

Beyond the Fence Line: Operationalizing Civil-Military Cyber Coordination at U.S. Military Installations

Michaela Lee

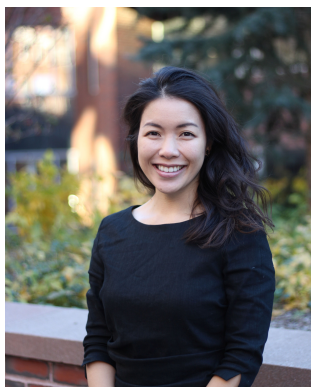
Deputy Chief Cyber Officer, State of New York, New York, NY, USA

U.S. military power projection increasingly depends on civilian critical infrastructure outside Department of War (DoW) control. Recent cyber campaigns—including China’s Volt Typhoon pre-positioning in energy grids, water systems, and transportation networks—have systematically targeted the “civil-military seam” where DoW authority ends but operational dependencies continue. Federal-state-local coordination architecture is inadequate to defend this seam. Military installations often depend on state-regulated utilities, locally-managed water systems, and privately-operated transportation networks, yet lack formalized coordination mechanisms with these entities. Resource constraints at state and local levels, jurisdictional fragmentation, and classification barriers preventing information sharing leave installations vulnerable to disruption of surrounding civilian infrastructure. DoW’s December 2024 directive requiring installations to coordinate “beyond the fence line” with state and local governments acknowledges this challenge but lacks an implementation framework. This article proposes operationalizing military installations as regional cyber resilience coordination nodes, or “seeds,” from which federal-state-local partnerships develop.

Keywords: cyber resilience, critical infrastructure, power projection, military readiness, civil-military seam

Disclaimer: The views expressed in this work are those of the author(s) and do not reflect the official policy and position of the State of New York or Executive Chamber, the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.

© 2025 The Author(s) unless otherwise stated. As an open access journal, The Cyber Defense Review publishes articles under Creative Commons licenses, and authors retain copyright where applicable.



Michaela Lee serves as the Deputy Chief Cyber Officer for Operations for New York State. In this role, she oversees cybersecurity operations across New York and works closely with other members of the Governor’s Office, state agencies, local governments, and federal partners to ensure the security and resilience of the state’s critical infrastructure. Before joining New York, Michaela was the Director for Strategy and Research at the White House Office of the National Cyber Director, helping develop and implement the National Cybersecurity Strategy and leading special projects on technology and democracy. Previously, she served as a Tech and Human Rights Manager at BSR, where she covered responsible AI, privacy, and end-to-end encryption. Michaela is a Non-Resident Fellow with the Carnegie Mellon Institute for Strategy & Technology and a term member at the Council on Foreign Relations. She received a bachelor’s degree from UC Davis and a Master of Public Policy from the Harvard Kennedy School.

INTRODUCTION

In September 2024, reports emerged that U.S. telecommunications firms had been compromised by Chinese hackers (Krouse, McMillan, and Volz 2024). Subsequent reports revealed that Salt Typhoon, a Chinese state-sponsored cyber espionage group, had compromised at least 600 companies across more than 80 countries (Viswanatha and Krouse 2025). The campaign was primarily an intelligence operation, but it also demonstrated persistent access to networks critical to civilian and military everyday communications. When combined with Volt Typhoon pre-positioning in energy grids, transportation networks, and water and wastewater systems, a clear strategic picture emerges: adversaries are systematically mapping and infiltrating civilian critical infrastructure. Protecting critical infrastructure from sophisticated cyber threats is not merely a homeland security task; it is a fundamental prerequisite for maintaining military readiness, ensuring the lethality of the force, and projecting power in a contested world.

Cyber threat actors often disregard jurisdictional boundaries and distinctions between federal, state, and local authorities. They exploit the very interdependencies that make our society efficient and connected: information and communications technology, cloud-native services, shared utilities, and global supply chains. Karen Gutteri (2025) persuasively argues that these threats are most critical at the “civil-military seam,” where there are gaps between military systems and assets controlled by the Department of War (DoW) and civilian-owned and -operated installation support infrastructure essential to military operations.

This article proposes operationalizing military installations as coordination nodes, or “seeds,” for regional cyber resilience, providing the federal-state-local coordination framework required by DoW’s December 2024 policy directive to establish resilience “beyond the fence line.”

