Force Generation Under Fire: The Homeland Is Not A Sanctuary

DISCLAIMER: The opinions expressed in this essay are those of the author and do not necessarily reflect the official policy or position of the Department of Defense or any other U.S. Government agencies

Introduction: The End of Sanctuary

For much of the post–Cold War era, the United States treated the homeland as a secure rear area, something of an unquestioned foundation from which combat power could be generated and projected abroad. That assumption no longer holds. Modern conflict no longer confines disruption to distant theaters. Energy grids, communications networks, water/wastewater management, transportation, logistics systems, and digital infrastructure have become operational terrain. In an era of peer competition, the systems that enable force generation are themselves targets.

Russia's sustained strikes against Ukrainian energy infrastructure demonstrate that modern warfare extends beyond battlefield attrition into systemic disruption.[1] Meanwhile, China's military modernization emphasizes rapid, multi-domain operations designed to achieve decisive outcomes before external powers can fully mobilize. Time has reemerged as the decisive variable. The objective is not necessarily destruction, but slowing response, compressing decision windows, and shaping political calculations.

The Joint Force relies on resilient national infrastructure to generate and project airpower. Yet much of that infrastructure lies outside direct military control and within fragmented public-private governance structures. Comprehensive protection is neither fiscally nor structurally feasible. The question is not whether disruption will occur, but whether combat power can be sustained despite it.

As peer competition intensifies, the Air Force must doctrinally normalize the homeland as contested and institutionalize a framework of Sense–Absorb–Project (SAP). By prioritizing early detection, degraded-mode resilience, and continuity of force generation, the United States can deny adversaries the strategic advantage of time and preserve decisive airpower under pressure.

Infrastructure and Force Generation in Modern Conflict

Airpower is often discussed in terms of weapon systems, munitions, and trained personnel. Yet none of these capabilities can be employed at scale without the infrastructure that enables them. Electrical power sustains command centers, maintenance facilities, and fuel distribution systems.

[1] United Nations Human Rights Monitoring Mission in Ukraine, "Attacks on Ukraine's Energy Infrastructure," 2023.

Communications networks enable intelligence fusion and synchronized decision-making. Transportation systems move personnel and equipment from air base to theater. Digital networks, including industrial control systems, underpin logistics tracking and installation operations. These systems form the connective tissue of force generation. When degraded, sortie generation slows, command coherence frays, and operational tempo declines. Modern infrastructure is characterized by interdependence of all systems. The United States formally recognizes sixteen critical infrastructure sectors whose integrated operations enable national power while simultaneously creating pathways for cascading failure.[2] Power disruptions affect communications; communications interruptions degrade logistics visibility; cyber intrusions targeting industrial control systems can halt fuel pumps or disable maintenance databases. Because infrastructure sectors are optimized for interconnectedness, localized disruption can produce cascading effects. Even the USS *Gerald R. Ford*, one of the most advanced warships ever built, has encountered fundamental infrastructure issues, with its vacuum-based sewage system repeatedly clogging and failing during extended deployments. This shows that high-end technological prowess can be undermined by basic system reliability problems.[3]

The Russia–Ukraine war provides a contemporary case study in operating under sustained infrastructure pressure. Since 2022, Russian forces have conducted repeated strike campaigns against Ukraine's energy grid, substations, and transportation networks.[4] Winter strike campaigns resulted in marked losses in generation capacity, affecting national resilience and military sustainment alike.[5] International observers reported that attacks on electrical infrastructure produced downstream failures in water systems, heating networks, and rail transport, revealing the cascading nature of interconnected infrastructure.[6] Cyber activities coincided with kinetic strikes on Ukrainian infrastructure, illustrating the convergence of physical and digital operations in contemporary warfare.[7]

Yet Ukraine's armed forces continue to generate combat power. Military effectiveness was preserved not by preventing all damage, but by prioritizing essential functions, restoring critical

---

[2] Cybersecurity and Infrastructure Security Agency (CISA), National Infrastructure Protection Plan, 2023, https://www.cisa.gov/national-infrastructure-protection-plan

[3] Jay Hilotin, "'Sewage Crisis' Hits USS Gerald Ford Aircraft Carrier: Report," Gulf News, February 23, 2026, https://gulfnews.com/world/americas/sewage-crisis-hits-uss-gerald-ford-aircraft-carrier-report-1.500452069

[4] Reuters, "Russia Pummels Ukraine's Power Grid," February 17, 2026.

