One Fight: Integrating Homeland Infrastructure Defense

Tuesday morning at Travis Air Force Base. Dormant malware, embedded for years in the supervisory control and data acquisition systems of the regional power grid, executes. Autonomous AI agents spread the intrusion across dozens of connected systems simultaneously, killing power across the region faster than human operators can respond.[1] Within hours, commercial electricity to the installation drops. Backup generators engage, but GPS signals across Northern California degrade, consistent with spoofing from a vessel offshore. Then more than forty small drones activate from commercial storage facilities less than three miles from the flightline, pre-positioned in shipping containers weeks earlier and invisible to every externally oriented sensor. The wing commander needs to launch AMC aircraft to support the joint force commander's Pacific mobility plan in six hours. But his staff discovers that no single authority connects these threats into a coherent defensive response. The Cybersecurity and Infrastructure Security Agency confirmed in 2024 that a People's Republic of China state-sponsored group known as Volt Typhoon had embedded hidden footholds in the computer systems controlling U.S. energy, water, transportation, and communications networks. Not to steal data, but to hold the ability to disrupt or destroy these systems on command during a future conflict.[2] The 2024 Defense Science Board report warned that the Department of Defense is "dependent on increasingly fragile homeland infrastructure" and that "conflict is effectively underway."[3] Yet AFDP 3-27, Homeland Operations, still frames the problem as a binary of homeland defense versus defense support of civil authorities, with no integrating construct for the combined kinetic and non-kinetic attack that adversaries are already preparing.[4] To close this gap, the USAF should revise AFDP 3-27 to incorporate integrated infrastructure defense doctrine centered on two mechanisms: a Multi-Domain Infrastructure Threat Assessment for operational planning and Homeland Defense Response Conditions for execution. Together, these tools close the doctrinal seam between kinetic and non-kinetic threats, protect the joint force commander's power projection capability, and establish collaborative frameworks with joint and interagency partners.

The Dowding System: Integration as Doctrine

The challenge of defending a homeland against multi-domain attack is not new. In 1940, Britain faced a similar problem. Radar stations, ground observers, anti-aircraft batteries, fighter squadrons, and civil defense teams each operated independently against an adversary who combined all of them into a single campaign. Air Chief Marshal Hugh Dowding's tilted the odds in Britain's favor with a new doctrine. He fielded an integrated system of filter rooms that correlated data from

---

[1] Cybersecurity and Infrastructure Security Agency, National Security Agency, and Federal Bureau of Investigation, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Joint Cybersecurity Advisory AA24-038A, February 7, 2024; Congressional Research Service, "Agentic AI and Cyberattacks," CRS In Focus IF13151, January 2026.

[2] CISA, NSA, and FBI, "PRC State-Sponsored Actors," AA24-038A. CISA assessed that Volt Typhoon actors were pre-positioning for disruption rather than conducting traditional espionage.

[3] Defense Science Board, *Report on Department of Defense Dependencies on Critical Infrastructure*, Executive Summary (Washington, DC: Department of Defense, August 2024), 1.

[4] Air Force Doctrine Publication 3-27, *Homeland Operations* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, November 21, 2022), 1–3.

multiple sensors, sector stations that pre-delegated engagement authority, and a tiered readiness system that escalated defensive posture based on threat indicators.[5]

As historian Stephen Bungay argued, the Dowding System was the decisive advance of the Battle of Britain. Radar was one input to a C2 architecture that fused early warning with engagement authority and civilian coordination.[6] A modern comparison is easy. The sensors exist, as CYBERCOM and CISA monitor cyber threats, NORAD tracks air threats, and the Joint Interagency Task Force 401 is fielding counter-UAS capabilities.[7] The effectors exist in the form of cyber hunt teams, C-UAS systems, defensive counterair fighters, and Air National Guard alert forces. What is missing is Dowding's filter room. No current doctrine connects these elements into a single defensive architecture with pre-delegated authorities and tiered response protocols.

Divided Defense Against Integrated Attack

Five Air Force doctrine publications address five aspects of homeland infrastructure defense. No publication addresses the integrated threat.

