G1VE TECHNOLOGIES

Blackout Before the Blockade: How Beijing Could Turn Taiwan's Infrastructure Into the First Battlefield

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

Apr 12, 2026

Original source

https://www.linkedin.com/pulse/blackout-before-blockade-how-beijing-could-turn-first-w-b--adfdc/

Section I: Stop Imagining the First Blow as a Missile Salvo

If Beijing ever decides to escalate decisively against Taiwan, too many Western observers will misread the opening phase because they are still picturing war as a clean kinetic event. They imagine a visible first strike. Missiles over the Strait. Amphibious formations. Fighter sweeps. A dramatic, undeniable military opening. But that framing is both outdated and strategically dangerous. In a modern coercion campaign, the smarter opening move is often not to destroy the target's forces first. It is to shake the target's confidence in daily continuity — power, fuel, connectivity, port flow, emergency response, logistics, and public trust in the state's ability to absorb shock.

That is why I titled this piece Blackout Before the Blockade. Because the true first battlefield may not be a beach, an airbase, or a naval chokepoint. It may be the invisible architecture of civil functionality. If an adversary can make the public fear rolling blackouts, fuel shortages, digital disruption, telecom degradation, port paralysis, or hospital stress before any decisive kinetic phase begins, then deterrence is already being eroded from the inside. That kind of erosion is difficult to photograph, which is precisely why it is so effective.

Section II: The Campaign Is Already Underway

Reuters reported that Chinese cyberattacks against Taiwan's infrastructure averaged roughly 2.6 million per day in 2025. That is not a normal background level of hostile cyber activity. That is not random probing. That is not ambient friction. That is sustained battlespace preparation at industrial scale. When a state adversary repeatedly probes energy, telecom, transport, and other essential networks, it is not merely scanning for vulnerabilities. It is studying dependencies, mapping failure points, and testing how much access it can build before the strategic moment arrives.

The obvious mistake is to think cyberattacks matter only if they produce immediate, dramatic outages. That is amateur-level thinking. Professional coercion works on accumulation. You learn how the system behaves under stress. You identify the operators who respond fastest. You observe redundancy patterns. You study restoration timelines. You seed uncertainty about what might fail in crisis. You prepare options. You turn infrastructure into a pressure dial.

That is what should alarm allied planners. Not just the volume of attacks. The operational logic behind the volume.

Section III: Beijing Does Not Need to Land Troops to Create Strategic Shock

A blockade is usually imagined in naval terms. Ships. Air corridors. Maritime exclusion. Interdiction. But modern coercion does not need to wait for a formal blockade declaration to begin generating blockade effects.

If China can create widespread concern that Taiwan's grid is unstable, that LNG access is uncertain, that logistics routing is vulnerable, that telecom continuity is fragile, and that public messaging is polluted with panic-inducing disinformation, then it can begin extracting strategic value before a single amphibious wave leaves harbor. A public that loses confidence in continuity becomes easier to intimidate. Markets become more skittish. Supply chains start

hedging. Political arguments intensify. Civil friction grows. Every one of those effects can help an adversary.

Reuters' March reporting showed how Taiwan's officials are already watching this logic play out. Taiwanese officials expressed concern that Beijing could exploit U.S. distraction during the Middle East war and noted the resumption of large-scale Chinese air incursions near Taiwan on March 14–15. The point was not simply to fly planes. The point was to reinforce the perception that when U.S. attention shifts, pressure around Taiwan rises. That is strategic theater with real deterrence consequences.

Section IV: Cognitive Warfare Is Part of the Infrastructure Fight

The infrastructure campaign does not operate alone. It is married to narrative warfare.

Reuters reported that Taiwan reviewed AI-generated online videos pushing the idea of a devastating energy crisis. The Institute for the Study of War documented PRC-linked propaganda claiming Taiwan's LNG supply would run out in 11 days. That is not just generic disinformation. It is infrastructure-focused cognitive warfare. The goal is to make the public rehearse collapse in its mind before any real collapse occurs.

That matters because public confidence is itself a form of critical infrastructure. If households begin hoarding. If investors start repricing continuity risk. If businesses start contingency planning against cascading shutdowns. If local rumor outruns official communication. Then an adversary can generate self-inflicted disruption without ever having to deliver the full physical blow.

This is why "cognitive warfare" should not be treated as some airy strategic buzzword. It is a practical mechanism for magnifying infrastructure pressure. The power grid and the information grid are now part of the same battlefield.