The stakes are clear. As a recent Cyberspace Solarium 2.0 report documents, U.S. military power projection depends on 18 commercial seaports, 69 civilian airports, 40,000 miles of commercial rail, and countless municipal utilities—all outside DoW direct control (Fixler, Montgomery, and Lane 2025). The *2025 Annual Threat Assessment of the U.S. Intelligence Community* identified the threat even more clearly:

If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces (ODNI 2025).

By identifying China's cyber campaigns against defense critical infrastructure as a top-tier threat, the Office of the Director of National Intelligence (ODNI) openly flags this challenge; the current federal-state-local coordination architecture is insufficient to defend the civil-military seam. What does operational cyber resilience look like from the perspective of a county office responsible for managing municipal water systems that serve nearby military installations? Do federal strategies adequately translate into actionable guidance for local utilities, transportation authorities, and emergency managers? And most critically: how can the U.S. bridge the persistent gap between federal recognition of cyber threats and the state/local capacity necessary to address them?

THE THREAT LANDSCAPE: CIVILIAN INFRASTRUCTURE AS CONTESTED TERRAIN

For many adversaries of the U.S., civilian infrastructure is an attractive target in geopolitical cyber conflict. Electrical grids, telecommunications, transportation networks, and health systems increasingly have become fair game, marking a stark evolution from past decades, when military operations largely avoided civilian targets under international norms.

The inconsistent application of deterrence strategy by the U.S. and others has helped adversaries undermine such norms. Today, adversaries see civilian infrastructure not just as collateral, but as a pressure point. It can be exploited for strategic leverage, political disruption, financial gain, and psychological effect, often as part of hybrid or pre-kinetic strategies.

Russia's cyber operations against Ukraine since 2022 are real-world demonstrations of adversary strategies targeting civilian infrastructure to degrade military response. Russia systematically attacked Ukrainian power grids, water systems, and telecommunications in an attempt to disrupt military logistics and undermine civilian morale simultaneously. Blackouts, disrupted logistics, and widespread distributed denial-of-service (DDoS) attacks caused societal and military disruption in tandem. Ukraine's resilience offers instructive lessons. Through rapid repair capabilities, distributed generation, international partnerships (including Starlink satellite communications and the Cyber Defense Assistance Collaborative),

and prior experience with Russian cyber tactics, Ukraine maintained critical capabilities despite sustained attacks (Smith 2022; Simonite 2022).

In 2020, Iranian actors attempted to manipulate Israeli water treatment systems to increase chemical dosing levels—potentially endangering the health of civilians (Jeffries et al. 2022). In 2023, Iranian actors compromised programmable logic controllers used by water and wastewater organizations. Such examples show how civilian infrastructure is no longer collateral; it is strategic.

The People's Republic of China's campaigns further illustrate the trend toward pre-positioning, that is, infiltrating critical infrastructure well before any overt conflict. Unlike traditional espionage operations, Volt Typhoon demonstrated deliberate pre-positioning in operational technology (OT) systems controlling physical infrastructure. The campaign targeted telecommunications networks, energy grids, water systems, and transportation infrastructure, which are precisely the sectors essential to military power projection. Technical analysis revealed sophisticated tradecraft, where adversaries utilized living off the land (LOTL) techniques that leverage native system utilities to avoid detection while maintaining persistent access for years (CISA 2024).

These tactics indicate a fundamental shift in how adversaries approach conflict, blending traditional military strategies with asymmetric cyber operations that target civilian infrastructure. This shift demands that the security of critical infrastructure is elevated to the same level of care and political importance as is the case for traditional national security assets.

The Dissolution of the Perimeter

For years, cybersecurity doctrine was anchored in the notion of the perimeter—a virtual boundary defending internal systems from external threats. However, the emergence of cloud-native architectures, remote workforces, Internet of Things ecosystems, and software supply chains has dissolved this boundary. Today, organizations rely on software-as-a-service (SaaS) providers for key business processes and depend on code libraries developed by unknown third parties. Meanwhile, many critical infrastructure providers still rely on legacy systems that were never designed to withstand cyberattacks. Attack surfaces have expanded exponentially, as has the number and sophistication of adversaries.

While DoW has adapted to this evolving challenge through Zero Trust principles, the civilian critical infrastructure upon which installations depend operates under different constraints. Implementing Zero Trust architectures is challenging in environments with legacy OT that don't easily integrate with modern authentication mechanisms. Resource constraints further complicate critical infrastructure entities' ability to adopt Zero Trust security architectures or maintain continuous monitoring capabilities.

