the FOUNDATION FOR
INFRASTRUCTURE RESILIENCE

CHINA AS STRATEGIC ARCHITECT

Consolidated Threat Assessment — The Patient Architect in a Burning World

March 2026 | Open-Source Intelligence Compilation

Stephen Volandt, President

Foundation for Infrastructure Resilience

Contents

Legal Disclaimer

The Foundation for Infrastructure Resilience makes no representations or warranties of any kind, whether express, implied, statutory or otherwise regarding the content of this document, third-party content or references to services or information referenced or available through links herein, and further disclaims all warranties regarding any information contained herein, including any implied or express warranties of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, arising out of any course of dealing or usage of trade.

Public Interest and First Amendment Protections

This publication constitutes protected speech on matters of significant public concern: critical infrastructure security, national defense, public safety, and emergency preparedness. It is entitled to the highest level of First Amendment protection. All factual claims are sourced to specific, citable publications from federal government agencies (CISA, FBI, DOE, DHS, Congressional committees, EMP Commission, FERC), peer-reviewed research, published cybersecurity research from recognized firms (Dragos, CrowdStrike, Palo Alto Unit 42, Recorded Future, Microsoft Security, Forescout Vedere Labs), investigative journalism from recognized outlets, and public filings. FIR does not use or disclose any classified, proprietary, trade secret, or non-public information.

Anti-SLAPP Notice and Litigation Deterrence

Any legal action brought against FIR will be treated as a Strategic Lawsuit Against Public Participation (SLAPP). FIR will respond with immediate motions to dismiss under applicable state anti-SLAPP statutes — including the North Carolina Strategic Litigation Against Public Participation Act (N.C.G.S. § 1-767 through 1-774, enacted 2023). See FIR Volume 1 v6.0 for full legal framework including Public Record Reliance Declaration, Intellectual Property, Use With FIR Certification Framework, and Non-Regulatory Status provisions.

Preface and Version History

This document has evolved through six major versions, each reflecting deepening evidence of China's role as the four-party ecosystem's dominant architect. Versions 1.0 through 3.0 characterized China as an interested observer. Version 4.0 introduced the "calibrator" framework. Version 5.0 elevated China to "strategic architect" based on the Liaowang-1 deployment and MizarVision targeting front company. Version 5.2 incorporated the Iran war's first 17 days and the summit delay.

Version 6.0 represents a fundamental recast. The Iran war is no longer a breaking development — it is a 25-day dataset that validates every element of the strategic architect thesis. China's non-intervention for Iran confirms that the ecosystem is transactional, not protective. The Hormuz closure provides the live-fire proof of concept for the Taiwan LNG blockade that previous versions could only theorize. The summit has shifted from a fixed capstone event to a movable leverage point. And the Foreign Adversary Equipment (FAE) supply chain — Chinese components

embedded inside U.S. critical infrastructure — emerges as the sleeper threat that outlasts any kinetic conflict.

The recast shifts from "here's what China is doing this week" to "here are the enduring structural dynamics that will persist regardless of how the current crisis resolves." Five years from now, the specific Iran war details will be dated. China's patient architecture will still be operative.

Executive Summary

The dominant analytical framing of the Iran war has been geographically and temporally narrow: a Middle East conflict with implications for U.S. stockpiles and Pacific deterrence. This assessment argues that framing inverts the strategic reality. **The Iran war is China's investment portfolio appreciating in real-time.** Every U.S. missile expended against Iran is one fewer for Taiwan defense. Every carrier redeployed to the Middle East widens the Pacific gap. Every day the Hormuz crisis persists, China's energy stockpiling looks more prescient. Every week of war produces intelligence data that directly improves China's Taiwan contingency planning.

China does not need to act while the United States exhausts itself. This is the defining characteristic of the strategic architect: designing the conditions for U.S. strategic exhaustion without firing a shot.

Four lines of effort operate simultaneously:

LINE OF EFFORT 1 — INTELLIGENCE HARVEST: The Liaowang-1 intelligence ship, a 500-satellite network, and the MizarVision front company provide China an unprecedented real-time dataset on U.S. combat operations — every intercept corridor, EW signature, reload timing, and carrier air wing pattern directly applicable to a Taiwan contingency. The Iran war is the most valuable live-fire intelligence event China has observed since the Gulf War.

LINE OF EFFORT 2 — MUNITIONS ATTRITION: China has a documented structural interest in depleting the specific U.S. interceptor inventories (THAAD, SM-3, PAC-3 MSE, SM-6) most critical to Taiwan's defense. By providing Iran targeting data that improves strike accuracy, China accelerates that attrition without expending a single Chinese weapon. Through Day 25: THAAD 20-50% expended, SM-3 ~20%, PAC-3 MSE ~25%.

LINE OF EFFORT 3 — TAIWAN COERCIVE OPTION — THE HORMUZ PROOF: The Strait of Hormuz closure is the live-fire demonstration of exactly the coercive blockade China would execute against Taiwan. Taiwan's LNG reserves would be exhausted in approximately 11 days. The Hormuz closure has demonstrated that even nations with weeks of strategic buffer are in crisis within a month. Japan (95% Hormuz-dependent) in energy emergency. South Korea's PM canceled a China trip. Brent past $112. This is the proof of concept for China's Taiwan playbook: energy blockade achieves coercion without a single shot fired.

LINE OF EFFORT 4 — DIPLOMATIC LEVERAGE: China arrives at any eventual summit holding the Liaowang-1 dataset, influence over Iranian calibration, the LNG quarantine option,

and the demonstrated appearance of restraint as currency. The most important battle of the Taiwan question may be won at a negotiating table, not in the Taiwan Strait.

Central Finding: China does not need to invade Taiwan, fire on U.S. forces, or directly arm Iran to win the most consequential strategic campaign of this crisis. It needs only to be present, patient, and positioned. The four-party ecosystem — Iran as the kinetic arm, Russia as the capability multiplier, North Korea as the financial and attribution layer — is operating in a manner that serves Chinese interests at every node, whether or not Beijing has explicitly directed any of it.

