that hosts monthly statistics and routine news updates.[36] The "165 Dashboard" emphasizes two monthly metrics: (1) cases handled and (2) financial losses. *Cases handled* measure performance: "Are we doing the things we said we would do?" *Financial losses* measure effectiveness: "Are the things we are doing achieving desired results?" While no metric captures the full picture, these twin indicators provide government officials, legislators, and voters a common operating picture to chart progress. Extending the 165 Dashboard model beyond cyberfraud – visualizing disinformation, public trust, and resilience to manipulation – would strengthen Taiwan's ability to compete against China in the cognitive domain.

Public and private industry should expect friction

In May 2025, Taipei City officials using new anti-fraud tools detected 1,623 fraudulent advertisements on Meta platforms. City officials notified Meta to remove the scam ads but later reported to MODA that the company missed statutory 24-hour deadlines for 77 ads (5% of the total). MODA met with Meta representatives and later fined the company.[37] For its part, Meta affirmed its commitment to work with regulators and highlighted its removal of 146,000 accounts and 1.6 million scam ads since 2024.[38] Taiwan's CIB likewise reported that Meta removed 26,000 scam ads in just three months between March and June 2025.[39]

At first glance, this interaction may appear adversarial, but friction is practically inherent in any partnership. Even as Taiwan levied fines, MODA and its interagency partners met with Meta and four other major online advertisers to streamline fraud reporting from local jurisdictions, which were still using an antiquated paper-based process. Within a month, MODA expanded access to its "Fraud Reporting and Inquiry Platform" so that local officials could digitally transmit scam ad notifications to companies. [40]

Clear rules are necessary for fruitful cooperation; private companies pursue profit in compliance with the laws and regulations on the books. Enhanced mechanisms for communication help reduce frustration; automated processes and digital platforms help accelerate action. These lessons have applications beyond fighting scam ads. Countering harmful content such as calls for violence or disinformation requires public-private partnerships that will be both challenging and essential. The Anti-Fraud Initiative's experience managing friction provides a model for balancing regulatory enforcement with productive collaboration.

Scaling ahead with a "Rest-of-Society" approach

In a war, China's cognitive domain operations will strike military, government, and civilian individuals for targeted effects. Taiwan's military and intelligence services will duly focus on protecting their forces from cognitive attacks; they will be hard-pressed to also shield everyday civilians, business leaders, and local officials from cognitive manipulation. Taiwan will need the "rest-of-society" to ensure its own cognitive resilience. The AFCC tackled criminal threats in the cognitive domain without turning to the military or intelligence services.

Malicious actors will almost certainly push harmful messaging via Short Message Service (SMS) and social media, disrupting lifesaving updates the government plans to push to personal devices (e.g., missile strike alerts and evacuation orders). Under the Anti-Fraud Initiative, MODA implemented an SMS protocol so that all official government text messages are delivered from a unique "111" phone code, making authentication intuitive for everyday people.[41]

The Anti-Fraud Initiative also led several public awareness campaigns to educate people to detect and report online scams. **Though not a panacea, such campaigns can help harden minds against manipulation.** A well-crafted 90-second YouTube video can boost people's ability to recognize online manipulation. [42] Such low-cost and scalable interventions can contribute to whole-of-society resilience.

Conclusion

The Anti-Fraud Initiative showcased the necessity of clear laws and regulations to guide private industry, especially social media companies and telecoms. Ill-defined expectations for businesses will almost certainly lead to public policy failure.[43] [44] [45] The AFCC modeled a holistic approach built on collaboration with companies and access to legislative remedies. In cognitive warfare, Taiwan will need to continuously refine regulations in dialogue with the private sector to achieve alignment and compete against evolving threats.

In just two years, the AFCC showed how an interagency effort can achieve meaningful results. It also showed that the pace and scale of cognitive domain operations will overwhelm any manual process. To succeed, automated detection tools proved crucial, as did streamlining coordination with telecoms and social media companies. Ultimately, the AFCC's success depended on transparency and collaboration, key pillars for building a resilient society in physical and cognitive domains. Taiwan's Anti-Fraud Initiative shows that democracies can compete in the cognitive domain, not by controlling speech, but by building resilient institutions, partnerships, and public trust.

End notes

[1] *Indo-Pacific Command Posture Statement, Before the Armed Services Committee*, 1119th Cong., 2d sess. (April 2025) (statement of Admiral Samuel Paparo, Commander of U.S. Indo-Pacific Command), https://armedservices.house.gov/uploadedfiles/indopacom_posture_statement_2025.pdf.

[2] U.S. Department of War, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: Department of War, 2025), 37.

[3] National Security Bureau (NSB), "Analysis of China’s Cognitive Warfare Tactics Against Taiwan in 2025," January 11, 2026, https://www.nsb.gov.tw/en/#/%E5%85%AC%E5%91%8A%E8%B3%87%E8%A8%8A/%E6%96%B0%E8%81%9E%E7%A8%BF%E6%9A%A8%E6%96%B0%E8%81%9E%E5%8F%83%E8%80%83%E8%B3%87%E6%96%99/2026-01-11/Analysis%20of%20China%E2%80%99s%20Cognitive%20Warfare%20Tactics%20Against%20Taiwan%20in%202025.