In the new threat landscape, cyber resilience cannot be confined to firewalls or access control lists. A vulnerability in a widely used open-source component can place everything from hospital record systems to water utilities at risk. Resilience, therefore, must be systemic: it must anticipate unknown risks, account for interdependencies, and incorporate recovery into its very design.

The Convergence of Threat Actors and Insignificance of Attribution

The line between nation-state and criminal cyber actors is increasingly blurred, and this poses challenges for how the United States responds to cyberattacks. Sophisticated criminal groups now possess capabilities once reserved for intelligence agencies, and they frequently operate under tacit approval, or even direct guidance, of adversary governments. The Conti ransomware group, for example, operated with impunity out of Russia and, in some cases, appears to have shared resources and targets with state-sponsored actors. North Korea's Lazarus Group has conducted both state espionage and high-profile cryptocurrency theft to fund the regime.

For the U.S. federal government, the distinction between state and non-state actors matters significantly. Intelligence agencies have different authorities and restrictions based on the nature of the adversary, and any diplomatic or military responses hinge on clear attribution to a foreign government. However, for state and local governments or operators of critical infrastructure who are often on the front lines of these intrusions, the identity of the attacker is much less relevant. Whether a hospital system is taken down by a ransomware gang or a nation-state adversary, the operational consequences are the same: catastrophic.

This convergence benefits adversaries by creating plausible deniability and complicating coordinated response strategies. Intelligence agencies have limited authority to act domestically, while civilian critical infrastructure providers often lack insight into the sophistication or intent of attackers. The result is paralysis in moments of crisis and fragmentation in long-term strategy. The challenge is paradoxical; the United States must simultaneously prepare for strategic cyber conflict (such as one involving China and Taiwan) while also attempting to counter highly distributed, persistent ransomware attacks across sectors. Although counter-strategies, operational considerations, and effects of these threats are unique, both can cause comparable damage and disruption, particularly at the civil-military seam.

The Information Domain as Target and Enabler

Cyber-capable adversaries do not need to physically destroy infrastructure because non-kinetic cyber disruption can achieve similar effects without triggering escalatory action. In the information domain, data flows between military and civilian systems are targets for exploitation. Consider mobilization as an information-intensive process. When personnel receive deployment orders, they access information through commercial internet connections.

Logistics systems track equipment movement through civilian transportation networks, generating data about timing, routes, and cargo. Each of these information flows potentially reveals operational patterns, timing, and intentions to adversaries with access to civilian infrastructure.

Russia has used these tactics to great effect in its war with Ukraine. In addition to disruptive attacks, Russia has targeted Western logistics entities and technology companies involved in the coordination, transport, and delivery of foreign assistance to Ukraine (CISA 2025). Adversaries targeting civilian infrastructure can exfiltrate data revealing military dependencies and timing, manipulate data to cause operational confusion (e.g., incorrect fuel delivery schedules, altered cargo manifests), or deny access to data systems, forcing manual operations that slow mobilization.

The Civil-Military Seam as Battlespace

The “civil-military seam” describes where DoW authority ends but operational dependencies continue. This boundary manifests across four dimensions. Physically, it is the installation fence line separating military-controlled assets from civilian-owned infrastructure. Jurisdictionally, it divides federal military authority from state and local regulatory control over, for example, utilities, transportation, and telecommunications. Operationally, it separates DoW’s cybersecurity standards and resources from civilian operators’ often-limited capabilities. Informationally, it creates barriers between classified threat intelligence held by military and federal agencies and uncleared civilian infrastructure operators who need that intelligence to defend critical systems.

Adversaries exploit these seams through several mechanisms. They target civilian infrastructure knowing that DoW cannot unilaterally defend it. They leverage jurisdictional complexity, understanding that unclear roles and responsibilities create gaps in coverage. They exploit resource disparities, recognizing that small municipal utilities lack sophistication to detect nation-state intrusions.

The strategic implication is that resilience cannot be achieved through military hardening alone. If surrounding infrastructure degrades, military installations degrade with it. Conversely, securing civilian infrastructure serves both civilian essential services and military readiness, making resilience a shared civil-military imperative.