[5] International Energy Agency, Ukraine's Energy System Under Attack, 2023, https://www.iea.org/reports/ukraines-energy-system-under-attack

[6] United Nations Human Rights Monitoring Mission in Ukraine, "Attacks on Ukraine's Energy Infrastructure Harm Civilian Population," 2023, https://ukraine.un.org

[7] Microsoft, Microsoft Digital Defense Report, 2023.

systems rapidly, dispersing capabilities, and operating in degraded modes. Infrastructure resilience became a determinant of endurance. The lesson is that military effectiveness depends on sustaining operations despite disruption. This dynamic is consistent with broader peer-competitor thinking. The U.S. assessed that China's modernization efforts emphasize integrated, multi-domain operations designed to disrupt command, control, communications, and logistics systems in a Taiwan contingency.[8] Rather than seeking platform-on-platform annihilation alone, adversaries increasingly pursue systemic friction.

Infrastructure warfare, therefore, aims to impose a tempo disadvantage rather than an immediate collapse. If force generation relies upon interconnected civilian systems, homeland defense doctrine must assume those systems will be contested. The strategic challenge is not comprehensive protection of every node, but preservation of operational tempo when nodes fail.

The Coordination Constraint

Defending national critical infrastructure presents a structural challenge that extends beyond military capability. Unlike traditional defense domains, the majority of U.S. critical infrastructure is privately owned and governed through a patchwork of federal, state, local, and regulatory authorities. This fragmentation complicates unified defensive action during crisis and limits the Air Force's authority over many systems upon which force generation depends.

The scale of the challenge is compounded by decades of underinvestment. The American Society of Civil Engineers' 2025 Infrastructure Report Card estimates a multitrillion-dollar gap between current funding levels and what is required to bring U.S. infrastructure to a state of good repair.[9] While recent legislation has improved funding levels, significant modernization gaps remain. Attempting to comprehensively harden or defend all infrastructure nodes against peer adversaries would exceed available resources and statutory authorities.

Coordination across agencies further complicates the problem. Homeland defense involves the Department of Defense, the Department of Homeland Security, the Department of Energy, state authorities, private utilities, and industry operators. Each entity operates under distinct legal mandates and operational cultures. The decisive weakness in complex organizations is rarely capacity itself, but the inability to synchronize distributed elements under pressure.[10] The United States possesses significant infrastructure resilience assets, cyber defense capabilities, and

---

[8] U.S. Department of Defense, Military and Security Developments Involving the People's Republic of China 2025, https://www.defense.gov

[9] American Society of Civil Engineers, *2025 Infrastructure Report Card* (Reston, VA: ASCE, 2025).

[10] Stanley McChrystal and Anna Butrico, *Risk: A User's Guide* (New York: Portfolio/Penguin, 2021).

emergency response mechanisms. The challenge lies in aligning them coherently under time, pressure, and uncertainty.

Centralizing infrastructure control under federal authority would neither be feasible nor desirable. The diversity and distributed nature of U.S. infrastructure, more often a vulnerability, also creates resilience. Over-centralization risks bureaucratic delay and single points of failure. The Department of Defense's Mission Assurance Strategy already emphasizes identifying and prioritizing critical assets necessary for mission success rather than attempting universal protection.[11] This prioritization logic provides a foundation for doctrinal refinement.

Recognizing this constraint makes resilience a design principle rather than a reactive measure. If infrastructure cannot be fully secured and coordination cannot be perfectly centralized, the only viable approach is to ensure that military effectiveness persists despite those realities.

Sense–Absorb–Project (SAP): A Force-Generation Framework

Preserving airpower in a contested homeland requires more than infrastructure protection; it requires continuity of force generation under degraded conditions. Sense–Absorb–Project (SAP) provides a doctrinal framework grounded in resilience science, mission assurance policy, and fiscal realism. Rather than attempting comprehensive infrastructure defense, SAP prioritizes detection, degradation tolerance, and sustained projection of combat power.