---

1. China as Strategic Architect: The Thesis Stated

1.1 The Prior Framework and Its Limitation

Versions 4.0 and 4.1 characterized China as a "calibrator" — an actor that constrains Iranian behavior within guardrails protecting Chinese commercial interests while permitting sustained deniable pressure on the United States. That characterization was accurate as a description of Chinese messaging. It was incomplete as a description of Chinese action.

The evidence accumulated since February 28, 2026 establishes that China has actively provided the intelligence infrastructure that makes Iranian targeting operations more lethal, deployed its most advanced naval intelligence platform to a live combat zone to harvest U.S. operational data, pre-positioned 40 million barrels of oil in floating storage anticipating disruption, and positioned its diplomatic assets to convert resulting U.S. vulnerability into strategic concessions on the Taiwan question. These are not the actions of a calibrator. They are the actions of a strategic architect.

1.2 What "Strategic Architect" Means Analytically

A strategic architect does not need to control every actor in a system to benefit from every actor's actions. China's position is structurally analogous to a chess player who did not set up the board but has arranged the pieces such that every legal move available to the opponent serves the architect's interests. Iran's missile salvoes deplete U.S. interceptors. Russia's targeting data improves Iranian strike accuracy. North Korea's financial infrastructure insulates Iran's bounty network from OFAC interdiction. None require Chinese direction. All produce effects that advance Chinese strategic objectives.

1.3 The Line China Has Already Crossed

The Liaowang-1 deployment and MizarVision targeting front company constitute active Chinese contribution to lethal operations against U.S. forces — not through weapons, but through the targeting data that guides Iranian weapons to U.S. targets. In any prior era of great power competition, that would be classified not as non-participation but as active belligerence short of kinetic engagement.

1.4 The Iran War Validates the Thesis

China designed — or recognized and optimized — an ecosystem where proxies consume U.S. resources while China harvests the strategic dividend. The Iran war is that design operating as intended. China's

response confirms: condemning strikes verbally, providing zero military support, quietly solidifying its advantage. The Carnegie Endowment's March 2026 assessment is definitive: "A strategic partnership with Beijing falls far short of a military alliance." China's priority is surviving Trump's presidency without escalation while doubling down on import substitution and rare earth advantage. The Iran war is not a problem for China — it is a gift.

---

2. The Liaowang-1 and the Live-Fire Intelligence Harvest

2.1 What the Liaowang-1 Is

The Liaowang-1 is China's most advanced maritime intelligence platform, deployed by the PLA Navy to the Gulf of Oman in the days before Operation Epic Fury. From its position near the Strait of Hormuz, the ship's 6,000-kilometer sensor envelope covers the Arabian Sea, the Persian Gulf, and large areas of the Middle East. Accompanied by Type 055 destroyers and a Type 052D, the fleet operates in international waters where any action against it constitutes an act of war.

2.2 What the Liaowang-1 Is Collecting

Each day that the Liaowang-1 operates in the Gulf of Oman, it is constructing a high-resolution operational picture of how the U.S. military conducts high-intensity conflict. This is not abstract intelligence collection. It is the specific operational data that determines whether Chinese missiles hit American ships in a Taiwan scenario. Consider what the ship's 6,000-kilometer sensor envelope is recording:

Intercept corridor geometry: When Iran launches a salvo of Fateh-313 ballistic missiles at a U.S. base in Bahrain, the SM-3 and PAC-3 systems that intercept those missiles use specific approach angles, altitude profiles, and engagement geometries. The Liaowang-1 records every intercept — which approach corridors the U.S. systems use against which missile types, at what altitudes, on what timing sequences. In a Taiwan scenario, PLA DF-21D carrier-killer missiles will face these same interceptor systems. Knowing exactly how those systems engage — and where the gaps in their geometry are — allows PLA planners to design salvoes that exploit the blind spots. This data cannot be obtained any other way. Peacetime exercises use different geometries than combat operations. Only a live, high-intensity engagement against real missile threats produces authentic intercept corridor data.

Electronic warfare signatures: Every U.S. radar system, every jammer, every countermeasure emitter has a specific electronic signature — a fingerprint that identifies the system, its operating mode, and its capabilities. Under combat conditions, the full spectrum of U.S. electronic warfare capability is activated simultaneously: carrier air wing jamming, Aegis radar in full combat mode, THAAD tracking radar, Patriot search and engagement radars, and the electronic countermeasure environment created by EA-18G Growlers. The Liaowang-1 is cataloguing this entire electromagnetic order of battle in real-time — not the sanitized peacetime signatures that the PLA already has from SIGINT collection, but the full combat signatures that reveal which modes are

used when, what jamming techniques are employed against what threats, and where the seams between U.S. and allied electronic warfare systems create exploitable gaps.

Reload timing and magazine depth: This is the data point that converts intelligence into targeting doctrine. When an Aegis destroyer expends its SM-3 interceptors against an Iranian ballistic missile salvo, how long before its Vertical Launch System cells are reloaded? What is the sequence — which missiles are loaded first, from which magazines, using which pier-side or underway replenishment procedures? How many rounds does a destroyer actually carry versus its theoretical capacity? When the magazine is empty, what happens — does the ship withdraw to a rearming port, or does it remain on station with reduced capability? Each of these timing parameters defines a window of vulnerability. In a Taiwan scenario, the PLA's operational concept centers on overwhelming U.S. missile defense through salvo volume — firing enough missiles to exhaust magazine depth, then striking during the reload window. The Iran war is telling China exactly how wide that window is, for each ship class, against each missile type. No simulation, no wargame, no peacetime exercise produces this data. Only the Iran war does.

