G1VE TECHNOLOGIES

The Database Before the Barrage: China's AI-Powered Cognitive Warfare Map of Taiwan

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP

Mar 30, 2026

Original source

https://www.linkedin.com/pulse/database-before-barrage-chinas-ai-powered-cognitive-w-b--pbwee/

Section I: The First Strike May Arrive as Data, Not Missiles

Most democratic societies still imagine war beginning with a visible event: missiles, aircraft, sabotage, mobilization, or cyber disruption. But the leaked documents tied to the Chinese company GoLaxy suggest something much more dangerous. The battlespace around Taiwan is being prepared in advance through data aggregation, identity mapping, audience segmentation, AI-assisted propaganda design, and automated influence infrastructure. In other words, the barrage may begin long before the first kinetic salvo. It may begin with a database.

This is why the phrase "The Database Before the Barrage" is not rhetorical flourish. It is a strategic description. A state-affiliated PRC-linked firm reportedly compiled detailed files on Taiwanese politicians, political parties, companies, religious groups, civic organizations, and household records on a scale that touches essentially the entire island. The purpose was not benign research. It was to support cognitive warfare, election interference, and precision-targeted narrative operations inside Taiwan's social and political system.

For national security professionals, this is a critical shift. It means the contested battlespace is no longer just physical, cyber, or informational in the broad sense. It is individually and organizationally mapped. The adversary is not merely broadcasting messages. It is building machine-readable terrain maps of society itself: who matters, who influences, who persuades, who hesitates, who can be divided, and where local chokepoints of political effect actually live.

That is what makes this an elite-level mission assurance problem rather than a generic "disinformation" story. If an adversary can model your society at scale, then it can shape the timing, content, and distribution of influence operations with a precision that starts to look less like propaganda and more like pre-targeting.

Section II: What the GoLaxy Files Reportedly Contained

The reported scope of the data is staggering. According to the Taipei Times, the leaked documents showed a system containing 170 detailed files on Taiwanese politicians, roughly 23 million household registration records, information on 75 political parties, 1,478 Taiwanese firms, 13,000 religious groups, and nearly 24,000 civic organizations. The reporting also said the system supported inquiries connecting party leaders, offices, and geographic coordinates, allowing users to identify local political influence structures and map "pan-green" and "pan-blue" actors by locality.

ISW's summary reinforces that scale and adds further context: the database reportedly included tens of thousands of elite Taiwanese figures from academia, business, and religion, while also categorizing individuals and organizations by ideology, address, and "attitude toward China." It also cited evidence that GoLaxy generated weekly public-opinion reports in the run-up to Taiwan's 2024 presidential and legislative elections. That means the operation was not just about static data warehousing. It was about dynamic monitoring and influence support.

The Taipei Times added another telling layer: the system reportedly tied these structured datasets to more than 6.2 million news articles and social media posts, at least 10,000 Taiwan-related sources worldwide, and roughly 5,000 key social media accounts identified as targets. One report alone tracked 634,448 records of online content in a single week before the 2024

elections, including original posts and responses. This is not the architecture of a clumsy state media push. It is the architecture of a continuously learning influence machine.

Doublethink Lab's review of the leaked documents broadens the picture still further, describing GoLaxy's "GoPro" system as a holistic foreign information manipulation and interference platform capable of trend sensing, target profiling, AI content generation, and scaled distribution through managed accounts. It also found evidence of U.S. political targeting, institutional mapping, and account-farming methods designed to evade detection. Taiwan may be the frontline, but it is clearly not the only target set.

Section III: This Is Not Just Propaganda. It Is AI-Enabled Cognitive Warfare Infrastructure.

The most important conceptual mistake analysts can make here is to treat GoLaxy as merely a PRC propaganda project with better software. It is more serious than that. Doublethink Lab described a system designed around four functional pillars: intelligent perception, intelligent targeting, intelligent generation, and intelligent distribution. That sequence matters because it turns influence into an operational pipeline. First observe. Then identify pressure points. Then generate tailored narrative content. Then distribute it through bot-enabled or managed channels at scale.

According to the leaked materials summarized by Doublethink Lab and Taipei Times, GoLaxy was reportedly experimenting with audience simulation, multilingual virtual characters, and categorization of targets into groups such as "hardliner," "friendly faction," "swing group," and "objective group." This is extraordinarily important from a cognitive-security standpoint. It means the system was not merely pushing generic Beijing narratives. It was trying to model persuasion pathways across different segments of society and then tailor interventions accordingly.

Taipei Times also reported that at least 100 virtual characters were created to interact with target audiences using text, photos, audio, and video in more than 10 scenarios. That is the kind of detail that transforms this from "state media manipulation" into a synthetic engagement architecture. Once virtual personas, language-style simulation, and audience segmentation merge, the adversary no longer needs to flood the zone blindly. It can probe, test, adapt, and intensify narratives in a way that resembles persistent reconnaissance in the human domain.