Sense: Early Detection and System Awareness

Effective resilience begins with visibility. Modern infrastructure systems are deeply interdependent, and early anomalies often signal broader systemic stress. The National Institute of Standards and Technology (NIST) approach to cybersecurity underscores detection as essential to anticipating and mitigating systemic risk.[12] By mapping adversary techniques against industrial control systems, the ATT&CK framework underscores how operational technology becomes a gateway to cascading systemic disruption.[13] Recognizing uncertainty converts unforeseen risks into identifiable challenges, allowing organizations to adapt proactively.[14] Applied to force generation, this means fusing indicators from cyber defense, energy stability, transportation anomalies, and space-enabled interference into actionable warning. By institutionalizing cross-domain sensing, the Air Force can identify friction before it cascades into operational paralysis.

Absorb: Resilience Through Degraded Operations

---

[11] U.S. Department of Defense, Mission Assurance Strategy, 2023.
[12] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.
[13] MITRE, *ATT&CK for Industrial Control Systems*, https://attack.mitre.org
[14] Dylan Evans, *Risk Intelligence* (New York: Free Press, 2012).

Scientific research on infrastructure resilience consistently emphasizes that complex systems cannot be rendered invulnerable; they must instead be designed to absorb shock and recover rapidly. RAND defines resilience as the capacity to withstand, adapt to, and recover from disruption while maintaining critical functionality.[15] The Department of Energy similarly highlights grid resilience as a function of redundancy, segmentation, and restoration capability rather than absolute protection.[16]

The lesson Russia–Ukraine war shows is clear: resilience preserves operational tempo even when infrastructure damage occurs. Absorption must be selective and mission-focused. Installation-level degraded operating states, backup power prioritization for sortie-generation nodes, and rapid ICS restoration protocols offer far greater return on investment than universal fortification. Absorb accepts that disruption will occur and ensures it does not translate into mission failure.

Project: Sustaining Combat Power Under Pressure

The ultimate measure of resilience is continuity of combat power. Project ensures that force generation and deployment persist despite infrastructure degradation. Joint Publication 4-0 emphasizes sustainment as foundational to operational reach.[17] If sustainment flows continue, albeit at reduced efficiency, operational tempo can be preserved.

Adversaries can weaponize time to offset conventional disadvantages, delaying stronger opponents until strategic conditions shift.[18] Preserving sortie generation and deployment timelines denies adversaries the temporal advantage they seek. SAP's Project pillar integrates distributed command and control, mission-type orders, and prioritized sustainment under degraded conditions. It aligns with modernization investments already present in the FY26 Department of the Air Force budget, including survivable command and control systems and next-generation air dominance capabilities.[19] Rather than demanding expansive new spending, SAP ensures existing investments are doctrinally integrated toward continuity of force generation.

The Strategic Logic of SAP

SAP is an operational tempo doctrine. It recognizes that infrastructure vulnerability cannot be eliminated and that coordination constraints limit comprehensive protection. Instead, it aligns sensing, resilience, and projection around mission continuity. By preserving tempo, SAP transforms resilience into deterrence by denial. Adversaries may disrupt nodes, but they cannot paralyze force generation. In a contested homeland, the decisive question is not whether disruption occurs, but whether combat power endures.

---

[15] RAND Corporation, *Infrastructure Resilience Studies*, https://www.rand.org.
[16] U.S. Department of Energy, *Grid Modernization and Resilience*, https://www.energy.gov.
[17] Joint Chiefs of Staff, Joint Publication 4-0, Logistics (Washington, DC: JCS, 2019).
[18] Sean McFate, *The New Rules of War* (New York: William Morrow, 2020).
[19] Department of the Air Force, *FY26 President's Budget Request*, 2025.

Contemporary Threat Environment and Strategic Reality

The most plausible peer-contingency confronting the United States is not sustained homeland war, but a rapid, regionally concentrated campaign centered on Taiwan. The People's Republic of China (PRC) has oriented military modernization toward preventing Taiwanese independence and deterring or defeating U.S. intervention.[20] The Department of Defense assesses that the People's Liberation Army (PLA) is preparing for high-intensity joint operations intended to achieve objectives quickly before external powers can fully mobilize.[21]

Chinese strategic thought contains a tension between protraction and speed. Mao Zedong's theory of protracted war, articulated during the struggle against nationalists, Japan, and nationalists again, emphasized endurance, dispersion, and the strategic use of time.[22] Like Fabian strategy, Mao's approach traded space for time, allowing a weaker force to exhaust a stronger adversary through sustained resistance. Time was the decisive variable.

In a Taiwan contingency, however, time would likely favor the defender and its external supporters. Protracted conflict increases the probability of U.S. mobilization, allied intervention, economic sanctions, and maritime isolation. Allowing Taiwan to implement a modern Fabian defense: dispersing forces, extending resistance, and internationalizing the conflict. This would invert Mao's historical advantage and China is well aware of that.