Carrier air wing operational patterns: The Ford and Lincoln carrier air wings are flying combat sorties at a tempo not seen since the Iraq invasion. The Liaowang-1 records sortie rates, refueling track geometry, alert posture transitions, the specific radar and communications signatures of F/A-18E/F and F-35C operations under combat stress, and the time between "alert" and "airborne" for different threat levels. These patterns are the raw material for PLA anti-access/area-denial planning: knowing when carrier air wings are at peak and minimum readiness, how quickly they transition between postures, and what their radar signatures look like at each stage allows PLA targeting systems to time strikes for maximum impact against minimum defense.

Command and control architecture: The most strategically consequential data category. How long does it take from the moment a missile is detected to the moment an intercept is authorized? What communications protocols connect the detecting sensor to the decision-maker to the firing unit? Where are the organizational seams between U.S. and allied missile defense systems — the handoff points where an Israeli Arrow detects a threat and a U.S. Patriot engages it? Each seam is a potential point of failure. Each delay in the decision chain is a window for a faster adversary to exploit. China is mapping the entire command architecture of U.S. coalition warfare in real-time, under combat conditions where the actual decision latencies — not the theoretical ones from peacetime exercises — are visible.

None of this data could be generated by peacetime exercises. A live high-intensity conflict provides the only environment in which these signatures are fully authentic. China is receiving that data now, legally, from international waters, at no cost and no risk. Every additional day the Iran war continues, China's Taiwan contingency planning improves by a measurable increment. This is not a theoretical concern about future intelligence value. It is an active, ongoing intelligence operation producing real-time operational data that will be applied against U.S. forces in the next major crisis.

2.3 MizarVision and the Targeting Front Company

MizarVision, a Shanghai-based company, began publishing annotated imagery of U.S. military targets the week before Epic Fury. The company does not own satellites. It procures, processes, and publishes analyzed imagery without charge — the functional signature of a government front company conducting active targeting support under commercial cover. Western commercial satellite providers appeared to turn off postings of conflict areas as of March 3 in recognition of the targeting pipeline.

2.4 The 500-Satellite Network

China's fleet of more than 500 operational military and dual-use satellites forms the backbone of a persistent intelligence-sharing structure that transmits data to Iranian command systems. This is supplemented by the Russia-Iran Khayyam satellite constellation providing 1-meter resolution imagery approximately four times daily. China, Russia, and Iran have constructed a multi-layer ISR architecture covering every U.S. military asset in the theater.

2.5 Strategic Implication for Taiwan — Updated by Iran War

The Iran war provides unprecedented live-fire data on U.S. weapons performance, intercept rates, logistics chains, allied coordination, and domestic political response. This data directly improves China's Taiwan contingency planning across every relevant dimension: PLA strike timing to exploit reload gaps, electronic warfare countermeasures tuned to actual U.S. signatures, salvo sizing calibrated to actual intercept success rates, and coalition vulnerability assessment based on observed allied fragmentation under energy pressure. The dataset being accumulated now will be applied against U.S. forces in the next major crisis.

---

3. The Munitions Gap as a Chinese Strategic Asset

3.1 The Structural Deficit Before the Iran War

The Heritage Foundation's January 2026 report established that the U.S. entered the Iran conflict already holding a critically deficient interceptor inventory. SM-6 interceptor production was at approximately 125 units per year against assessed requirements exceeding 1,000 for a Taiwan scenario. PAC-3 MSE was at approximately 500 units per year against requirements that the Iranian salvo rate alone was consuming at rates exceeding production. The deficit was structural before the first Iranian missile was launched.

3.2 Iran War Consumption Rate — Updated Through Day 25

The Iran war has consumed U.S. interceptor inventories at rates that exceed peacetime replacement capacity by an order of magnitude. Through Day 25 of Operation Epic Fury, estimated depletion: THAAD interceptors 20-50% of inventory expended; SM-3 approximately 20% expended; PAC-3 MSE roughly 25% of required military plans consumed; SM-6 stocks drawn down significantly. Iran produces approximately 100 ballistic missiles per month against a U.S. interceptor production rate of six to seven per month. The PrSM (Precision Strike Missile) saw its first combat deployment. A David's Sling

malfunction allowed two Iranian ballistic missiles to strike southern Israel, wounding dozens — demonstrating that interceptor systems are not infallible under sustained salvo fire.

SYSTEM	TAIWAN RELEVANCE / STATUS
THAAD	Primary defense vs. DF-21D/DF-26 carrier-killers. Estimated 20-50% expended in Iran campaign. 534 total delivered; delivery gap since mid-2023.
SM-3 Block IIA	Intercepts mid-course ballistic missiles in exo-atmosphere. ~20% of total inventory expended. Critical for carrier strike group defense.
PAC-3 MSE	Defends airfields and command nodes vs. shorter-range ballistic and cruise threats. US at ~25% of required inventory. Annual production 600-650 units.
SM-6	Terminal defense vs. cruise missiles and aircraft. Consumed rapidly in Iranian drone/missile waves. VLS reload gap of multi-weeks.
Tomahawk LACM	Strike weapon against PLAN shore infrastructure. Smaller stockpile; used extensively in strikes against Iran.

Secretary of State Rubio's public statement establishes the asymmetric exchange rate: Iran produces approximately 100 ballistic missiles per month; the US produces six to seven interceptors per month. Each PAC-3 MSE interceptor costs approximately $3.9 million against an Iranian Fateh-313 costing under $500,000. Iran's deliberate doctrine — using cheap drones to trigger expensive interceptors before following with ballistic missiles — systematically degrades US magazine depth at an economically unsustainable ratio. Aggregate US Vertical Launch System inventories at an estimated 17,000 rounds are insufficient for even one full fleet reload. Pier-side rearming creates multi-week gaps during which ships are operationally defenseless.

3.3 China's Role in Accelerating the Deficit

China did not create this depletion. But by providing Iran the targeting data that improves strike accuracy and forces higher intercept rates, China accelerates it. The Liaowang-1's real-time sensor data, MizarVision's targeting imagery, and the 500-satellite ISR architecture all contribute to making Iranian salvoes more effective — requiring more U.S. interceptors per salvo. Each interceptor expended against an Iranian missile is one fewer available for the opening salvoes of a Taiwan contingency. This is a quantifiable Chinese strategic asset.