THE INTERDEPENDENCY FRAMEWORK: IDENTIFYING MILITARY DEPENDENCIES ON CIVILIAN INFRASTRUCTURE

Consider Joint Base Lewis-McChord (JBLM) in Washington State, home to I Corps and the only Army power projection platform west of the Rocky Mountains. The base depends entirely on Tacoma Power for electrical service to operate climate control systems that protect sensitive

equipment, power logistics systems that coordinate deployment and sustainment, maintain communications networks, and sustain force health protection for personnel and families. In the case of an extended outage, the base is required to be able to independently sustain operation of mission-critical facilities for at least fourteen days (Secretary of the Army 2020).

To address risks to military energy resilience, the Department of War has focused extensively on “inside the fence” backup power systems and microgrids. JBLM recently put forward plans to construct a microgrid to sustain critical facilities, noting that only 35% of their airfield’s critical facilities have backup generators in place, and none have alternative sources capable of providing continuous long-term power (Under Secretary of War Comptroller 2024).

On-site resilience strategies such as microgrids are necessary but insufficient, given the heavy reliance of bases on civilian infrastructure. For example, JBLM supports approximately 30,000 active duty service members, as well as nearly 295,000 civilians, family members, and local retirees who are also connected to the base. Many of them live in the surrounding region and are also dependent on civilian critical infrastructure for basic services (Military OneSource 2025).

In recognition of this challenge, DoW issued a new policy in December 2024 that requires components to include considerations “beyond the fence line” in their infrastructure resilience strategies. This policy includes a requirement to:

Undertake planning and assistance with State and local governments to ensure efficient preparedness and resilience of essential transportation, logistical, or other necessary resources *outside of a military installation* that are necessary in order to maintain, improve, or rapidly reestablish military installation mission assurance and mission-essential functions (Under Secretary of Defense for Acquisition and Sustainment 2024).

This new policy reflects a growing recognition that defense communities are crucial for delivering mission capabilities and projecting power. However, the policy intention currently lacks the enforcement mechanism necessary to ensure resilience against a Volt Typhoon-level threat. A notable challenge is that dependencies between installations and civilian networks are inherently multi-dimensional:

- Physical – electricity, water, fuel, and transportation.
- Digital – telecommunications, industrial-control systems, and logistics data.
- Human – workforce, contractors, and emergency-response capacity.

Because these dependencies span multiple jurisdictions, accountability is fragmented, and it is challenging to identify and map all potential vulnerabilities and their cascading effects. While the following survey is not exhaustive, it aims to provide an overview and examples of sector-specific implications that impact resilience at the civil-military seam for U.S. military installations.

Sectoral Implications

Energy. Grids and fuel logistics are primary operational enablers. OT vulnerabilities in electrical grids and pipelines, combined with distributed ownership and regulatory fragmentation, make the energy sector a high-leverage target for adversaries seeking to delay or complicate force projection. The May 2021 Colonial Pipeline ransomware attack exposed vulnerabilities in the U.S. fuel logistics system; although non-OT billing systems were compromised, uncertainty about system integrity led Colonial to preemptively shut down 5,500 miles of pipeline delivering 45% of the total fuel supply for the East Coast, which is home to multiple military installations (Mittal 2024).

Transportation and Ports. Strategic sealift and heavy equipment movement depend on commercial ports, railways, and intermodal connectors. Recent analysis by the Foundation for Defense of Democracies states that 90% of military equipment deploys through commercial seaports, such as the Port of Jacksonville, which handles military cargo for U.S. Central Command and U.S. Southern Command operations (Fixler, Montgomery, and Lane 2025). Rail infrastructure moves heavy equipment that cannot be transported by road or air. Strategic rail corridors from Fort Riley, Kansas to ports on both coasts carry tanks, artillery, and armored vehicles for overseas deployment. These rail networks are owned and operated by private companies—BNSF Railway, Union Pacific, and CSX Transportation—whose dispatch systems, signaling networks, and logistics software are potential cyber targets. Because many of these strategic assets are privately operated under federal safety regulation, a cohesive nation-level response depends on extensive public-private coordination.

Water and Wastewater. Military installations require water for human consumption, equipment cooling systems, firefighting, medical facilities, and food service operations. Most installations receive water from municipal systems managed by local governments or regional authorities. While some systems have mature cybersecurity programs, many small and mid-sized municipal systems operate with minimal cyber staff and outdated OT. The Oldsmar incident and other intrusions highlight the potential for public health consequences and operational degradation if water treatment or distribution systems are manipulated (Jeffries et al. 2022). The risk is particularly acute for hospitals. The CDC notes that emergency water storage capacity at hospitals typically lasts under two hours, whereas backup power may last for multiple days (Centers for Disease Control and Prevention and American Water Works Association 2019). This asymmetry makes water infrastructure disruption potentially more operationally significant than power outages.