Consequently, contemporary PLA modernization appears oriented toward speed and concentration consistent with elements of *Niederwerfungsstrategie*, a strategy of decisive annihilation, and *Gesamtschlacht*, the concentrated operation designed to produce rapid political decision.[23] Prussian military theory, refined in the nineteenth century, emphasized the rapid concentration of force to deliver decisive blows before an adversary could complete mobilization.

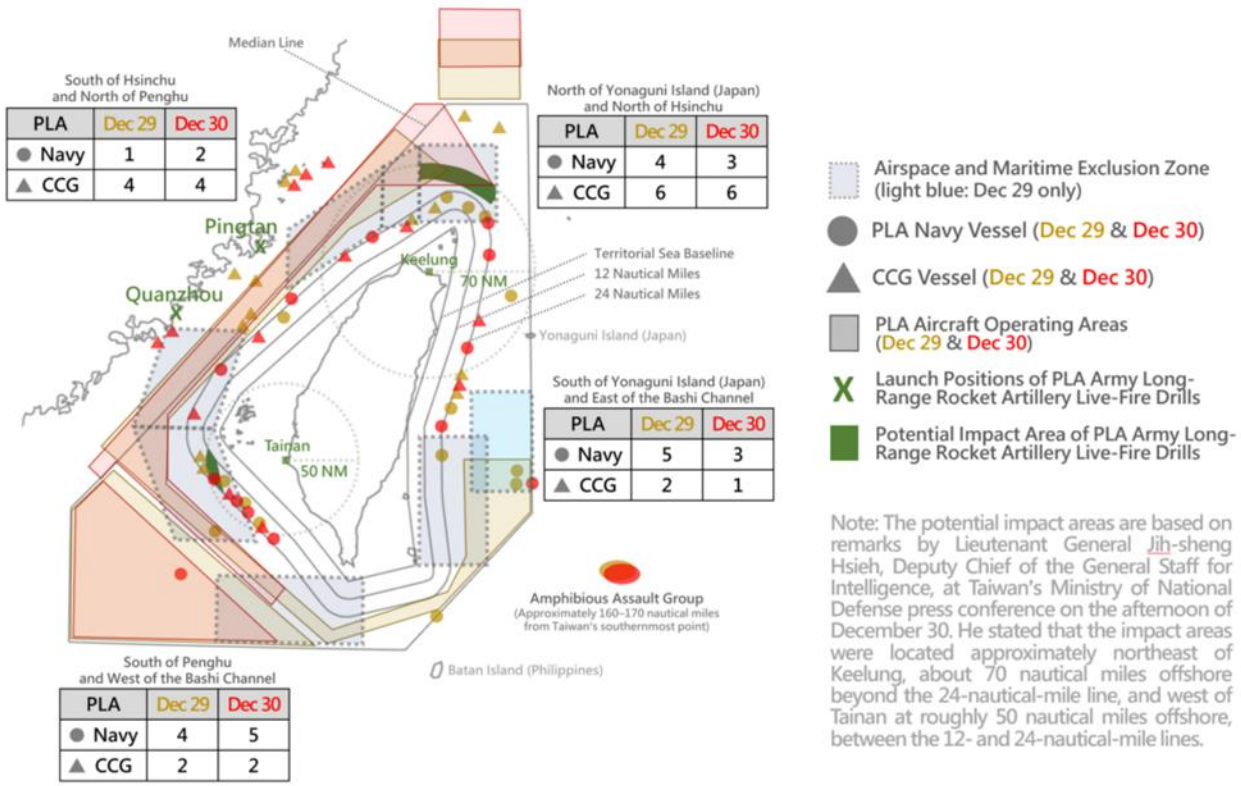
---

[20] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2025* (Washington, DC: DoD, 2025).

[21] Ibid.

[22] Mao Zedong, *On Protracted War* (1938), in *Selected Works of Mao Tse-Tung*, Vol. II (Beijing: Foreign Languages Press, 1965).

[23] Paret, Peter, ed. Makers of Modern Strategy: From Machiavelli to the Nuclear Age. Edited by Gordon A. Craig and Felix Gilbert. Princeton, NJ: Princeton University Press, 1986. Pg 531. ISBN 0-691-02764-1.