AFDP 3-27, published in November 2022, organizes homeland operations around the two principles of homeland defense and defense support of civil authorities.[8] The publication's treatment of homeland defense is built almost entirely around NORAD's air sovereignty mission, which largely consists of intercepting unknown aircraft and managing air patrols. Its treatment of DSCA is centered on natural disasters and CBRN incidents. The threat framework assumes either a traditional military attack or a civilian emergency but does not account for the gray-zone operations that characterize the current threat. Volt Typhoon's cyber pre-positioning is simultaneously espionage, preparation of the operational environment, and an act short of armed conflict, but the publication lacks a paradigm for an attack designed to blur every boundary the doctrine relies upon. Worse, the framing documents it cites (the 2021 Interim National Security Strategic Guidance and the 2007 National Strategy for Homeland Security) predate the threats that now define the problem. Volt Typhoon (or similar gray-zone cyber threats) are ignored entirely. So is the counter-UAS imperative that drove JIATF-401's creation and the infrastructure vulnerabilities recognized in the DSB.[9]

The subordinate publications splinter the problem further. AFDP 3-01, Counterair Operations, frames defensive counterair entirely as a theater mission, and if one searches for homeland air

---

[5] Stephen Bungay, *The Most Dangerous Enemy: A History of the Battle of Britain* (London: Aurum Press, 2000), 61–69.

[6] Bungay, *The Most Dangerous Enemy*, 63.

[7] Secretary of Defense Pete Hegseth, "Establishment of Joint Interagency Task Force 401," memorandum (Washington, DC: Department of Defense, August 28, 2025).

[8] AFDP 3-27, *Homeland Operations*, 1–6. The publication's Chapter 1 defines homeland operations through the binary of homeland defense and DSCA, with homeland defense addressed almost exclusively through NORAD air sovereignty missions and DSCA organized around natural disasters, CBRN incidents, and national special security events.

[9] AFDP 3-27, *Homeland Operations*, 1–2, 4–6. The publication references the 2021 Interim National Security Strategic Guidance and the 2007 National Strategy for Homeland Security as its foundational framing documents.

defense, the publication points to NORAD and stops there.[10] It elides the mass low-cost drone defense and the ugly math of a hundred-million-dollar fighter being killed on the ramp by a ten-thousand-dollar loitering munition. AFDP 3-12, Cyberspace Operations, at least concedes that the Air Force depends on civilian infrastructure, but goes no further. There is no operational outline for defending that infrastructure alongside kinetic threat response, and the idea that cyber pre-positioning might serve as the opening act for a kinetic attack simply does not appear.[11] AFDP 3-10, Force Protection, draws its doctrinal boundary at the installation perimeter even though the JIATF-401 guidance pushed counter-UAS authorities beyond it.[12] AFDP 3-85, Electromagnetic Spectrum Operations, addresses theater-level EMS operations but does not connect GPS spoofing or communications jamming to homeland infrastructure defense.[13]

Fragmentation is dangerous because adversaries do not fragment their attacks. Russia's campaign against Ukrainian infrastructure integrates cyber operations against SCADA systems, EW to degrade air defenses, drone swarms exceeding five thousand per month by late 2025, and cruise missiles targeting high-value nodes. Moscow executed one campaign across four domains.[14] On the other side, Ukraine's Operation Spiderweb should alarm anyone responsible for homeland defense. The Security Service of Ukraine hid 117 FPV drones inside containers, loaded them onto trucks, and drove them deep into Russian territory. They then launched all of them against five air bases spread across five time zones, wrecking more than forty bombers on the ground at an estimated seven billion dollars in damage.[15] Not a single sensor saw it coming. An adversary intelligence service could copycat Spiderweb against installations within the U.S. homeland using commercial shipping containers and storage facilities. Meanwhile, agentic AI systems have already demonstrated the ability to conduct large-scale cyber campaigns autonomously, operating at speeds no human defensive team can match.[16] And the pace of improvement is exponential. The complexity of tasks AI agents can complete autonomously has been doubling approximately every

---

[10] Air Force Doctrine Publication 3-01, *Counterair Operations* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, June 15, 2023).

[11] Air Force Doctrine Publication 3-12, *Cyberspace Operations* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, February 1, 2023), 5. AFDP 3-12 acknowledges that "The Air Force depends on US critical infrastructure and key resources (CI/KR) for many of its activities" but provides no operational framework for defending civilian infrastructure in coordination with kinetic threat response.

[12] Air Force Doctrine Publication 3-10, *Force Protection* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, June 1, 2023); "JIATF-401 Announces Updated Guidance to Counter Drone Threats in the Homeland," Department of War press release, January 6, 2026.

[13] Air Force Doctrine Publication 3-85, *Electromagnetic Spectrum Operations* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, November 15, 2023). AFDP 3-85 is organized entirely around theater-level Joint Electromagnetic Spectrum Operations; it contains no homeland-specific EMS defense content.

