Operational Preparation of the Homeland:
Sustaining Airpower and Public Confidence Through Civil-Military Integration

Section 1: The Threat Is Already Inside

The U.S. homeland is already under attack — and not a shot has been fired. Since at least 2019, Chinese state-sponsored cyber actors designated Volt Typhoon have maintained persistent access to American critical infrastructure — power grids, water treatment systems, telecommunications networks, and transportation systems — pre-positioned to disrupt these services at a moment of Beijing's choosing.[1] A second campaign, Salt Typhoon, compromised the backbone infrastructure of at least nine major U.S. telecommunications providers, accessing call metadata, communications content, and even congressional staff emails.[2] These are not espionage operations. They are operational preparation of the environment (OPE) — the deliberate shaping of an adversary's homeland to enable future military operations. This essay argues the USAF must sustain decisive airpower — the nation's primary deterrent — by conducting operational preparation of its own homeland: building the civil-military integration, rehearsed response mechanisms, and collaborative strategies that ensure the force can generate combat power even when the operational environment comes under attack.

This distinction matters. Under the Chinese People's Liberation Army's doctrine of systems confrontation, warfare is understood as a contest between opposing operational systems rather than between fielded military forces.[3] Victory comes not from destroying an enemy's army but from paralyzing the system that allows that army to function — its communications, logistics, energy supply, and command architecture. The Typhoon campaigns follow this logic precisely: pre-position inside the civilian infrastructure that American military power depends on, then hold it at risk to delay or deny U.S. force projection during a crisis. The aim is not to destroy aircraft on the ramp but to collapse the operational environment from which they generate combat power. The intended effect is twofold: degrade the military's ability to project force and erode public confidence that the government can protect essential services — systems paralysis designed to break a population's will to resist.

Joint doctrine already recognizes this dependency. Joint Publication (JP) 1, Volume 1 states plainly that the security and effective operations of U.S. critical infrastructure — including energy, transportation, communication, and the defense industrial base — are essential to mobilize,

---

[1]Cybersecurity and Infrastructure Security Agency (CISA), "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Advisory AA24-038A, February 7, 2024.

[2]CISA, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," Advisory AA25-239A, September 3, 2025.

[3]Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern War* (Santa Monica, CA: RAND Corporation, 2018), 5–7.

project, and sustain joint forces.[4] The 2026 National Defense Strategy elevates the requirement further, directing the Department of War to prioritize bolstering cyber defenses for U.S. military and certain civilian targets as a core line of effort for homeland defense.[5] Air Force Doctrine Publication (AFDP) 3-27, Homeland Operations, acknowledges the threat environment directly: "Malicious cyber activity can degrade communications and temporarily cripple critical infrastructure."[6]

Don't mistake acknowledgment for action. The USAF possesses mature cyber capabilities and the civilian sector has built a sophisticated defense architecture. What is missing is the persistent, doctrinal integration of these two worlds during competition, before contact. If China is conducting OPE against our homeland, the USAF must build the relationships, processes, and exercises with civilian defenders now that will determine whether American airpower can generate combat power when a crisis arrives. No amount of kinetic readiness compensates for an operational environment that collapses before the first sortie launches.

Section 2: The Integration Gap

The United States is not defenseless against this threat. The USAF fields specialized cyber forces through the 16th Air Force, supported by joint doctrine for cyberspace operations. Meanwhile, civilian defenders have organized a parallel architecture of their own. Twenty-eight sector-specific Information Sharing and Analysis Centers (ISACs) operate under the National Council of ISACs, providing real-time threat intelligence to operators across the priority infrastructure sectors.[7] The Cybersecurity and Infrastructure Security Agency (CISA) conducts threat hunting, publishes adversary advisories, and coordinates national response. The architecture for defending critical infrastructure exists on both sides of the civil-military divide. The problem is that these two architectures operate in parallel, not in partnership.

More than 85 percent of U.S. critical infrastructure is owned and operated by the private sector.[8] The military cannot defend what it does not control, and no standing authority compels the Department of War to assume operational control of civilian infrastructure networks. This means that even when military intelligence identifies a specific threat to a specific piece of infrastructure — as it has with Volt Typhoon — translating that awareness into civilian defensive action requires crossing an institutional gap that current doctrine does not bridge. Military threat intelligence is expressed in tactics, techniques, and procedures and mapped to frameworks like MITRE

[4]Joint Publication 1, Vol. 1, *Joint Warfighting* (Washington, DC: Joint Chiefs of Staff, August 27, 2023), V-4.

[5]*2026 National Defense Strategy* (Washington, DC: Department of War, 2026), 17.

[6]Air Force Doctrine Publication 3-27, *Homeland Operations* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, November 21, 2022), 25.