3.4 The Production Ramp Cannot Close the Gap

Defense Production Act ramp-ups require 18-36 months to produce meaningful additional inventory. The window of maximum U.S. vulnerability is the 2026 calendar year — with the gap widening for every additional week the Iran war continues. The circular dependency compounds: munitions production depends on the defense industrial base, which depends on civilian infrastructure (energy, water, transportation, workforce), which is the same infrastructure Volt Typhoon is pre-positioned to disrupt.

3.5 The Taiwan Interceptor Calculus

If X interceptors consumed in the Iran war through Day 25, and production rate is Y per month, and a Taiwan contingency requires Z interceptors for the opening salvo exchange, the gap in Pacific theater is (Z - (remaining inventory + Y × months until contingency)). This gap is China's most quantifiable strategic asset — and it grows with every additional day of the Iran war. Beijing is watching this arithmetic in real-time.

---

4. The Pacific Force Posture Gap

4.1 Current Carrier Posture — Updated

The USS Abraham Lincoln carrier strike group has redeployed from the South China Sea to the Middle East. The USS Gerald R. Ford has deployed to support Iran operations. The USS George Washington is in maintenance. The western Pacific carrier posture is at its lowest point since 2022 — possibly the lowest since the Taiwan Strait crises.

4.2 Allied Compensation — Degraded by Hormuz

Japan and South Korea — the two Pacific allies most capable of contributing to Taiwan defense — are managing their own Hormuz-driven energy emergencies. Japan (95% Hormuz-dependent) declared an energy emergency within three weeks of the closure. South Korea's PM canceled a planned China trip to manage domestic economic fallout. Their ability to contribute military assets to a Taiwan contingency is degraded by their own crisis — a crisis created by the same ecosystem whose architect is China.

4.3 China's Assessment of the Gap

China sees the widest Pacific force posture gap since the Taiwan Strait crises. It also sees U.S. willingness to use force (Iran), which complicates the calculus — a demonstration of U.S. military capability cuts both ways. But the net assessment favors Beijing: the U.S. has demonstrated willingness but is consuming the capability it would need to back that willingness in the Pacific.

---

5. Taiwan's LNG Vulnerability: The Hormuz Proof

5.1 Taiwan's Energy Import Dependency

Taiwan imports 97% of its energy by sea. LNG powers approximately 47% of electricity generation following the May 2025 nuclear closure. Coal provides approximately 39%, with approximately 42-45 days of reserve. Oil reserves are approximately 146 days but only 4.7% of generation capacity. LNG reserves would be exhausted in approximately 11 days under a total blockade. LNG "boils off" in storage and cannot be adequately stockpiled.

The reserve figures by fuel type are the critical variable:

FUEL TYPE	RESERVE DURATION / STRATEGIC ASSESSMENT
LNG	Approximately 11-12 days under normal consumption. LNG "boils off" in storage — cannot be stockpiled. Powers 47% of electricity generation. The decisive vulnerability.
Coal	Approximately 42-45 days. More storable than LNG. Powers ~39% of generation. Could extend grid operation if LNG burden is shifted.
Oil / Crude	Approximately 146 days. However, oil-fired capacity is only 4.7% of total. The reserve is largely non-generative for grid purposes.
Renewables	12% of current mix. Cannot compensate for LNG loss at scale. Offshore wind running years behind schedule.

5.2 Why LNG Is the Strategic Lever

LNG is physically incapable of being adequately stockpiled. Taiwan's three main LNG terminals and Taichung coal port cluster along the west coast — within PLA missile range — with shipments funneled through the Taiwan Strait. TSMC consumes approximately 10% of Taiwan's total power. When LNG reserves fall below the critical threshold and grid stability degrades, TSMC's fabs go offline. The semiconductor rationale for Western military commitment to Taiwan evaporates before a blockade completes its second week.

5.3 The Hormuz Proof — Live-Fire Validation

The Strait of Hormuz closure is the centerpiece development for this section. What Version 5.2 could only theorize, the Hormuz crisis demonstrates empirically:

The Strait of Hormuz — through which approximately 20% of global petroleum flows — has been effectively closed for 25 days. The cascading consequences validate every element of the LNG coercion thesis:

Japan (95% Hormuz-dependent) declared an energy emergency within three weeks. The world's third-largest economy, with one of the most sophisticated energy management systems on earth, is in crisis from a single chokepoint disruption. Taiwan has 7-11 days of LNG storage. If Japan — with far greater reserves and far more diversified supply — is in emergency within a month, Taiwan would be in crisis within days.

South Korea (70% Hormuz-dependent) — PM canceled a China trip to manage domestic economic fallout. South Korea's semiconductor industry (Samsung, SK Hynix) faces the same energy vulnerability as TSMC.

IEA chief assessment: "Worse than the two energy crises of the 1970s and the fallout of the Ukraine war put together."

Brent crude past $112 and rising. Global economic shockwave affecting stock markets, commodity prices, and trade flows worldwide.

Gulf state energy infrastructure under direct attack: Kuwait's Mina al-Ahmadi refinery (730,000 bpd capacity) struck by Iranian drones. Qatar's Ras Laffan LNG facility (17% of global LNG capacity, ~$20B annual loss, ~9% GDP hit) struck.

Panama Canal at maximum capacity (36-38 vessels daily) as global shipping reroutes.

The Hormuz closure is the proof of concept for China's Taiwan playbook. Iran demonstrated that a single chokepoint closure — using missiles, drones, naval mines, and fast attack craft — can destabilize the global economy within weeks. China is watching this lesson in real-time via the Liaowang-1 and its satellite network. The Taiwan Strait is China's Hormuz: narrower, closer to PLA bases, and defended by a Coast Guard that has already practiced the quarantine template in the South China Sea.

China pre-positioned for the disruption: approximately 40 million barrels of Iranian and Venezuelan crude in floating storage on tankers anchored in Chinese coastal waters in the weeks before the strikes — suggesting advance awareness or strategic hedging. While Japan and South Korea scramble, China draws from pre-positioned reserves.