[14] Center for Strategic and International Studies, "Russia's Intense Air Campaign in October," CSIS Missile Defense Project analysis, February 2026. In October 2025 Russia launched approximately 5,300 Shahed-type UAVs, 74 cruise missiles, and 148 ballistic missiles against Ukrainian infrastructure.

[15] Center for Strategic and International Studies, "How Ukraine's Spider's Web Operation Redefines Asymmetric Warfare," CSIS analysis, February 2026. On June 1, 2025, the Security Service of Ukraine launched 117 FPV drones from trucks concealed within Russian territory, striking five air bases across five time zones and damaging over forty strategic aircraft.

[16] Congressional Research Service, "Agentic AI and Cyberattacks," CRS In Focus IF13151, January 2026. CRS noted that agentic AI systems now allow threat actors to perform tasks that normally require teams of sophisticated hackers, democratizing nation-state-level attack capability.

seven months, with the trend accelerating such that AI systems that could barely string a paragraph together in 2019 can now independently execute multi-hour technical operations.[17] China's Volt Typhoon represents a harrowing convergence of kinetic and non-kinetic, particularly when augmented by AI. A hyper-capable cyber offensive teeing up a kinetic campaign designed to prevent U.S. forces from deploying is unfortunately not the stuff of science fiction. As the DSB concluded, adversaries have moved past simple competition to campaigns that disrupt civilian infrastructure on which DoD depends.[18] The adversary has integrated its attack. The question is whether USAF doctrine will integrate its defense.

Two Mechanisms for Integrated Defense

The systems theorist Donella Meadows argued that the most effective interventions in complex systems target information flows and system rules rather than individual components.[19] The homeland defense problem is a systems problem insofar as five doctrine publications optimize for their respective domains, but system-level integrated defense is neglected. The two mechanisms proposed here aim to fill this gap. The Multi-Domain Infrastructure Threat Assessment creates the missing information flow while the Homeland Defense Response Conditions create the missing system rule.

Multi-Domain Infrastructure Threat Assessment. The MDITA is a required planning product, analogous to how joint intelligence preparation of the operational environment is required for operational planning, that integrates infrastructure analysis across domains. It should be embedded as a new section in AFDP 3-27 and cross-referenced in AFDP 5-0 as a required input for any operation dependent on force generation from the homeland.[20]

An MDITA contains five elements. First, an infrastructure dependency map identifying the critical civilian infrastructure on which each installation supporting JFC force generation depends (power, water, fuel, communications, and GPS).[21] Second, a combined threat analysis identifying kinetic (drones, cruise missiles, sabotage, interior pre-positioned threats on the Spiderweb model) and non-kinetic vulnerabilities (cyber intrusion, agentic AI exploitation, EMS disruption) for each dependency, analyzed as a combined set. Third, correlation indicators (e.g., criteria that can assist a commander in determining if nefarious activity in the power grid and drone activity near the base are coincidental or organized). Fourth, a responsibility matrix that answers, before a crisis, which organization defends which piece of infrastructure against which threat (the question the DSB

---

[17] Model Evaluation and Threat Research, "Measuring AI Ability to Complete Long Tasks," METR research paper, March 2025, updated January 2026.

[18] DSB, *Dependencies on Critical Infrastructure*, 1. The Task Force concluded that "the distinction between 'competition' and 'conflict' is not serving the Department well."

[19] Donella H. Meadows, *Thinking in Systems: A Primer*, ed. Diana Wright (White River Junction, VT: Chelsea Green Publishing, 2008), 145–165.

[20] Air Force Doctrine Publication 5-0, *Planning* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, January 22, 2025).

[21] DSB, *Dependencies on Critical Infrastructure*, 1–2.

found no one could currently answer).[22] Fifth, a power projection impact assessment quantifying how each dependency's degradation affects force generation.

A Travis AFB example illustrates the concept. The MDITA would map Travis's dependence on Pacific Gas and Electric's regional grid, catalog both the cyber vectors (Volt Typhoon access to PG&E's SCADA systems) and kinetic vectors (pre-positioned drones targeting the Vacaville substation three miles from the base), identify the correlated indicator (simultaneous Volt Typhoon activation and anomalous drone sightings near the installation), assign defensive responsibilities (CISA leads grid cyber defense, JIATF-401 leads C-UAS, the wing handles installation protection), and quantify the impact: if Travis loses commercial power for seventy-two hours, how many AMC sorties supporting the Pacific mobility plan are lost? That number transforms homeland infrastructure defense from an abstract concept into the joint force commander's operational problem.