[4] “打核心、追金流、斷生計 政府宣示以團隊作戰模式打詐掃黑,” *Yahoo News Taiwan*, January 2026, https://tw.news.yahoo.com/share/7efcc0b5-fb9c-3a11-805b-45e759597686.

[5] Jorij Abraham, Boice Lin, and Michelle Shen, “State of Scams in Taiwan Report 2025,” *Global Anti-Scam Alliance* (2025) https://www.gasa.org/research.

[6] Charlotte Lee, "Taiwan to penalize Meta over Facebook scam ads," *Taiwan News*, May 21, 2025, https://taiwannews.com.tw/news/6116025.

[7] "詐騙島：全台一天損失 1,300 萬，誰是最大共犯？" *CommonWealth Magazine*, December 17, 2024, https://www.cw.com.tw/article/5133305.

[8] Jorij Abraham, Sam Rogers, Clement Njoki, and James Greening, “The State of Scams in Taiwan 2024,” *Global Anti-Scam Alliance*, 2025.

[9] Centre for Research on the Epidemiology of Disasters, *EM-DAT: The International Disaster Database*, https://www.emdat.be/.

[10] Kenechi Okeleke, “Towards a digital nation: addressing the scam economy in Asia Pacific,” *GSMA Intelligence*, March 2025, 9.

[11] National Security Bureau (NSB), "Analysis of China’s Cognitive Warfare Tactics Against Taiwan in 2025," January 11, 2026, https://www.nsb.gov.tw/en/#/%E5%85%AC%E5%91%8A%E8%B3%87%E8%A8%8A/%E6%96%B0%E8%81%9E%E7%A8%BF%E6%9A%A8%E6%96%B0%E8%81%9E%E5%8F%83%E8%80%83%E8%B3%87%E6%96%99/2026-01-11/Analysis%20of%20China%E2%80%99s%20Cognitive%20Warfare%20Tactics%20Against%20Taiwan%20in%202025.

[12] “Analysis of China’s Cognitive Warfare Tactics Against Taiwan in 2025,” *National Security Bureau*, January 11, 2026, https://www.nsb.gov.tw/en/assets/documents/news/3510977a-3c93-4b15-b1f8-246653335a0d.pdf.

[13] “Cognitive Warfare: Strengthening and Defending the Mind,” *NATO Allied Command Transformation*, April 5, 2023, https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

[14] Nathan Beauchamp-Mustafaga, “Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations,” *Jamestown Foundation China Brief* 19, no. 16 (September 6, 2019), https://jamestown.org/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/.

[15] Jackson Smith and Nathan Beauchamp-Mustafaga, “PLA Social Media Warfare and the Cognitive Domain,” *Jamestown Foundation China Brief* 23, no. 16 (September 8, 2023), https://jamestown.org/pla-social-media-warfare-and-the-cognitive-domain/.

[16] Libby Lange, “Decoding China’s AI-Powered Algorithmic Cognitive Warfare,” *Special Competitive Studies Project*, November 2024, https://www.scsp.ai/resource/decoding-chinas-ai-powered-algorithmic-cognitive-warfare/.

[17] Libby Lange, “Decoding China’s AI-Powered Algorithmic Cognitive Warfare,” *Special Competitive Studies Project*, November 2024, https://www.scsp.ai/resource/decoding-chinas-ai-powered-algorithmic-cognitive-warfare/.

[18] Joanna Octavia, “Online Fraud and Scams in Taiwan,” *Safer Internet Lab* (2025), 5.

[19] Joanna Octavia, “Online Fraud and Scams in Taiwan,” *Safer Internet Lab* (2025), 3.

[20] Joanna Octavia, “Online Fraud and Scams in Taiwan,” *Safer Internet Lab* (2025), 3.

[21] "Strengthening Cybersecurity Resilience and Anti-Fraud Measures," *Ministry of Digital Affairs*, September 2025, https://moda.gov.tw/en/press/press-releases/13876.

[22] Jorij Abraham, Boice Lin, and Michelle Shen, “State of Scams in Taiwan Report 2025,” *Global Anti-Scam Alliance* (2025) https://www.gasa.org/research.

[23] Chiu Chun-fu, “打詐新篇章：AI技術偵測可疑廣告,” *Liberty Times*, September 4, 2025, https://news.ltn.com.tw/news/society/paper/1722827.

[24] Huang Li-yun and Lee Hsin-Yin, “Police bust major international telecommunications fraud ring,” *Focus Taiwan*, February 5, 2026, https://focustaiwan.tw/society/202602050012.

[25] Wayne Fan, “Securities Investment Anti-Fraud Zone: Market Insights,” *Taiwan Stock Exchange*, December 31, 2025 https://www.twse.com.tw/market_insights/en/detail/8a8216d69a3d6cf9019b9600cce806b4

[26] “彭金隆：台灣各銀行AI打詐見效！警示帳戶數「首次負成長」 但誤鎖帳戶民怨呢?” Blocktempo, https://www.blocktempo.com/taiwans-ai-anti-fraud-efforts-yield-results/.