Telecommunications and Data Networks. Military installations rely on commercial internet service providers for daily administrative functions, coordinating unclassified logistics, communicating with personnel, and storing non-classified data on cloud-based platforms. Persistent

adversarial access to carrier networks enables them to analyze traffic, conduct man-in-the-middle operations, and establish routes for denying or manipulating connectivity. The Salt Typhoon incident highlights the strategic value of pre-positioning within telecommunications infrastructure. The broader ecosystem's components— including Domain Name System (DNS), routing, backbone fiber, and mobile networks— are vulnerable to both observation and disruption.

JBLM alone depends on at least 15 distinct civilian critical infrastructure entities. Other military installations have similar profiles and must also navigate numerous operational relationships with municipal entities, critical infrastructure operators, and state and local officials. The remaining sections of this article will lay out the challenges and opportunities for stronger coordination and resilience across the civil-military seam.

STATE AND LOCAL PERSPECTIVES: BRIDGING FEDERAL STRATEGY AND OPERATIONAL REALITY

Federal cyber strategies often assume state and local entities will implement federal guidance and priorities. The reality is much more complex. States face competing demands for limited resources: education funding, healthcare costs, infrastructure repair, and numerous other priorities. Cybersecurity competes with these pressing needs, often without dedicated funding.

Resource Constraints and Competing Priorities

Federal strategies and guidance establish national priorities but often have limited funding or operational support for state and local implementation. This creates a strategic disconnect: federal plans assume state capacity that doesn't exist, while states may struggle to operationalize federal guidance without corresponding funding or technical assistance.

This resource disparity manifests in several ways. State budgets often operate under balanced budget requirements and tax revenue constraints that limit discretionary spending, leaving little fiscal flexibility for cybersecurity investments that lack dedicated funding streams. States also struggle with significant personnel constraints, often unable to compete with the federal government and the private sector for cyber talent. Technology gaps exacerbate this issue, as many state and local systems operate on outdated legacy technology with deferred upgrades and a history of poor vulnerability management. Furthermore, training deficiencies mean cybersecurity awareness remains inconsistent, and the issue as a whole struggles to compete for executive attention against more immediate, visible challenges.

Jurisdictional Complexity and Authority Gaps

Critical infrastructure protection involves overlapping federal, state, local, and private sector authorities. Utilities are regulated at the state level, but interstate transmission is regulated at the federal level. Water systems are locally managed but federally regulated for quality without federal cybersecurity standards. Telecommunications are federally regulated, but state commissions maintain some limited oversight over them. This fragmentation means no single entity has comprehensive authority or visibility.

Private sector complications add complexity. Most critical infrastructure is privately owned. States can regulate entities within their jurisdiction, but enforcement mechanisms are limited. The Colonial Pipeline decision to shut down, for instance, while rational from a corporate risk perspective, created cascading effects that state and federal authorities had limited ability to prevent or mitigate.

Information Sharing: The Persistent Barrier

Many of the most frustrating gaps in federal-state coordination involve information sharing. Classification systems designed for the federal government create barriers preventing effective cooperation with state and local partners. Federal threat intelligence is often classified, which prevents it from being shared with state officials who lack clearances. While some state officials maintain clearances, most stakeholders at the operational level—including utility operators, emergency managers, and local officials—typically do not. This means actionable threat intelligence never reaches the people who must respond to it.

Even when state officials hold clearances, “need to know” determinations may prevent sharing. Amid uncertainty, private sector infrastructure operators may fear that reporting cyber incidents will trigger regulatory consequences, lawsuits, or public disclosure that can damage their reputation. Years of inconsistent federal engagement with states on these matters have created trust deficits. These structural barriers impede information sharing even when it is in the best interest of all parties to cooperate.

Coordination Gaps at the Civil-Military Interface

Given the gaps stated above, it is no surprise that military installations and surrounding civilian infrastructure often operate as separate worlds, despite deep operational interdependencies. Many installations lack regular engagement with local utility operators, emergency managers, or municipal officials. Communication occurs only during crises, which can result in mistrust and unfamiliarity with each others’ procedures. Military installations may not understand civilian infrastructure vulnerabilities or operational constraints, while civilian operators may not understand military mobilization requirements, critical timing windows, or priority needs during crises.