Compilation by K. Tristan Tang based on Taiwan's Ministry of National Defense press releases

For further analysis, see: K. Tristan Tang, "PLA Justice Mission 2025 Further Rehearses Taiwan Invasion Operations," China Brief, The Jamestown Foundation, January 9, 2026.

The Schlieffen Plan later operationalized this logic: victory must precede strategic encirclement and protraction before another force is able to mobilize. As late 1914 history demonstrates, strategies predicated on speed fail when systemic resilience denies the decisive window, but modern Chinese doctrine reflects a technologically updated variant of this speed-centric logic. Chinese military writings describe "system destruction warfare" as targeting critical nodes and operational linkages rather than engaging in attritional force-on-force combat alone.[24] The aim is not global annihilation of U.S. forces, but paralysis of the systems that enable intervention, command networks, logistics flows, space-enabled communications, and regional bases during the conflict's opening phase.[25] Cyber and information warfare expand the tools available for this strategy. Public reporting has identified PRC-linked cyber actors gaining access to U.S. critical infrastructure networks, suggesting potential preparation for crisis exploitation.[26] Cyber operations can disrupt energy systems, transportation scheduling, logistics databases, and communications networks without triggering immediate kinetic escalation. Information operations can amplify uncertainty, sow domestic confusion, and compress political decision-

[24] Elsa B. Kania and John Costello, "China's Military Strategy and 'System Destruction Warfare,'" Center for a New American Security, 2018.
[25] DoD, *Military and Security Developments Involving the PRC 2025*.
[26] U.S. Department of Justice and CISA advisories regarding PRC-linked cyber actors targeting U.S. critical infrastructure, 2024.

making timelines. These domains allow speed and concentration without overt escalation into war.

Large-scale kinetic attacks on the continental United States would risk escalation beyond Beijing's regional objectives. Instead, limited cyber disruption, space interference, and information operations could create friction. This in turn complicates mobilization, slows deployment, and injects hesitation during the decisive opening phase of a Taiwan campaign.

This strategic posture reflects acute awareness of time. Were Mao once weaponized protraction, contemporary Chinese strategy must avoid being trapped by it. Rapid concentration and early decision reduce the window in which the United States can marshal its structural advantages. If delay benefits the defender, speed becomes the attacker's shield. Yet structural realities temper the plausibility of permanent paralysis. The geographic scale, distributed infrastructure, and adaptive capacity of the United States complicate sustained immobilization. The likely aim is not national collapse, but tempo disruption sufficient to shape the opening campaign.

The strategic problem, therefore, is delayed reaction. If a Taiwan contingency unfolds under conditions of domestic friction, whether cyber-induced infrastructure instability or degraded communications, the Joint Force must still generate and project combat power rapidly. Recognizing time as the decisive variable clarifies the defensive requirement: infrastructure resilience is not merely protective; it is a counter-speed strategy designed to deny decisive advantage.

Institutionalizing SAP: Doctrinal Refinement and Operational Implications

If speed and early decision define the adversary's strategy, then doctrine must deny that advantage. A contingency shaped by systemic disruption and compressed timelines places a premium on preserving force-generation tempo despite friction. The Air Force cannot assume uninterrupted access to infrastructure or flawless interagency coordination. It must institutionalize resilience as an operational requirement rather than an aspirational goal.

Implementing Sense–Absorb–Project therefore requires more than conceptual endorsement; it demands doctrinal normalization of a contested homeland and explicit incorporation of force-generation continuity into Air Force and Joint planning constructs.

Reframing the Homeland in Air Force Doctrine

Air Force Doctrine Publication (AFDP) 3-27, *Homeland Operations*, should explicitly state that infrastructure degradation is an expected operating condition in peer conflict rather than a contingency. Current doctrine distinguishes homeland defense from forward combat operations

in ways that imply episodic crisis response.[27] SAP requires reframing homeland operations as persistent, multi-domain competition. Infrastructure disruption—whether cyber intrusion, power instability, GPS interference, or logistics data corruption—must be treated as operational friction inherent to peer conflict. AFDP 3-27 should incorporate a subsection addressing **"Contested Infrastructure and Force Generation Continuity,"** identifying power, communications, transportation, and digital control systems as operationally relevant dependencies. It should require installation-level identification of minimum essential functions necessary to sustain sortie generation and define degraded operating modes for bases under infrastructure stress. Codifying these dependencies forces planners to account for disruption rather than assume availability.