Homeland Defense Response Conditions. The HDRC is a tiered posture framework modeled on DEFCON, FPCON, and INFOCON which are constructs every Airman already understands. Its purpose is to pre-authorize defensive actions across domains when threat indicator thresholds are met, replacing the current patchwork in which commanders must address separate authority chains at different speeds when an attack spans multiple domains. It operates across four tiers.

Tier	Trigger	Key Actions	Power Projection Link
HDRC-4: Normal	No cross-domain indicators active	MDITAs current; routine monitoring through existing channels	Baseline force generation posture
HDRC-3: Elevated	Cross-domain correlation indicators detected	Elevated C-UAS posture; cyber hunt-forward with CISA; civilian infrastructure coordination cells activated	Contingency planning for degraded ops; interceptor inventory preserved
HDRC-2: Imminent	Confirmed hostile activity in multiple domains, same region	Pre-delegated C-UAS authorities active; ANG DCA elevated; Homeland ACE dispersal; NORTHCOM/CYBERCOM/CISA joint coordination	JFC assets disperse to alternate locations; backup power/comms activated
HDRC-1: Active Attack	Confirmed kinetic/non-kinetic effects on homeland infrastructure	Full HD authorities; ANG activation; engineer rapid repair; full interagency coordination under NRF	Alternative force generation sites; contested departure; restoration prioritized by JFC requirements

HDRC-4, Normal, represents the baseline: MDITAs are current and routine monitoring continues through existing channels. HDRC-3, Elevated, triggers when cross-domain correlation indicators are detected. Example actions include elevated C-UAS posture, cyber hunt-forward coordination with CISA, and, importantly, activation of coordination cells with regional civilian infrastructure operators to build working relationships before a crisis. HDRC-2, Imminent, triggers when confirmed hostile activity is detected in multiple domains targeting the same region. Pre-delegated C-UAS engagement authorities activate per JIATF-401 guidance, ANG defensive counterair alert posture elevates, and Agile Combat Employment dispersal planning initiates for power-projection

[22] DSB, *Dependencies on Critical Infrastructure*, 1–2. The DSB recommended that DoD "normalize engagement between installation commanders and civilian infrastructure operators."

forces.[23] HDRC-1, Active Attack, triggers full homeland defense authorities. ANG activation, engineer rapid repair forces, contested departure procedures, and full interagency coordination under the National Response Framework.

Every HDRC tier explicitly includes power projection protection measures because the joint force commander's force generation is the organizing principle. HDRC-3 identifies at-risk installations and begins contingency planning. HDRC-2 initiates dispersal, extending the Agile Combat Employment concept to the homeland context, just as Ukrainian air forces have sustained operations under daily bombardment by dispersing to pre-planned sites. HDRC-1 activates alternative force generation sites and contested departure procedures. The USAF maintains decisive airpower while defending homeland infrastructure by treating homeland defense as a precondition for power projection instead of a choice between the two.

Protecting the Joint Force Commander's Fight

China's and Russia's homeland attack doctrines are not designed to conquer U.S. territory. Rather, they are designed to prevent U.S. power projection. If Volt Typhoon degrades the commercial power feeding Travis Air Force Base, the adversary gains nearly as much as if it had sunk the airlift fleet altogether. If mass drone attacks force the USAF to divert combat aircraft to fly defensive counterair over the homeland, the adversary wins without firing a shot in the Pacific. AFDP 3-27's definition of the homeland includes Guam, the Northern Mariana Islands, and other territories that function simultaneously as homeland installations and forward power projection platforms in INDOPACOM.[24] If agentic AI systems launch a coordinated denial-of-service attack against Guam's power utility and telecommunications providers, the result is both a homeland infrastructure crisis and the loss of the joint force commander's primary Pacific staging base. The distinction between homeland defense and power projection collapses entirely at Andersen Air Force Base.

The MDITA's power projection impact assessment ensures planners know which infrastructure failures degrade which capabilities, enabling targeted hardening rather than the trap of defending everything and therefore defending nothing. The HDRC allocates proportional responses (e.g., directed energy and drone interceptors for mass low-cost threats at HDRC-2, or conventional air and missile defense only at HDRC-1 against confirmed high-end threats) preserving the joint force commander's theater interceptor inventory rather than expending four-million-dollar Patriot missiles against thirty-thousand-dollar drones over the homeland.[25] The Homeland ACE concept at HDRC-2 ensures that when Travis faces attack, AMC tankers and C-17s disperse to pre-coordinated alternate airfields, maintaining the Pacific mobility timeline from distributed locations rather than a single vulnerable hub, just as Ukrainian air forces have sustained operations under constant bombardment.