Section V: Military Pressure, Political Delay, and Infrastructure Risk Are Converging

The Institute for the Study of War reporting adds another important layer. In March, the PLA conducted 121 aerial incursions into Taiwan's ADIZ. The China Coast Guard also made four incursions near Kinmen and one near Pratas. That activity matters less as a standalone tactical event than as part of a cumulative operational picture. Gray-zone maritime activity, air pressure, cyber pressure, and propaganda are all reinforcing one another. They are shaping the psychological battlespace while consuming Taiwanese attention and readiness capacity.

Then there is the political bottleneck. ISW reported that Taiwan's proposed $40 billion special defense budget intended to support 200,000 unmanned systems, integrated air and missile defense improvements, and domestic arms initiatives has been obstructed, with rival budget versions closer to $12 billion. The delays have also affected systems such as HIMARS, M109A7 howitzers, and TOW and Javelin missiles. Here is the strategic problem: infrastructure resilience, military readiness, and political cohesion cannot be separated. If legislative drag slows deterrence investments while an adversary increases pressure in cyber, maritime, and information domains, the combined effect is greater than the sum of its parts.

Section VI: The Data Mapping of Taiwan Should Terrify Serious Planners

The March Institute for the Study of War reporting about a PRC-linked AI-driven database is one of the most underappreciated signals in the open-source environment. The reporting described data covering roughly 23 million Taiwanese household records, 170 politicians, around 1,500 companies, 13,000 religious groups, and 24,000 civic organizations. That is not casual intelligence collection. That is social-terrain preparation for influence, coercion, disruption, and targeting.

Why does that matter to an infrastructure article? Because infrastructure is not just wires, substations, pipelines, ports, and routers. It is also the human ecosystem that sustains continuity under stress. Which companies matter? Which local figures matter? Which communities panic first? Which institutions stabilize the public? Which narratives move fastest? Which leaders can be discredited? Which sectors can be pressured? That is infrastructure intelligence in the broadest and most dangerous sense.

An adversary that understands both the physical network and the social network can shape collapse narratives with much greater precision.

Section VII: What a Real Resilience Strategy Looks Like

If Taiwan and its partners are serious, resilience cannot remain a buzzword. It has to become a whole-of-system discipline.

That means:

- Grid redundancy;
- Distributed backup generation;
- Telecom resilience;
- Port and fuel continuity planning;
- Rapid cyber hunt and restoration teams;
- Hospital continuity protocols;
- Trusted emergency communications;
- Public disinformation inoculation;
- Manual fallback procedures;
- Fast allied technical support pathways; and,
- Clear public messaging designed to preserve confidence during degraded conditions.

A military-first-only view of Taiwan misses this. Taiwan's defense is not only about missiles, ships, aircraft, and mines. It is also about keeping the system legible and functioning under pressure. If the lights stay on, if the networks stay partially alive, if the public remains informed, if emergency response holds, and if the economy can keep moving through shock, then Beijing's coercive leverage narrows.

That is why I would argue bluntly that critical infrastructure resilience is now a warfighting function in the Taiwan theater.

Section VIII: The AI Governance Layer Cannot Be Ignored

If AI is going to be used in infrastructure monitoring, anomaly detection, traffic management, cyber defense, restoration prioritization, or emergency communications, then it must be governed with the same seriousness as any other mission-support technology.

1) Scaling governance mechanisms with degrees of autonomy—

A monitoring dashboard is one thing. A system that begins reprioritizing restoration or response resources on its own is something else entirely. The higher the autonomy, the tighter the control structure must be.

2) Supporting human control and accountability—

Grid operators, telecom leaders, emergency managers, and cyber commanders must be able to understand and override AI outputs. Human control cannot be performative.

3) Implementing continuous monitoring, post-deployment oversight—

A crisis changes operating conditions. AI tools that behave well in peacetime can fail under adversarial stress, degraded data, or manipulated inputs.

4) Employing defense-in-depth and containment strategies—

Manual fallback modes, segmented networks, offline contingencies, redundant communications, and restoration playbooks are essential. No single AI-enabled node should become a single point of catastrophic failure.

5) Conducting system-level risk assessments—

Do not assess the model alone. Assess the ecosystem: vendors, cloud exposure, OT/IT boundaries, staff training, data integrity, legal authorities, and public communications dependencies.

Section IX: Thought-Provoking Close & Bottom Line

The first battle over Taiwan may begin long before the first obvious kinetic blow.

It may begin with a surge of cyber pressure. It may begin with energy panic narratives. It may begin with telecom instability. It may begin with logistics anxiety. It may begin with public doubt that the system can hold.

That is why the phrase Blackout Before the Blockade is not rhetorical flourish. It is a strategic warning.

If the first battlefield is continuity itself, then resilience is not a support function.

It is deterrence. It is mission assurance. It is civil defense. It is national defense.

And the side that understands that first will be far harder to coerce.

✨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.