[7]National Council of ISACs, "About ISACs," accessed February 2026.

[8]Brian E. Humphreys, "Critical Infrastructure: Emerging Trends and Policy Considerations for Congress," R45809 (Washington, DC: Congressional Research Service, July 8, 2019).

ATT&CK. Civilian infrastructure operators measure their security against compliance standards like NERC CIP for the energy sector or PCI-DSS for financial systems. In practice, translating a classified threat brief into guidance a civilian power company can execute is not a technology problem — it is a translation problem. These are not just different vocabularies. They reflect fundamentally different ways of understanding the same threat and its effects, and without a codified mechanism to translate between them, classified awareness cannot become unclassified action.

AFDP 3-27 recognizes the threat environment and acknowledges the USAF's role in homeland defense. It states that the department seeks to "preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure" and identifies the military's primary homeland cyber role as defending forward — projecting capability outward to stop threats before they reach their targets.[9] This is necessary but insufficient. Defending forward addresses the adversary's offensive capability but does nothing to harden the domestic infrastructure that the adversary has already penetrated. Air Force doctrine does not prescribe a mechanism for persistent, competition-phase integration between USAF cyber forces and civilian defenders who control the infrastructure Volt Typhoon is already inside.

China is conducting OPE against the American homeland. Yet the United States is not conducting the corresponding function — a joint intelligence preparation of the operational environment — of its own critical infrastructure from the perspective of military dependency. While military and civilian agencies each map portions of this problem independently, no organization currently maintains an integrated product that fuses military capability dependencies — which power grids feed which installations, which telecommunications providers carry command and control traffic, which water systems sustain which bases — with adversary pre-positioning intelligence routed to civilian defenders who control those systems.[10] This essay proposes that the USAF close this gap by adopting what might be called operational preparation of the homeland — the deliberate, continuous process of mapping military capability dependencies, fused with adversary threat intelligence, that drives the civil-military integration needed to defend the operational environment from which the USAF generates combat power. The gap is not capability. The gap is integration, and it needs a doctrinal framework to close it.

Section 3: Shaping Before Contact — The Doctrinal Solution

The doctrinal tools to operationalize this concept already exist. JP 3-57, Joint Civil-Military Operations, establishes a framework for civil-military integration that has been applied extensively in foreign operations — from humanitarian assistance in the Pacific to stability operations in the

[9]AFDP 3-27, *Homeland Operations*, 6.

[10]This framing draws on the joint intelligence preparation of the operational environment process described in Joint Guide, *Joint Intelligence Preparation of the Operational Environment* (Washington, DC: Joint Chiefs of Staff, May 26, 2022).

Middle East. Its mechanisms for civil-military dialogue, alignment, and integration through liaison, working groups, and dedicated coordination centers are proven and scalable.[11] What has not been systematically attempted is applying this framework to the homeland defense mission during competition. AFDP 3-27 must evolve to incorporate this application.

Operational preparation of the homeland would rest on three functional components, grounded in existing joint doctrine.

The first component is a targeted collection function — civil-military integration with the sector-specific defenders who possess the infrastructure knowledge the USAF lacks. The USAF should establish standing liaison relationships with the ISACs most critical to military power projection — energy, communications, defense industrial base, transportation, and water. These relationships cannot be episodic — activated during a crisis and dormant otherwise. They must be persistent, built into the regular coordination cycle of both organizations, with regular threat briefings, shared situational awareness, and mutual understanding of each other's decision-making processes. JP 3-57 describes exactly this kind of relationship: civil-military integration achieved through liaison officers who can explain how their organizations make decisions and identify conditions unfavorable to their operations.[12] Through these relationships, the USAF builds the capability dependency map that no organization currently maintains — the foundation of operational preparation of the homeland.

The second component is a validation function — a joint exercise program that tests whether integrated response mechanisms actually execute under friction. Information sharing sustains awareness; integration sustains resilience. From the dependency map, the USAF and its civilian partners must codify cooperative response mechanisms: communications protocols for military-civilian coordination during disruption; rollover procedures that reroute power and communications to alternate sources when primary pathways fail; warning protocols that link cross-sector indicators into coordinated trigger points; and logistics routes for moving jet fuel and generator fuel to installations under local law enforcement escort and route clearance. Ukraine's experience suggests this approach works: its ability to sustain military operations despite systematic Russian attacks on energy infrastructure came from pre-conflict preparation and rehearsed integrated response, not from improvisation after the first strike.[13] Exercises must simulate simultaneous disruption and then force execution of every codified mechanism under realistic friction, measuring time to restore minimum viable sortie generation and cross-sector indicator-to-action latency — the metrics that define whether integration actually works. The

[11] Joint Publication 3-57, *Joint Civil-Military Operations* (Washington, DC: Joint Chiefs of Staff, April 2, 2025), II-1 to II-4.