5.4 The Coercive Quarantine Playbook

China's preferred instrument is not a naval blockade — an act of war triggering allied response obligations. It is a "quarantine": a Coast Guard-led maritime enforcement operation, framed as routine inspection, that introduces sufficient delays into LNG tanker transit to degrade delivery rates without crossing the kinetic threshold. This playbook is already operational in the South China Sea. The legal ambiguity is the point. U.S. strategic ambiguity on whether a "quarantine" constitutes an act of war requiring military response is precisely the uncertainty China needs.

5.5 The U.S. Response Dilemma Under Current Posture

Breaking a Chinese LNG quarantine requires naval escort operations at WWII scale — assets currently in the Middle East, in maintenance, or insufficient as standalone combatants. It requires interceptor stocks currently depleted. And it requires a policy commitment to treat a Coast Guard action as an act of war — a threshold no U.S. administration has publicly crossed. The deterrent credibility gap is real and visible to Beijing.

---

6. China's Five-Step Coercive Playbook: The Non-Kinetic Path to Taiwan

The following sequence synthesizes the structural conditions documented in Sections 2-5 into a coherent operational playbook that China could execute in the current window without a single military engagement with U.S. forces. Each step builds on the previous one. No step requires kinetic escalation. The playbook succeeds through patience, positioning, and the exploitation of conditions that other actors' conflicts create.

Step 1 — Intelligence Harvest (NOW — ongoing through end of Iran conflict): The Liaowang-1, 500-satellite network, and MizarVision continue real-time collection on U.S. combat operations. Data is being catalogued and incorporated into PLA targeting models for a Taiwan

contingency. Every additional day of the Iran war produces operational intelligence that cannot be obtained any other way. This step requires no Chinese action beyond keeping the Liaowang-1 on station — which it is doing legally in international waters.

Step 2 — Ambiguity Engineering (NOW — through any eventual summit): China maintains rhetorical restraint publicly while providing active ISR support to Iran. The message to Tehran is "keep it deniable" rather than "stand down." The message to Washington is "we are exercising restraint and deserve credit for it." This preserves the U.S. need for Chinese "moderation" as a negotiating chip — a chip China intends to cash at the summit in exchange for structural concessions. Every day China refrains from arming Iran with advanced weapons or activating Volt Typhoon, it accumulates diplomatic currency. This step requires China to do nothing except be visibly not-escalating.

Step 3 — Impose the LNG Clock (Post-summit, if conditions favor): Coast Guard quarantine of LNG tanker approaches to Taiwan's western terminals. Not a blockade — a "quarantine" framed as routine inspection, health verification, or customs enforcement. Sufficient delays and uncertainty to begin degrading LNG delivery rates. Taiwan's 11-day LNG reserve begins counting down. TSMC goes offline before the second week. Taiwan faces a choice: capitulate to Chinese demands, or watch its economy collapse in real-time while the U.S. debates whether a Coast Guard action constitutes an act of war. The Hormuz closure has now proven at global scale that energy supply disruption produces this exact cascade within weeks — China does not need to theorize about the LNG clock; it has watched the Hormuz clock run on Japan and South Korea.

Step 4 — Summit Leverage (Concurrent with or following Step 3): China arrives at any eventual summit holding four cards simultaneously: the Liaowang-1 intelligence dataset (leverage: "we know your vulnerabilities"), influence over Iranian calibration (leverage: "we can escalate or restrain"), the LNG quarantine option (leverage: "Taiwan's clock is running"), and the demonstrated appearance of restraint (leverage: "we have been responsible partners — what have you given us in return?"). China trades the appearance of moderation for structural concessions: reduced Taiwan arms sales, relaxed semiconductor export controls, modified tariff architecture, tacit acceptance of the quarantine as a non-military action. The most important battle of the Taiwan question may be won at this table — not in the Taiwan Strait.

Step 5 — Fait Accompli (Endgame): If Taiwan capitulates under energy pressure before the U.S. can organize a military response — and the current force posture, depleted interceptor stocks, and allied energy crises make a rapid response structurally difficult — China achieves its core objective without firing a shot. Even if the quarantine does not produce capitulation, it demonstrates that China can impose unacceptable costs on Taiwan at any time of its choosing, fundamentally shifting the deterrence calculus. The playbook does not require completion to succeed — each step produces independent strategic value whether or not subsequent steps are executed.

The critical insight: This playbook does not require the Iran war to continue. Steps 1-2 are being executed now. Steps 3-5 can be executed at any point in the future when conditions favor them — and the Iran war is creating those conditions by depleting the interceptors, redeploying the carriers, distracting the allies, and consuming the institutional bandwidth that would otherwise be available

to respond. China is not on a timeline. China is on a trajectory. The trajectory is favorable and accelerating.

---

7. The Diplomatic Dimension — Strategic Dynamic, Not Fixed Date

7.1 What China Is Selling

China sells the appearance of restraint. Every day Beijing does not arm Iran with advanced weapons, does not activate Volt Typhoon against U.S. infrastructure, and does not execute the Taiwan quarantine generates diplomatic currency. This currency is perishable — it must be spent at the negotiating table. But the longer the Iran war continues, the more currency accumulates.

7.2 The Leverage Asymmetry

The U.S. needs China's cooperation on multiple fronts simultaneously: restraining Iranian proxies, mediating ceasefire, controlling oil markets, maintaining trade flows, managing North Korean escalation. China needs one thing from the U.S.: concessions on Taiwan. The leverage asymmetry is structural and growing.

7.3 The Iran War as Diplomatic Asset

China can offer to "help" with Iran — restraining proxies, mediating ceasefire, stabilizing oil markets — in exchange for concessions on Taiwan arms sales, semiconductor export controls, and tariff architecture. This is the "moderation as currency" trap: the more crises the ecosystem generates, the more opportunities for China to trade the appearance of help for structural concessions.