From a joint-force and critical-infrastructure lens, the implication is stark: this kind of system can soften social resilience before any overt crisis by undermining trust, amplifying division, targeting local governance chokepoints, and degrading the credibility of official information during emergencies. Cognitive warfare of this type is not just about elections. It is about whether a target society can think clearly under pressure when a real crisis arrives.

Section IV: Why This Matters for National Defense, Critical Infrastructure, and Mission Assurance

Taiwan's challenge is not merely to defend territory. It is to defend decision integrity. If public opinion can be manipulated, if election narratives can be shaped, if leadership legitimacy can

be incrementally eroded, and if critical communities can be segmented into predictable behavioral groups, then the opening phase of a future conflict may already be underway long before missiles fly. That has direct implications for mission assurance, civil defense, emergency communications, and continuity of government.

In a crisis, infrastructure operators depend on trusted public messaging. Military forces depend on population stability. Civil authorities depend on belief in lawful command. Election systems depend on confidence. Telecom networks and social platforms become both operational tools and attack surfaces. A database-driven cognitive warfare map can be used to target all of these indirectly by shaping which communities receive which narratives at what moment. That is why this issue belongs not only to intelligence services and ministries of defense, but also to critical infrastructure planners, emergency managers, telecom leaders, and national cyber authorities.

For the broader Indo-Pacific and allied democracies, the signal is equally clear. Taiwan is a frontline laboratory, but the operating model is exportable. Doublethink Lab found that GoLaxy's targeting scope extended well beyond Taiwan into Belt and Road corridors, U.S. institutions, journalists, scholars, military entities, and companies. Once this style of influence architecture matures, any open society with abundant data exhaust becomes targetable terrain.

This is why the right response cannot be a single silver bullet. Democracies need defense in depth for the cognitive domain: better election security, public-private information sharing, social-platform transparency, resilient emergency communications, attribution mechanisms, influence-intelligence fusion, and continuous monitoring of foreign information operations after deployment, not just before them. This is governance at scale, matched to the degree of automation the threat actor is employing.

Section V: The Smart Response Is Not Panic. It Is Layered Resilience.

There is a temptation, when reading about systems like this, to either overreact theatrically or underreact bureaucratically. Both responses are mistakes. The sober answer is layered resilience. Taiwan and its partners need to assume that AI-enabled narrative warfare will continue, improve, and localize. That means they must build defenses that can scale with it.

First, the intelligence community and civil authorities need better integrated awareness of influence operations as an operational, not purely informational, threat. Second, civil society must be treated as part of the resilience architecture, because narrative attacks are often aimed at trust, not just at facts. Third, infrastructure assurance must include communications assurance: the ability to maintain credible messaging during elections, emergencies, and mobilization periods. Fourth, democratic states need system-level risk assessments of how their own data ecosystems, platform dependencies, and political fragmentation can be exploited by AI-enabled foreign influence.

That is the real lesson here. The database is not the attack itself. It is the precondition for a smarter, faster, and more adaptive attack. If democracies wait until the kinetic phase to respond, they will have mistaken the detonation for the preparation.

Section VI: Bottom Line

China's reported GoLaxy architecture shows what cognitive warfare looks like when it matures into data-driven infrastructure. It is systematic. It is AI-enabled. It is socially granular. And it is built to operate before the shooting starts.

Taiwan's challenge, and the challenge for every exposed democracy, is no longer just to survive the barrage. It is to recognize that the barrage may begin with databases, dashboards, and AI-generated personas long before the first visible strike. The states that understand this early will harden not only their networks and missiles, but their social terrain. The ones that do not will eventually discover that they were being mapped, sorted, and shaped while still insisting they were at peace.

✨Call to Action✨:

Subscribe to my LinkedIn Newsletter, "Securing Our Future" for more information, research, case-studies, and literature around how National Defense Strategy, National Security, National Policy, Regulatory Compliance, A.I. (Artificial Intelligence) Governance/Ethics, Internal/External Audit, TPRM (Third-Party Risk Management), Fintech Innovations, and "all things GRC" (Governance, Risk Management, and Compliance) are continuously/dynamically re-shaping and Securing Our Future.

Let's navigate the future together.

🔍 About the Author:

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP, is a seasoned Artificial Intelligence (A.I.), National Defense and National Security Strategist and Subject Matter Expert (SME) in Governance, Risk, and Compliance (GRC), A.I. Governance/Ethics, Regulatory Compliance, Data Governance, Comprehensive/Integrated Risk Management, and Project/Program Management.

As the Managing Partner at G1VE | Technologies and the Strategic Board Advisor to many multi-domain, cross-industry organizations across both the Public Sector (I.e., Fortune 500 and Fortune 1000 companies) and Private Sector entities, W.B. leverages his extensive experience and deep subject matter expertise to drive innovative solutions that enhance organizational resilience and operational integrity. Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP, on LinkedIn to stay updated on the latest insights and trends in these critical areas.