A realistic scenario illustrates these gaps: A cyberattack disrupts a power grid during hurricane response. The military installation must mobilize for disaster relief while continuing to support its own mission. The civilian population needs power for life safety. State-level emergency management coordinates response but lacks visibility into military requirements. The military installation operates backup generators but needs fuel resupply through civilian logistics networks that were disrupted by hurricane damage and cyberattack. Who makes prioritization decisions? Through what mechanism? Based on what pre-established framework? Currently, such scenarios are often resolved through ad hoc coordination and improvisation—approaches that usually fail under stress.

Recent incidents demonstrate that these gaps are not theoretical. Winter Storm Uri caused cascading failures across Texas's electrical grid in February 2021, affecting multiple military installations including Fort Hood, Fort Sill, Fort Polk, and Fort Riley (Gabram 2021). While these installations maintained backup generation capacity consistent with DoW requirements, the broader grid collapse created secondary effects the military could not address unilaterally.

The Electric Reliability Council of Texas (ERCOT), which operates the state's independent grid, had no formal coordination mechanism with military installations. As the crisis unfolded, installations were treated as large commercial customers rather than entities with national security missions. No pre-established protocol existed for installations to communicate operational criticality to ERCOT operators, who needed to make load-shedding decisions. Consequently, some installation facilities experienced rolling blackouts alongside civilian neighborhoods, despite housing mission-critical operations.

Fuel resupply for backup generators became critical as the storm persisted beyond the typical 72-96 hour backup durations assumed by DoW planning. However, civilian fuel distribution networks were themselves compromised by power outages at pumping stations, refineries, and other pipeline infrastructure. Natural gas production facilities also lost power and were unable to pump gas to power plants, creating a cascading feedback loop that extended the crisis. The incident revealed fundamental coordination gaps. While installations understood their dependency on civilian infrastructure, no mechanism existed for real-time coordination with ERCOT, the Texas Division of Emergency Management, state energy offices, or fuel distributors. Information sharing was informal and episodic (Busby et al. 2021). The Texas winter storm illustrated what the DoW's December 2024 directive seeks to address: installations cannot achieve resilience inside the fence line when surrounding civilian infrastructure fails.

Having identified the gaps in the current structures, the following section proposes an operational framework for addressing them.

REGIONAL RESILIENCE AS STRATEGIC READINESS: MOVING FROM AWARENESS TO INTEGRATION

Military bases are among the most resource-intensive and infrastructure-dependent institutions in the nation. Their operational readiness depends on local utilities that are often managed by civilian and private sector entities with limited cybersecurity capabilities and resources. Because of this, resilience must be reciprocal. It is not enough for bases to harden their own networks and build internal redundancies. They must also actively assist their host communities in building resilience and institutionalizing coordination across federal, state, and local domains. The central requirement is not new technology or statutory authority, but an operational framework that aligns defense readiness with civilian continuity.

The “Seeds” Concept: Installations as Coordination Nodes

The core recommendation is to utilize military bases as coordination nodes—or “seeds”—for unifying federal, state, and local cyber defenses at the civil-military seam. Military installations offer unique advantages: their geographic distribution across the country (approximately 800 DoW installations across 50 states) covers a significant portion of critical infrastructure; active, reserve, and guard personnel have organic cyber capabilities based on private and public sector experience; installations have a strong, institutionally-stable presence in their communities; existing command structures and security clearances facilitate federal coordination; and they have a clear and direct operational interest in the security of surrounding infrastructure (Under Secretary of Defense for Acquisition and Sustainment 2024).

The “seeds” metaphor is deliberate. Installations don’t control surrounding ecosystems but provide growth opportunities from which broader resilience capabilities develop. This is not militarization of domestic infrastructure. Rather, it leverages existing military presence to bridge persistent federal-state-local gaps in cyber defense coordination—the same gaps adversaries actively exploit.

Consequently, installation commanders should treat engagement with state and local infrastructure partners as a normal function of readiness rather than a discretionary activity. Regular exchanges of information on critical dependencies, joint participation in regional planning forums, and inclusion in state or regional-level resilience exercises will create a shared understanding of operational risk. Such practices would also clarify the thresholds at which local disruptions become national security concerns.