Integrating Degradation into Operational Planning

AFDP 3-0, *Operations*[28], should integrate infrastructure degradation into operational design and force presentation decisions. Planning guidance should:

- Treat domestic deployment timelines as vulnerable to cyber and physical disruption.
- Require course-of-action comparison to assess resilience of force generation under degraded conditions.
- Incorporate mission assurance assessments into AFFORGEN readiness cycles.

Infrastructure should be elevated from background enabler to operational variable affecting tempo.

Normalizing Degraded Command and Control

AFDP 3-0.1, *Command and Control*[29], must normalize degraded communications as a baseline planning assumption. Doctrine should emphasize pre-delegated authorities, expanded commander's intent, and mission-type orders when communications are intermittent. Decision continuity must take precedence over information perfection. If adversaries seek to delay U.S. response through disruption, resilient C2 denies them leverage.

Aligning Cyber Doctrine with Mission Impact

AFDP 3-12, *Cyberspace Operations*[30], should explicitly prioritize defensive cyber efforts based on force-generation impact. Industrial control systems supporting installation energy, fuel distribution, and logistics functions should be designated operationally critical assets. Defensive cyber operations must be tiered according to sortie-generation consequences rather than network ownership alone. This shifts cyber defense from technical protection to mission assurance.

---

[27] Department of the Air Force, *Air Force Doctrine Publication (AFDP) 3-27, Homeland Operations* (Maxwell AFB, AL: LeMay Center, 2021).
[28] Department of the Air Force, *Air Force Doctrine Publication (AFDP) 3-0, Operations* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, 2023).
[29] Department of the Air Force, *Air Force Doctrine Publication (AFDP) 3-0.1, Command and Control* (Maxwell AFB, AL: LeMay Center, 2020).
[30] Department of the Air Force, *Air Force Doctrine Publication (AFDP) 3-12, Cyberspace Operations* (Maxwell AFB, AL: LeMay Center, 2023).

Joint Doctrine Alignment

Joint doctrine should reflect similar refinements. JP 3-27, *Homeland Defense*[31], should define mission continuity of force generation as a central objective of homeland defense operations. JP 5-0, *Joint Planning*[32], should require planners to assess domestic infrastructure disruption during early phases of peer conflict, including impacts on deployment timelines, logistics visibility, and space-enabled PNT. Embedding these considerations within the Joint Planning Process institutionalizes SAP across components and ensures resilience is evaluated alongside combat power.

Operational Effects of Doctrinal Change

These refinements produce tangible shifts:

1. Infrastructure degradation becomes a baseline planning assumption.
2. Installations maintain predefined degraded operating states with clear transition triggers.
3. Command authority is distributed to preserve tempo during communications disruption.
4. Cyber defense priorities align with sortie-generation impact.
5. Joint planners assess resilience as a determinant of strategic tempo.

Conclusion

Peer competition has reintroduced time as a strategic weapon. In a Taiwan contingency, the most plausible threat to the United States is not immediate destruction of the homeland, but delayed reaction—friction imposed through cyber disruption, information warfare, and systemic interference designed to slow mobilization and compress early decision-making. Speed and concentration define the adversary's logic.

The United States retains structural advantages in scale, redundancy, and adaptive capacity. Yet those advantages only matter if force generation endures under pressure. Infrastructure vulnerability cannot be eliminated, and coordination across fragmented governance structures will never be perfect. Waiting for comprehensive modernization or centralized control is neither realistic nor sufficient.

Sense–Absorb–Project is not an optional resilience initiative; it is a strategic necessity. Early detection denies surprise. Degraded-mode operations deny paralysis. Sustained projection denies the adversary the decisive advantage of time. By institutionalizing infrastructure resilience as a force-generation doctrine, the Air Force transforms vulnerability into endurance and endurance into deterrence.

---

[31] Joint Chiefs of Staff, *Joint Publication (JP) 3-27, Homeland Defense* (Washington, DC: Joint Chiefs of Staff, 2018).

[32] Joint Chiefs of Staff, Joint Publication (JP) 5-0, Joint Planning (Washington, DC: Joint Chiefs of Staff, 2020).

The homeland is no longer sanctuary. It is operational terrain. In that environment, the decisive question is simple: can the Joint Force project combat power under fire? If the answer is yes, tempo is preserved. If tempo is preserved, strategic decision remains ours.