7.4 The "Moderation as Currency" Trap — Enduring Dynamic

This pattern compounds over administrations. Each summit where China trades restraint for concessions establishes a new baseline. The structural shift is incremental but directional — toward Beijing's preferred endpoint on Taiwan.

---

8. The Four-Party Ecosystem Through China's Lens

8.1 Iran: Kinetic Arm Now Degraded but Still Operational

Iran's conventional military capability is significantly reduced by Operation Epic Fury. But Iran continues fighting on Day 25, still launching ballistic missiles and drones. The successor regime will need China more than ever — as primary oil buyer, technology supplier, and diplomatic protector. China's leverage over its kinetic arm increases as Iran weakens.

8.2 Russia: Capability Multiplier Benefiting from Distraction

Russia benefits from the oil price spike ($112+ Brent) funding its Ukraine campaign, from U.S. distraction reducing Ukraine peace pressure, and from interceptor competition degrading both theaters. Russia's

"credibility floor" is exposed — it did not defend Iran — but the transactional partnership continues because both parties benefit.

8.3 North Korea: Financial Infrastructure Unaffected and Expanding

North Korean IT worker infiltration, cryptocurrency laundering ($1B+ annually), and ammunition supply to Russia continue unaffected by the Iran war. Revenue is "at its highest levels since before extensive sanctions were imposed in 2018" (2026 ATA). The financial plumber operates independently of any kinetic conflict.

8.4 Volt Typhoon as Independent Activation

Volt Typhoon's confirmed pre-positioning inside U.S. critical infrastructure — communications, energy, transportation, water systems near military installations — is completely independent of the Iran war. It can be activated on China's timeline regardless of the ecosystem's status. This is the enduring threat that outlasts every kinetic conflict: Chinese cyber capability embedded inside U.S. infrastructure, waiting for the moment Beijing determines that a Taiwan contingency requires degrading U.S. deployment capability.

---

9. The Domestic Threat Landscape: The Ecosystem's Human Infrastructure

9.1 The Fatwa Architecture

Multiple binding fatwas from senior Grand Ayatollahs with Qom Seminary endorsement charge Trump and Netanyahu with Moharebeh — waging war against God — punishable by death under Article 279 of Iran's Islamic Penal Code. These fatwas do not expire. The 1989 Khomeini fatwa against Salman Rushdie was partially fulfilled 33 years after issuance. Current fatwas carry greater endorsement, larger financial backing ($40M+ confirmed via thaar.ir, with North Korean Lazarus Group infrastructure potentially increasing effective funds beyond OFAC reach), and are issued in the context of active military conflict that killed the issuing cleric's son.

9.2 Three Categories of Domestic Threat Actor

Category 1 — IRGC-Directed Cells: Highest capability, moderate-to-high detection probability. Require real-time Tehran communication. Currently constrained by internet blackout but operationally viable as "Barracks Internet" restores IRGC-cleared connectivity within 2-4 weeks.

Category 2 — Pre-Activated Proxy Networks (Hezbollah/Fatimiyoun): Most operationally dangerous near-term category. Convicted Hezbollah sleeper agent Ali Kourani told the FBI: "In the event that the United States and Iran went to war, the US sleeper cell would expect to be called upon to act." That scenario has arrived. Iran's Foreign Ministry publicly acknowledged that several military units are "operating according to old general instructions" — the dead-man's-switch architecture. Pre-arranged activation requires no interceptable communication.

Category 3 — Self-Radicalized Lone Actors: Highest probability of near-term occurrence. The Austin, TX shooting of March 1 (Ndiaga Diagne, 2 killed, 14 wounded, Iranian flag imagery), the

Toronto boxing gym attack against Iranian dissident Salar Gholami, and multiple smaller incidents illustrate the speed at which fatwa messaging translates into kinetic action within 48 hours of major provocations.

9.3 Confirmed Cyber Activity Since February 28

DieNet group DDoS against a US port. Fatimiyoun Cyber Team code injection and PII release from a US township. Attack on Truth Social claimed by Iran-aligned hackers. CrowdStrike confirmed reconnaissance and DDoS activity — "behaviors that often precede more aggressive operations." Handala (MOIS-linked) showing reduced public blog activity consistent with active operational tempo.

9.4 Institutional Degradation at the Moment of Peak Threat

CISA at approximately 38% staffing. FBI's specialized Iran counterintelligence unit (CI-12) degraded by personnel actions immediately before Operation Epic Fury. NTAS website not updated since February 17. Approximately 18,000 known/suspected terrorists with jihadist ties documented as having entered the country (NCTC Director Kent, December 2025).

9.5 The March 9 Dead-Man's Switch Confirmation

Federal law enforcement alert confirmed the United States intercepted encrypted communications believed to have originated in Iran that may serve as an operational trigger for sleeper assets outside the country. The transmission was relayed across multiple countries shortly after the death of Khamenei. This is the numbers station architecture: shortwave radio broadcasts using pre-shared encryption keys, requiring no internet, no cellular network, and no return signal. The dead-man's switch has been triggered.

9.6 Bandwidth Consumption as China's Domestic Strategy

The Iranian domestic threat — fatwa architecture, Hezbollah/IRGC sleeper networks, self-radicalized lone actors, numbers station-activated assets — consumes U.S. domestic security bandwidth simultaneously with munitions attrition and Pacific force posture degradation. A government managing domestic casualties, active war, and institutional gaps has reduced capacity to respond to a Taiwan quarantine. This is the domestic dimension of China's architect role: Iran's kinetic arm creates the homeland distraction that opens the Pacific window.

The March 9 encrypted activation signal — confirmed by federal law enforcement as an operational trigger for sleeper assets — represents the dead-man's switch architecture in operation. The domestic threat is not theoretical — it is active and underway. CISA at approximately 38% staffing. The FBI's specialized Iran counterintelligence unit (CI-12) degraded by personnel actions immediately before Epic Fury. Approximately 18,000 known or suspected terrorists with jihadist ties documented as having entered the country (NCTC Director Kent, December 2025 testimony).