Institutionalizing Routine Coordination

Experience from both cyber incidents and natural disasters demonstrates that the nature of the relationships established before a crisis determines the effectiveness of the response. Formal structures—such as standing working groups that link installations, National Guard cyber

units, emergency managers, and utilities—can convert episodic cooperation into habitual coordination. Over time, these relationships form a regional network capable of identifying interdependencies, rehearsing response procedures, and coordinating restoration priorities. The value lies not in creating new organizations but in normalizing contact across the existing ones.

Routine coordination also enables the development of clear protocols for rapid coordination during actual cyber incidents. This reduces the risk of improvised responses. Participants know whom to call, what information to share, and how decisions get made.

Integrating Resilience into Readiness Frameworks

Resilience must be treated as a measurable dimension of military readiness. Operational plans that assume assured access to power, water, and digital connectivity should incorporate the risk of local infrastructure disruption and the time required to restore essential services.

Joint vulnerability assessments could help map critical dependencies and single points of failure that could affect multiple customers, including installations. This coordinated mapping would enable military and civilian partners to identify mutually reinforcing investments that could be fulfilled through programs such as the Defense Community Infrastructure Program.

Aligning Incentives and Information Flows

Persistent information asymmetries continue to be a significant impediment to joint resilience. Classified threat reporting seldom reaches those who operate the systems upon which installations depend, while local operational data rarely informs federal planning. The DoW, the ODNI, and the Cybersecurity and Infrastructure Security Agency should continue refining methods to share actionable intelligence at appropriate classification levels.

Parallel adjustments to grant programs and infrastructure funding mechanisms could incentivize civilian operators to adopt security measures that also enhance military continuity, ensuring that national defense and economic resilience advance together rather than in parallel.

Embedding Resilience in Strategic Culture

Ultimately, resilience should be recognized as a strategic attribute of power, rather than a support function. Adversaries seek to exploit friction within the national enterprise, assuming that the fragmentation of responsibilities will slow response and recovery. Countering that assumption requires a culture of planning that anticipates degradation. Integrating civilian infrastructure resilience into national defense planning would demonstrate that the United States can sustain operations under prolonged pressure—an assurance that contributes directly to deterrence credibility.

CONCLUSION: RESILIENCE AS A SHARED IMPERATIVE

Military readiness and civilian critical infrastructure cybersecurity have become inextricably linked by technology, logistics, and shared vulnerabilities. As cyber threats grow more sophisticated and indiscriminate, resilience will depend on hardened systems and on trust, coordination, and sustained partnership across jurisdictions.

Adversaries systematically exploit the gap between federal cybersecurity strategy and under-resourced state and local implementation. Closing this gap requires recognizing that military installations and civilian communities share vital interests in resilient infrastructure. A more resilient power grid, for example, serves residential customers, businesses, hospitals, and military installations simultaneously. This is not a zero-sum competition; it is an alignment of interests.

The December 2024 DoW directive provides the policy mandate. But policy without implementation mechanisms falls short. The future of the nation's cybersecurity will not be determined by technological advancements alone, but by our ability to foster seamless, collaborative resilience across jurisdictional, sectoral, and organizational boundaries. This requires new governance models spanning public and private sectors, intelligence sharing mechanisms balancing security with accessibility, and funding that prioritizes infrastructure resilience.

Military installations and their host communities represent natural starting points for collaboration. This article has proposed leveraging military installations as regional coordination nodes—"seeds" from which federal-state-local partnerships can grow through formalized structures: standing working groups, joint vulnerability assessments, shared threat intelligence, and rehearsed crisis response protocols. By building regional cyber resilience ecosystems around these critical locations, the nation can develop scalable models demonstrating that collaborative cyber defense is operationally feasible.

The path forward requires political will, sustained commitment, and modest resource investment, but the alternative is continuing a fragmented approach that allows adversaries to methodically map and infiltrate the civilian infrastructure foundation of American military power. Whether the United States can defend this foundation depends not on recognizing the threat—which is clear—but on implementing the collaborative partnerships that will drive national resilience.