---

[23] Air Force Doctrine Note 1-21, *Agile Combat Employment* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, December 1, 2022).

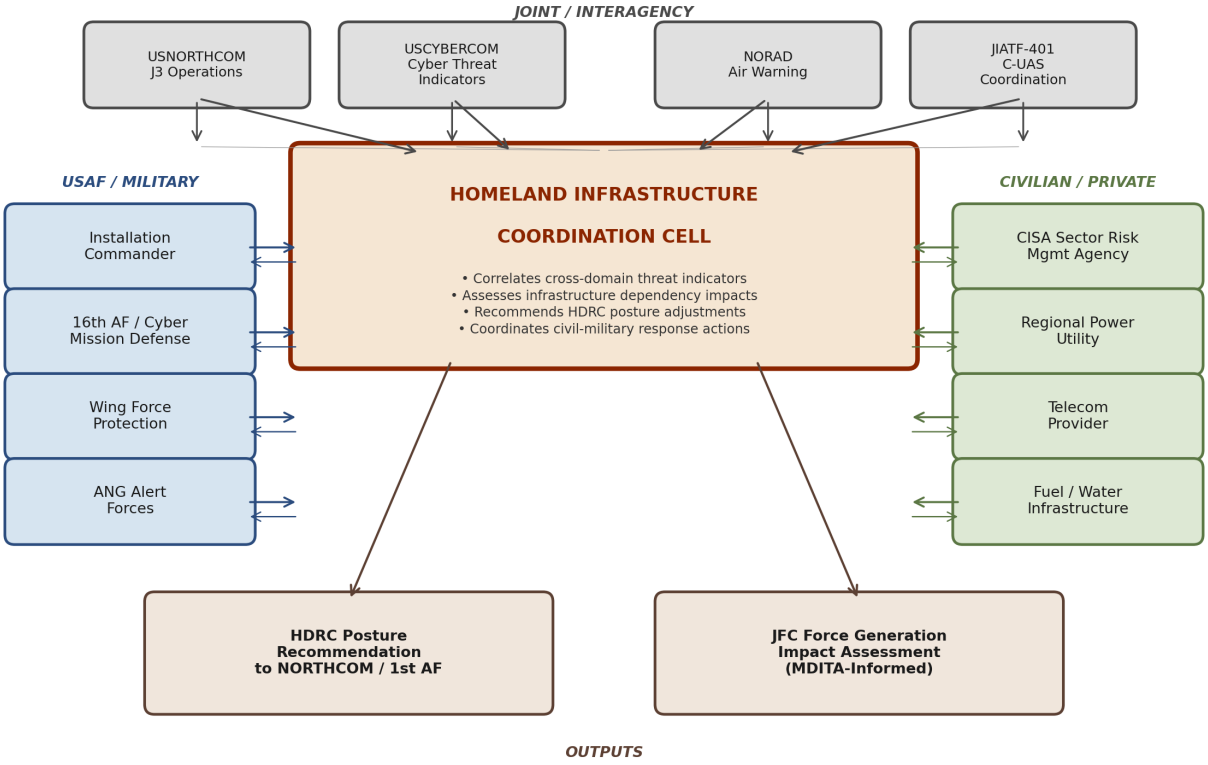
[24] AFDP 3-27, *Homeland Operations*, 2. AFDP 3-27 defines the homeland as "the 50 states, four territories, and numerous island possessions," explicitly including Guam and other USINDOPACOM territories.

[25] Congressional Research Service, "Russia's War Against Ukraine: Air Campaign," CRS In Focus, updated January 2026. Shahed-type one-way attack drones cost an estimated $30,000–$50,000 per unit; a Patriot PAC-3 interceptor costs approximately $4 million.

Collaborative Strategies for Multi-Domain Defense

The MDITA and HDRC are designed as shared frameworks. Because its infrastructure dependency mapping requires data from civilian entities, the MDITA cannot be completed by the Air Force alone. This creates a standing civil-military planning relationship rather than crisis-response improvisation. The DSB specifically recommended normalizing engagement between installation commanders and civilian infrastructure operators; the MDITA codifies that recommendation in doctrine.[26] Dowding's system succeeded because it integrated civilian Observer Corps volunteers with military operators as permanent elements of the same architecture. The MDITA makes civilian infrastructure operators participants in homeland defense planning on the same model.