[12] JP 3-57, II-4.

[13] NATO Energy Security Centre of Excellence, "Table Top Exercise Coherent Resilience 2020: Hybrid Threats & the Black Sea Region," September 13–17, 2021. European External Action Service, "EU Cybersecurity Exercises in Ukraine," September 2021. See also Paul Nakasone, testimony before the Senate Armed Services Committee, March 7, 2023, describing a U.S. hunt-forward team deployment to Kyiv on December 3, 2021.

objective is not to test whether organizations can talk to each other. It is to prove that the integrated system holds under pressure before it is tested under fire. Venues like the Air Force Doctrine 2035 Wargame offer an immediate opportunity to stress-test this posture: inject concurrent grid instability, telecom compromise, and fuel distribution disruption, then measure whether the force sustains minimum viable sortie generation and executes the civil-military response mechanisms this framework demands.

The third component is a dissemination function — a knowledge translation architecture that converts the products of operational preparation into actionable guidance for both military planners and civilian defenders. Section 2 identified the translation problem between military threat intelligence and civilian compliance frameworks. The solution is not a new technology platform — it is an established process for translating classified military threat awareness into unclassified, sector-specific, actionable defensive guidance — accelerated by emerging capabilities in automated indicator sharing and machine-speed threat detection. JP 3-57 provides the model through civil information management, which it defines as the process of collecting, processing, and disseminating information from civilian organizations and government entities to feed the commander's common operational picture while informing civilian partners.[14] Applied to homeland cyber defense, this means building a two-way translation function: military intelligence on adversary pre-positioning flows outward as actionable guidance to civilian defenders, while civilian infrastructure vulnerability data and threat detections flow inward to inform military operational planning. Civil-military operations centers, as described in JP 3-57, provide the organizational model — a dedicated space for operational cooperation between military forces and civilian partners, distinct from the joint operations center.[15]

These three components share a common characteristic: none of them require new authorities, new technology, or significant new funding. They require doctrinal commitment to applying existing civil-military frameworks to a mission where they have not previously been applied. The cooperation incentive is natural: private infrastructure owners whose networks are already compromised want the threat intelligence military forces possess — formalizing these partnerships through memoranda of agreement requires no enforcement authority, only doctrinal will. The investment is in process and people — the cheapest and most durable form of military capability.

Section 4: Maintaining Decisive Airpower

The purpose of operational preparation of the homeland is not to protect infrastructure — it is to sustain the deterrent. Decisive airpower is the output the joint force commander (JFC) requires; infrastructure matters most where its loss collapses the USAF's ability to generate it. The dependency map proposed in Sections 2 and 3 answers that question precisely — which

[14]JP 3-57, B-1 to B-2.

[15]JP 3-57, II-6.

disruptions are survivable and which are catastrophic. With that map, the USAF can target its resilience investments at the nodes that matter.

Two dependencies underlie every other: power and communications. Without power, there is no sortie generation, no maintenance, no fuel pumping, no weapons loading. Without communications, there is no command and control, no tasking, no intelligence dissemination, no joint integration. Every other mission function cascades from these two. Whether the initiating event is a cyber intrusion, a kinetic strike, sabotage, or coordinated insider attack, the effect converges on these same nodes. USAF installations depend on commercial power, civilian telecommunications, municipal water, and commercial fuel distribution — every one of which is a known Volt Typhoon target.[16] The question is not whether these systems will be attacked in a conflict. The question is whether the USAF has mapped its dependencies precisely enough to know which disruptions are survivable and which collapse the ability to launch, recover, arm, refuel, and retask aircraft with sufficient command-and-control continuity to meet JFC-directed timelines — the minimum viable sortie generation that defines decisive airpower in a degraded environment.

Agile Combat Employment (ACE) distributes forces to complicate adversary targeting — the right strategy — but every dispersed location adds power, communications, and logistics dependencies that must be mapped and managed. The USAF does not need independent power grids at every forward operating site. It needs the dependency map that operational preparation of the homeland produces — and then it needs to ensure the specific power and communications channels essential to sustaining airpower at each location can survive disruption, through backup generation, satellite communications alternatives, or coordinated restoration agreements with civilian providers.[17]

Ukraine demonstrated both the vulnerability and the solution. Russian forces conducted sustained kinetic strikes against Ukrainian energy infrastructure — attacks often preceded by cyber reconnaissance and network disruption — yet Ukraine sustained military operations throughout because it had prepared for degraded conditions before the attacks began — through distributed generation, pre-positioned repair capability, and rehearsed civil-military coordination.[18] The lesson is clear: resilience is cheaper than reconstitution, and preparation during competition is orders of magnitude more effective than improvisation during conflict.