---

10. Infrastructure Attack Doctrine: The Shared Playbook

10.1 Iran's Documented OT Penetration — Persists Regardless of War Outcome

IRGC-affiliated CyberAv3ngers achieved operational control of U.S. water treatment PLCs, with CISA confirming "deeper access capable of more profound cyber-physical effects." This capability is not eliminated by air strikes on Iranian missile factories. The cyber implants persist inside U.S. infrastructure independent of the kinetic war.

10.2 Volt Typhoon's Independent Access — The Enduring Threat

Volt Typhoon has maintained access to U.S. critical infrastructure for at least five years, progressing inside operational control loops. Dragos assesses that many water-sector utilities will never reach the sophistication needed to find and remove these compromises. This is the infrastructure threat that outlasts any war.

10.3 The AI Acceleration Factor

Generative AI is reducing the time between vulnerability discovery and weaponized exploit development. The advantage this provides to offensive actors — particularly well-resourced state actors like China — is compounding quarterly. The defensive gap at Level 0 (physical process layer) is widening.

10.4 The FAE Supply Chain as Permanent Backdoor

Foreign Adversary Equipment (FAE) — Chinese-manufactured components inside U.S. critical infrastructure (transformers, inverters, SCADA controllers, telecommunications equipment) — represents the long-term structural vulnerability that outlasts any kinetic conflict. These components are not removed by military action against Iran. They are not addressed by cyber hygiene programs. They are embedded in the physical infrastructure itself, with potential backdoors at the firmware level that no network monitoring tool can detect. The Diamond Blue certification framework's FAE inventory requirement (Transition tier) directly addresses this threat.

---

11. Attack Timeline Estimate: Iran's Three Tiers — Adjusted for Degradation

The Iranian homeland attack timeline is governed by three constraint layers with distinct restoration timelines. This analysis is subordinated to the China thesis: the Iranian attack timeline affects China's strategic position primarily by determining how long US domestic security bandwidth is consumed.

TIER / TIMING	THREAT VECTOR / ASSESSMENT
TIER 1: NOW (Active)	Lone-actor attacks and pre-activated proxy/hacktivist operations. No Tehran direction required. Austin shooting (Mar 1, 2 killed, 14 wounded) and Toronto boxing gym attack illustrative. CISA at 38% staffing; FBI Iran CI unit degraded.

TIER / TIMING	THREAT VECTOR / ASSESSMENT
TIER 2: 2-4 Weeks (Mar 20 - Apr 9)	IRGC-cleared “Barracks Internet” partially restored. Directed cyber operations against US water/power OT and financial sector DDoS become viable. Dead-man’s-switch architecture already activated (March 9 signal confirmed).
TIER 3: 4-8 Weeks (Late Mar - Late Apr)	New Supreme Leader Mojtaba Khamenei consolidates command authority. Full-spectrum directed operations become viable. Personal motivation (father assassinated) plus religious mandate plus IRGC allegiance = high authorization probability.
CRITICAL VARIABLE	If Russian Sandworm-derived OT tooling transfers to IRGC cyber units via air-gapped channels, Tier 2 operations escalate from nuisance to genuinely destructive.

Tier 1 (Active, ongoing): Fatwa-inspired lone actors, hacktivist DDoS, social media operations, and numbers-station-activated sleeper assets. Active since Day 1. Degraded capability but sustained intent.

Tier 2 (Days to weeks): Coordinated Hezbollah/IRGC cell operations, CyberAv3ngers OT exploitation, and cartel-facilitated physical operations. Partially degraded by war damage but operational capability persists.

Tier 3 (Weeks to months): Sustained infrastructure disruption campaign combining cyber and physical attack vectors. Requires remaining Iranian coordination capability — degraded but not eliminated. The dead-man’s switch architecture means some Tier 3 operations may execute on pre-programmed instructions without ongoing state direction.

---

12. China Constraint Assessment: What Beijing Will and Will Not Do

IRANIAN ACTION	CHINA CONSTRAINT ASSESSMENT
Close Hormuz to Chinese shipping	ACTIVE CONSTRAINT — China’s primary commercial red line.
Spectacular attributable attack on US soil	LIKELY CONSTRAINT — Confirmed attribution would destroy diplomatic leverage.
Deniable cyber attacks on US water/power OT	NO CONSTRAINT — Deniable operations serve China’s interest. Volt Typhoon accesses the same infrastructure.
Proxy/lone-actor attacks on US soil	NO CONSTRAINT — Plausible deniability preserves dynamics. Consumes US domestic security bandwidth.
Continued missile/drone salvoes against US forces	NO CONSTRAINT — Depletes interceptor inventories critical to Taiwan’s defense. China’s ISR improves strike effectiveness.

IRANIAN ACTION	CHINA CONSTRAINT ASSESSMENT
Assassination attempts on fatwa targets	AMBIGUOUS — Attribution would destabilize, but fatwas operate on religious obligation not Chinese signaling.

The Dangerous Paradox: China's constraining influence — keeping Iranian operations deniable and sustained — is more dangerous than either active assistance or full restraint. It strips away attack vectors the US might deter (spectacular attributable events) while keeping open the vectors most useful to China (OT degradation, interceptor attrition, bandwidth consumption). China has optimized Iran's attack posture for Chinese strategic benefit.

Validated by Iran war non-intervention:

China WILL: Continue ISR support through Liaowang-1 and satellite network. Maintain economic relationship with Iran's successor regime regardless of outcome. Pre-position resources (oil, rare earths, technology) for future contingencies. Trade restraint for diplomatic concessions. Maintain Volt Typhoon pre-positioning independent of any diplomatic engagement.

China WILL NOT: Provide lethal weapons to Iran. Intervene militarily to defend Iran, Russia, North Korea, or any other ecosystem partner. Risk secondary sanctions that would damage the Chinese economy. Activate Volt Typhoon unless Beijing determines a Taiwan contingency requires it.