REFERENCES

- Busby, Joshua W., Kyri Baker, Morgan D. Bazilian, Alex Q. Gilbert, Emily Grubert, Varun Rai, Joshua D. Rhodes, Sarang Shidore, Caitlin A. Smith, and Michael E. Webber. 2021. "Cascading risks: Understanding the 2021 winter blackout in Texas." *Energy Research & Social Science* 77 (July). <https://doi.org/10.1016/j.erss.2021.102106>.
- Centers for Disease Control and Prevention and American Water Works Association. 2019. *Emergency Water Supply Planning Guide for Hospitals and Healthcare Facilities*. Technical report. U.S. Department of Health

- and Human Services. <https://www.cdc.gov/water-emergency/media/pdfs/2024/07/emergency-water-supply-planning-guide-2019-508.pdf>.
- CISA (Cybersecurity and Infrastructure Security Agency). 2024. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, February 7, 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.
- CISA (Cybersecurity and Infrastructure Security Agency). 2025. *Russian GRU Targeting Western Logistics Entities and Technology Companies*, May 21, 2025. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a>.
- Fixler, Annie, Mark Montgomery, and Rory Lane. 2025. *Military Mobility Depends on Secure Critical Infrastructure*. Foundation for Defense of Democracies (FDD), March 2025. <https://www.fdd.org/analysis/2025/03/27/military-mobility-depends-on-secure-critical-infrastructure/>.
- Gabram, Douglas M. 2021. *Statement on Installation Resiliency: Lessons Learned from Winter Storm Uri and Beyond*. Testimony before the Subcommittee on Readiness of the Committee on Armed Services, House of Representatives, March 26, 2021. <https://www.govinfo.gov/content/pkg/CHRG-117hhr48485/html/CHRG-117hhr48485.htm>.
- Guttieri, Karen. 2025. "Fighting Through Disruption: Reframing Cyber Resilience for Power Projection and Strategic Credibility." *Cyber Defense Review* 10 (1): 93–114. <https://doi.org/10.55682/cdr/egvf-mkys>.
- Jeffries, Blaine, Stephanie Saravia, Cedric Carter, and Zachary Ankuda. 2022. *Cyber Risk to Mission Case Study*. Technical report. MITRE, October 14, 2022. <https://apps.dtic.mil/sti/trecms/pdf/AD1183009.pdf>.
- Krouse, Sarah, Robert McMillan, and Dustin Volz. 2024. "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack." *Wall Street Journal* (September 26, 2024). <https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835>.
- Military OneSource. 2025. *Military Installations: Joint Base Lewis-McChord*, October 26, 2025. <https://installations.militaryonesource.mil/in-depth-overview/joint-base-lewis-mcchord>.
- Mittal, Manav. 2024. "Colonial Pipeline Cyberattack Drives Urgent Reforms in Cybersecurity and Critical Infrastructure Resilience." *International Journal of Oil, Gas and Coal Engineering* 12 (5): 106–119. <https://doi.org/10.11648/j.ogce.20241205.11>.
- ODNI (Office of the Director of National Intelligence). 2025. *Annual Threat Assessment of the U.S. Intelligence Community*. Technical report. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>.
- Secretary of the Army. 2020. *Army Directive 2020-03 (Installation Energy and Water Resilience Policy)*. Technical report. Department of the Army, March 31, 2020. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN21689_AD2020_03_FINAL_Revised.pdf.
- Simonite, Tom. 2022. "How Starlink Scrambled to Keep Ukraine Online." *WIRED* (May 11, 2022). <https://www.wired.com/story/starlink-ukraine-internet/>.
- Smith, Brad. 2022. "Defending Ukraine: Early Lessons from the Cyber War," June 22, 2022. <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.
- Under Secretary of Defense for Acquisition and Sustainment. 2024. *DoD Instruction 4715.28 (Military Installation Resilience)*. Department of Defense, December 17, 2024. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/471528p.PDF?ver=ar5bin4QPM3DMnDxjLv0Mw%3D%3D>.
- Under Secretary of War Comptroller. 2024. *Energy Resilience and Conservation Investment Program (ERCIP) FY 2025 Military Construction, Defense-Wide Project List by State/Country*. Department of War. https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/07_Military_Construction/14-Energy_Resilience_and_Conservation_Investment_Program.pdf.
- Viswanatha, Aruna, and Sarah Krouse. 2025. "Chinese Spies Hit More than 80 Countries in 'Salt Typhoon' Breach, FBI Reveals." *Wall Street Journal* (August 27, 2025). <https://www.wsj.com/politics/national-security/chinese-spies-hit-more-than-80-countries-in-salt-typhoon-breach-fbi-reveals-59b2108f>.

Received 3 July 2025; Revised 27 October 2025; Accepted 5 November 2025