Figure 1. Homeland Infrastructure Coordination Cell (HDRC-3 Activation)



Activated at HDRC-3 (Elevated). The coordination cell integrates military and civilian participants around MDITA-identified infrastructure dependencies, enabling unified cross-domain threat assessment and pre-authorized collaborative response.

The HDRC framework is designed for joint adoption. While this essay recommends initial codification in AFDP 3-27, the HDRC tiers align with NORTHCOM's homeland defense mission and should ultimately be proposed for inclusion in JP 3-27 and JP 3-28. Joint integration points exist at every tier. Army air and missile defense under NORTHCOM provides ground-based fires

---

[26] DSB, *Dependencies on Critical Infrastructure*, 1–2. The DSB specifically recommended standing coordination mechanisms between DoD installations and the private-sector entities that own the infrastructure the military depends on.

at HDRC-2 and HDRC-1, CYBERCOM provides cyber threat indicators feeding HDRC trigger assessment, Navy and Coast Guard provide maritime domain awareness for offshore EMS threats, and JIATF-401 coordinates C-UAS across all services. Ukraine's experience demonstrates that public communication during sustained infrastructure attacks is a strategic function. Accordingly, each HDRC tier should include a communication coordination element linking AFDP 3-61 and AFDP 3-13 to ensure coherent messaging and counter adversary disinformation while maintaining the will of the populace to prevail.

Challenges and Counterarguments

Three objections deserve address. First, expanding military planning to include civilian infrastructure raises concerns about Posse Comitatus and military overreach. The MDITA is a planning product, not an operational authority. The HDRC's interagency triggers ensure civilian agencies retain the lead for civilian infrastructure while military authorities apply only to installation defense and force generation protection. Dowding's system integrated Civil Defence without militarizing British society.

Second, dedicating forces to homeland defense competes with the joint force commander's forward requirements. This is the false dichotomy the essay rejects. If homeland infrastructure is degraded, the joint force commander does not receive forces at all.[27] The MDITA enables efficient allocation by identifying which infrastructure truly matters for power projection, preventing the trap of defending everything.

Third, interagency friction is real. The HDRC does not subordinate civilian agencies. Instead, it establishes coordination triggers at defined thresholds following the National Response Framework model. The MDITA's collaborative development builds relationships in peacetime, and the DSB specifically recommended exactly this type of engagement.[28]

Doctrinal Recommendations

This essay recommends five specific doctrinal actions. First, revise AFDP 3-27 to add a chapter on integrated homeland infrastructure defense that replaces the binary homeland defense/DSCA framework with a spectrum addressing gray-zone infrastructure threats, incorporates the MDITA as a required planning product, and establishes the HDRC framework. Second, amend AFDP 3-01 to include a homeland defensive counterair section addressing mass drone defense and integration with non-kinetic threat indicators. Third, amend AFDP 3-12 to recognize cyber pre-positioning as a distinct threat category requiring coordination with air defense and force protection. Fourth, amend AFDP 5-0 to require the MDITA as an input for operations dependent on homeland force generation. Fifth, amend AFDP 3-10 to extend the doctrinal aperture beyond the installation perimeter to include infrastructure dependencies identified in the MDITA and interior pre-positioned threats demonstrated by Operation Spiderweb.

Conclusion

---

[27] DSB, *Dependencies on Critical Infrastructure*, 1.

[28] DSB, *Dependencies on Critical Infrastructure*, 1–2.

Return to Travis Air Force Base. The same wing commander faces the same Tuesday morning, but now he has a current MDITA that mapped regional infrastructure dependencies six months ago. Cross-domain indicators were correlated at HDRC-3 two days earlier when Volt Typhoon signatures appeared alongside anomalous UAS activity. By the time the drone swarm activates from those nearby storage facilities, pre-delegated C-UAS authorities are already active, AMC aircraft are dispersing to alternate departure points, and CISA is coordinating with Pacific Gas and Electric on grid restoration priorities informed by the military's power projection requirements. The joint force commander's mobility plan stays on schedule.

The adversary has integrated its attack. Russia demonstrated it in Ukraine. China has pre-positioned for it across the American homeland. The MDITA and HDRC are the doctrinal mechanisms to integrate the defense, and they can be drafted tomorrow and implemented within the current AFDP 3-27 revision cycle. You cannot project power from a burning ramp. It is time AFDP 3-27 reflected that.