This creates a complete doctrinal posture. Operational preparation of the homeland, as described in Sections 2 and 3, builds the dependency map, fuses it with adversary threat intelligence, and drives the civil-military integration needed to defend the infrastructure that military operations depend on. That same map enables targeted redundancy planning for functions where failure is

[16]CISA Advisory AA24-038A.

[17]This analysis draws on the infrastructure resilience framework in AFDP 3-27, *Homeland Operations*, 25, and the communications resilience principles in JP 6-0, *Joint Communications System* (Washington, DC: Joint Chiefs of Staff, December 4, 2023), I-3 to I-4.

[18]International Energy Agency, *Energy System Resilience: Lessons Learned from Ukraine* (Paris: IEA, February 2026). See also Cybersecurity and Infrastructure Security Agency, "The Power of Resilience," August 20, 2025.

catastrophic — not a call to defend everything, but to fortify and defend what collapses airpower generation first and rehearse how installations fight through loss while restoration proceeds. Neither integration nor resilience alone is sufficient. Together, they ensure the USAF can deliver decisive airpower for the joint force commander even when the operational environment is under attack. A posture that visibly sustains airpower reassures the public, and signals adversaries that disruption will not paralyze the force.

Section 5: Collaborative Strategies

Operational preparation of the homeland cannot be executed by a single organization. It requires a force structure that spans national, state, and local levels — and the USAF already possesses the building blocks.

The Air National Guard (ANG) is the most immediate enabler. ANG cyber units already possess dual-status authority that allows them to operate under both federal Title 10 and state Title 32 authorities — a legal framework uniquely suited to the civil-military integration mission.[19] ANG cyber personnel live in the communities whose infrastructure they would defend. They understand local utility providers, regional telecommunications architectures, and state emergency management structures. Positioning ANG cyber units as embedded liaisons to state-level critical infrastructure defenders and regional ISACs transforms a latent capability into an operational one, without new force structure or authorities. In the framework of operational preparation of the homeland, the ANG provides the distributed collection network — the personnel who build and maintain the dependency map at the regional level.

At the national level, the USAF should leverage its existing relationships with U.S. Cyber Command, the intelligence community, and the Sector Risk Management Agencies (SRMAs) designated to coordinate federal risk across each infrastructure sector. The Defense Cyber Crime Center's Defense Industrial Base Collaborative Information Sharing Environment already demonstrates that military-to-civilian threat sharing can work at scale when the process is designed for the recipient rather than the originator.[20] Extending this model through ISAC and SRMA partnerships would operationalize the dissemination function across priority infrastructure sectors.

Installation commanders represent the local execution layer. Every USAF installation depends on surrounding civilian resources and services. Installation commanders already coordinate with local emergency management agencies for natural disaster response. Expanding this coordination to include cyber threat awareness and capability dependency mapping creates a distributed network

[19]For dual-status authority and ANG cyber operations, see AFDP 3-27, *Homeland Operations*, 17; and DODI 3025.22, *The Use of the National Guard for Defense Support of Civil Authorities.*

[20]Defense Cyber Crime Center, "Defense Industrial Base Collaborative Information Sharing Environment (DCISE)," accessed February 2026.

of civil-military integration points that validates and refines the dependency map with ground truth.

These collaborative strategies build on authorities and relationships that already exist. The doctrinal innovation is not creating new structures. It is organizing existing ones around a function — operational preparation of the homeland — that gives them coherence, purpose, and a shared output. Because capability dependencies cross domain boundaries — a cyber attack on a power grid creates a physical effect that degrades an air domain capability — this is inherently a multi-domain posture, not a single-domain program.

Conclusion

The threat to American military power is not hypothetical — it is pre-positioned and waiting. Chinese cyber actors, and others, have spent years conducting OPE against the American homeland, embedding themselves inside the power grids, telecommunications networks, and water systems that the USAF depends on to generate combat power. The doctrine to respond exists in JP 3-57. The civilian defense architecture exists in ISACs and CISA. What is missing is the mirror function: the USAF's deliberate, persistent operational preparation of its homeland.

This essay has argued that AFDP 3-27 must evolve to incorporate this function — a continuous, competition-phase process of mapping capability dependencies, fused with adversary threat intelligence, that drives the civil-military integration needed to defend and sustain the operational environment from which the USAF generates airpower. The mechanisms are proven. The authorities exist. The need is urgent. What remains is doctrinal commitment — the decision to prepare the homeland before contact rather than scramble to restore it after the first disruption. The connective tissue between military awareness and civilian resilience will not build itself. The USAF must build it now.