[27] Carol Yang, “Taiwan Government Strengthens Cybersecurity Against AI-Driven Fraud,” *Taiwan News*, October 15, 2025, https://taiwannews.com.tw/news/6220348.

[28] Chiu Chun-fu, “打詐新篇章：AI技術偵測可疑廣告,” *Liberty Times*, September 4, 2025, https://news.ltn.com.tw/news/society/paper/1722827.

[29] “Establishment of the Anti-Fraud Coordination Platform,” *Taiwan High Prosecutors Office*, August 13, 2025, https://www.tph.moj.gov.tw/4421/4509/4515/1316451/post.

[30] “Enforcement Trends in National Security and Trade Secret Protection," *Hsinchu District Prosecutors Office*, September 26, 2025, https://www.scc.moj.gov.tw/295481/295482/295494/1329856/post.

[31] Rapid Response: the Rise of Suspicious Websites at the Start of The Israel-Hamas War 2024,” *Cujo AI,* 2024, https://cujo.com/wp-content/uploads/2024/01/Rapid-Response-the-Rise-of-Suspicious-Websites-at-the-Start-of-the-Israel-Hamas-War-by-CUJO-AI.pdf

[32] Angela Me, ed., "Ukraine: Organized Crime Dynamics in the Context of War," *United Nations Office on Drugs and Crime*, July 2025, https://ow.ly/R6B250WqoHW

[33] Benjamin Sando, "What Would Taiwan's Gangs Do During a Possible PRC Invasion?" December 3, 2025, *Global Taiwan Brief* 10, No. 21, https://globaltaiwan.org/2025/12/taiwans-gangs-possible-prc-invasion/.

[34] Martin Purbrick, "Criminal Organizations as Vectors of Influence in Taiwan," *Jamestown Foundation China Brief* 25, No. 6, September 5, 2025, https://jamestown.org/criminal-organizations-as-vectors-of-influence-in-taiwan/

[35] "Navigating Taiwan's New Anti-Fraud Law: How Can Businesses Comply?" *Tookitaki*, December 13, 2024, https://www.tookitaki.com/blog/navigating-taiwans-new-anti-fraud-law-how-can-businesses-comply

[36] "165 Anti-Fraud Dashboard," *National Police Agency, Ministry of the Interior*, https://165dashboard.tw/.

[37] Lu Yen-tzu and James Lo, "MODA fines Meta NT$2.5 million over delayed fake ads removal," *Focus Taiwan*, August 21, 2025, https://focustaiwan.tw/society/202508210019.

[38] "Meta hit with second fine in Taiwan over Facebook ad transparency issues," *Campaign Asia,* July 2, 2025, https://www.campaignasia.com/article/meta-hit-with-second-fine-in-taiwan-over-facebook-ad-transparency-issues/vaxe661le7no06dvpk9d1pe9uf

[39] Yao Yue-hung and Jason Pan, "Social media scams still common: police," *Taipei Times*, July 29, 2025, https://www.taipeitimes.com/News/taiwan/archives/2025/07/29/2003841099

[40] "MODA Accelerates Takedown of Fraudulent Content by Digitizing Workflows and Partnering with Local Governments for Effective Anti-Fraud Operations, " *Ministry of Digital Affairs*, 25 October 2025, https://moda.gov.tw/en/press/press-releases/17728.

[41] "The 111 Government SMS Platform Sent Out Over 4 Million Messages, with 30 Agencies Cooperating to Reduce the Risk of Scams." *Ministry of Digital Affairs*, January 31, 2024, https://moda.gov.tw/en/press/press-releases/10531.

[42] Jon Roozenbeek, Sander van der Linden, Beth Goldberg, Steve Rathje, and Stephan Lewandowsky, "Psychological inoculation improves resilience against misinformation on social media," *Science Advances* 8, No. 24 *(2022),* https://doi.org/10.1126/sciadv.abo6254.

[43] Emily Denniss and Rebecca Lindberg, "Social media and the spread of misinformation: infectious and a threat to public health," *Health promotion international* vol. 40, 2 (2025): daaf023. doi:10.1093/heapro/daaf023,

[44] Molly Montgomery, "Disinformation as a wicked problem: Why we need co-regulatory frameworks, *Brookings Institute*, August 2020, https://www.brookings.edu/articles/disinformation-as-a-wicked-problem-why-we-need-co-regulatory-frameworks/.

[45] Bhaskar Chakravorti, "The Misinformation Paradox: Why Regulating Online Content at Home May Make Matters Worse in the World," *Defeating Disinformation UnConference*, September 2022, https://digitalplanet.tufts.edu/wp-content/uploads/2023/02/The-Misinformation-Paradox-Why-Regulating-Online-Content-at-Home-May-Make-Matters-Worse-in-the-World-.pdf.

The views expressed in this article are those of the author and do not reflect the official policy or position of DKI APCSS, the Department of War, or the U.S. Government. The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense (DoD) of the linked websites, or the information, products, or services contained therein. DoD does not exercise any editorial, security, or other control over the information you may find at these sites.

February 2026