Key finding confirmed: China does not intervene kinetically for partners. Its support is economic, technological, and diplomatic. This means the U.S. cannot deter China's infrastructure pre-positioning by threatening China's partners. The ecosystem's kinetic arm can be degraded; the architect's position improves as a result.

---

13. Consolidated Net Assessment — Key Judgments

On China as Strategic Architect: China has crossed the active-belligerence threshold through intelligence support, not weapons. The Liaowang-1 dataset, MizarVision targeting, and 500-satellite ISR architecture constitute active contribution to lethal operations against U.S. forces. The Iran war is China's most valuable live-fire intelligence collection event in history.

On the Hormuz Proof: The Strait of Hormuz closure is the live-fire validation of the Taiwan LNG coercion thesis. Japan in energy emergency within weeks. Taiwan has 7-11 days of LNG. The proof of concept for China's preferred coercive instrument has been demonstrated at global scale.

On Munitions and Force Posture: THAAD 20-50% expended. PAC-3 MSE ~25%. SM-3 ~20%. Production ramp cannot close the gap within 2026. Pacific carriers redeployed to Middle East. The window of maximum U.S. vulnerability is now — and widening.

On the Diplomatic Dimension: China's leverage grows with every week of war. The "moderation as currency" trap compounds: each crisis creates more opportunities for China to trade restraint for structural concessions on Taiwan.

On Strategic Patience: China's non-intervention in Iran confirms the same pattern as non-intervention in Syria, Venezuela, and Armenia. The ecosystem is transactional, not protective. China's investment portfolio — munitions depletion, intelligence harvest, energy leverage validation, allied distraction — appreciates with every additional day of conflict. Beijing is in no hurry.

On the Enduring Infrastructure Threat: Volt Typhoon is inside U.S. infrastructure. FAE is inside the supply chain. These capabilities are completely independent of the Iran war and will persist regardless of its outcome. Community-level resilience — specifically the FIR Diamond Blue three-tier framework — is the only scalable defense against a threat that is permanent, structural, and embedded in the physical infrastructure of the U.S. homeland.

FINAL ASSESSMENT: China does not need to fire a shot to win the most important battle of the Taiwan question. It needs the Liaowang-1 to keep collecting. It needs Iran to keep expending U.S. interceptors. It needs the Hormuz closure to keep validating the LNG coercion thesis. It needs the domestic threat to keep consuming U.S. security bandwidth. And it needs the FAE supply chain to remain embedded inside U.S. critical infrastructure as the permanent structural backdoor that no kinetic war will remove.

The four-party ecosystem is generating exactly the strategic environment in which China's patient, non-kinetic coercive playbook is most likely to succeed. Whether Beijing designed this outcome or simply recognized and optimized it, the result is the same: a United States militarily stretched, domestically distracted, diplomatically pressured, and facing a Taiwan coercive option it lacks the credible capacity to deter.

---

14. Aggravating Structural Factors

The 16,000-Missile Projection: The IC projects homeland missile threats expanding from 3,000+ to 16,000+ by 2035. This five-fold increase in missile delivery systems provides the long-term strategic context: the infrastructure resilience imperative is not temporary — it is compounding with the threat trajectory.

Coal Plant Retirements and Level 0 Fuel Resilience: The generation mix is shifting from fuel-stockpiled sources (coal: 30-90 day on-site reserves) and fuel-loaded sources (nuclear: 18-24 month cycle) toward just-in-time pipeline-dependent sources (gas: hours of on-site fuel) and grid-reference-dependent sources (solar/wind/battery: stranded by anti-islanding). In 2010, coal + nuclear provided ~65% of US generation with months of fuel independence. By 2025, they provide ~35% and declining. Every coal plant retired moves the grid further from Level 0 fuel resilience — a trend that has not been assessed from a national security resilience perspective.

The Iberian Peninsula Blackout (April 2025): Spain, Portugal, and parts of southern France experienced a sudden cascading grid failure affecting approximately 60 million people. Communications degraded within minutes, transportation paralyzed within hours, water pressure declined within 24-48 hours as backup generators exhausted fuel. The event lasted hours — but confirmed at continental scale that the cascading failure sequence in the FIR Reference Architecture is not theoretical. A BSE extends this validated sequence from hours to months.

2026 Annual Threat Assessment Confirmation: The IC confirms "selective cooperation" bolstering threats while cautioning that "adversary alignment overstates the depth." FIR's framework is consistent: structural alignment producing compounding effects without formal coordination.

Iran War as Aggravating Factor: Every pre-existing structural vulnerability — munitions deficit, force posture gap, allied dependence on Middle East energy, domestic institutional degradation — has been aggravated by the Iran war. The war did not create these vulnerabilities. It accelerated them.

The 16,000-Missile Projection: The IC projects homeland missile threats expanding from 3,000+ to 16,000+ by 2035. The infrastructure resilience imperative is not temporary — it is compounding with the threat trajectory.

---

15. References

All sources are open-source as of March 2026.

Primary Sources

- ODNI, 2026 Annual Threat Assessment
- Carnegie Endowment, "Why Are China and Russia Not Rushing to Help Iran?" March 2026
- U.S.-China Economic and Security Review Commission, China-Iran Fact Sheet, March 2026
- Heritage Foundation, Interceptor Inventory Assessment, January 2026
- CSIS, Taiwan Blockade Wargame Analysis
- IEA, Hormuz Energy Impact Assessment, March 2026
- Dragos, OT Cybersecurity Year in Review 2025
- CrowdStrike, Russian Hacker Surge Assessment, March 2026

Companion FIR Assessments

- FIR, The Four-Party Ecosystem v6.0 (Volume 1)
- FIR, U.S. Critical Infrastructure Vulnerability Assessment v4.0 (Volume 3)

- FIR, U.S. Military Infrastructure Vulnerability Assessment v1.0 (Volume 4)
- FIR, Critical Infrastructure Reference Architecture v5.4
- FIR, Grading Rubric and Scoring System v2.3