WIDENING THE APERTURE:
REFOCUSING INSTALLATION–COMMUNITY COOPERATION AGAINST EMERGENT THREATS

PART 1: DEFINING THE THREAT // OCTOBER 2025

ASSOCIATION OF DEFENSE COMMUNITIES | Matrix

ACKNOWLEDGEMENTS

Authors

Peter Keiser, Matrix Design Group

Sal Nodjomian, Matrix Design Group

Brad Johnson, Matrix Design Group

Charlie Perham, Matrix Design Group

Eric Turner, Matrix Design Group

Editor

Randy Ford, Association of Defense Communitites

Layout

Will Noonan, Association of Defense Communitites

CREDITS

Front Cover: Marine Corps photo by Cpl. Joshua Barker, USMC Training and Education Command

Page 3: Army photo by SFC Renee Serutine of the 175th Cyber Operations Squadron, Maryland Air National Guard

Page 4: Army photo by SGT William Parsons

Page 5: Army photo by SSG Jacob Slaymaker

Page 6: Marine Corps photo by Ted Maj. Zacahry Leuthardt

Page 7: Army photo by SFC Renee Serutine

Page 8: Oklahoma National Guard photo by Leanna Maschino

CONTENTS

INTRODUCTION

The advantages of collaboration between Department of War installations and the cities, counties, and states that host them are well-documented. The fact that terms such as Intergovernmental Support Agreements, Enhanced Use Lease, and Military Installation Resilience Review are now common within the lexicon of defense communities is proof of the successes that collaborative programs and methods have demonstrated, both from the standpoint of installation readiness and from increased economic opportunities. However, the focuses of installation – community cooperation initiatives have traditionally been limited to aspects such as land use compatibility, installation resiliency, and opportunities for cost-savings. Official military–civilian partnerships in the forms of Memorandums of Understanding or other agreements are common, but also usually constrained to resource coordination for natural disaster or public safety response, or financial contracts for shared utilities and similar services. These partnerships and cooperation initiatives for emergency response and safety are valuable and necessary, however, they are inadequate to address emerging threats that have the potential to cause substantial harm to both installation readiness and shared installation – community infrastructure.

The most significant categories of emergent threats are those delivered via cyber means or unmanned systems (drones). Multiple examples from the ongoing war in Ukraine and elsewhere conclusively demonstrate that our military installations and the infrastructure they share with civilian communities are increasingly vulnerable to surveillance, disruption, and attacks from these delivery platforms. These examples illustrate how state and non-state actors can deliver strategic impact with minimal cost and high probability of success—posing serious threats to our military missions, forces, assets, and critical support systems.

While numerous actions are being taken across the nation to mitigate these threats, defense communities have a distinct opportunity to contribute to developing solutions that will help safeguard shared installation – community assets and protect the military missions that drive local civilian economies. Doing so requires a purposeful increase in the scope of existing civilian-military cooperation. It necessitates “widening the aperture” of installation–community partnerships to include defense against emergent threats.

This report is the first of a series that explores the challenges associated with the emergent threats posed by cyber and drone systems shared by Department of War (DoW) installations and their local communities in the Continental United States. Using existing Office

of Local Defense Community Cooperation (OLDCC) frameworks as a catalyst, the goal of this series is to provide an unclassified discussion on insights and possible opportunities for installations, local defense community support organizations, and communities to meet these shared challenges by expanding on their existing successes and partnerships. This first report introduces and defines our emergent threat focuses and their impacts on the safety and prosperity of our defense communities. Further installments will discuss the specifics of drone threats and cyber threats respectively with the goal of exploring how existing installation – community cooperation can be built upon to provide mutually beneficial readiness, resilience, and safety solutions.

Although the true impacts of these emergent threats are not fully defined, and strategies to effectively counter them are not fully developed, it is certain that safeguarding our communities, installations, and national defense assets against these threats requires swift, coordinated, and innovative actions to meet emergent threats head-on. Local installation–community partnerships are perfectly positioned to rise to this challenge and take these critical actions.

DEFINING THE THREAT

Geography has long been the greatest ally of the United States throughout its 250-year history. With oceans to the east and west, allies to the north and south, and no near-peer military in the entire hemisphere, our nation has a deep, effective, and 360-degree buffer zone from its enemies. Behind this buffer zone, our military has been able to enjoy a relative assumption of security for its installations as they project power to front lines and combat zones hundreds or thousands of miles from the Continental United States.

Emergent threats invalidate the security assumption that installations on United States soil are naturally protected and safe simply because they are far "in the rear" of a conventional war or conflict. The "emergent" label is appropriate to classify these threats because they contain modern technology that has only recently reached the point of affecting the landscape of warfare and national security in a way that carries serious ramifications for United States military installations. This report explores two of the most prevalent emergent threat categories:

Drone Threats

The DoW generally uses the term "unmanned systems" to describe drones, and there are many additional labels that pertain to unpiloted / remotely controlled tools, their supporting equipment, and their networks. This report uses the term "drone" because it is the most traditional and accessible label and it encompasses the widest range of relevant technology including air-, land-, or sea-based platforms and their various methods of control.

Two recent, well-publicized[1] events have drones at the forefront of military discourse. These events are Ukraine's "Spider's Web" attack on Russian air bases which destroyed or severely damaged numerous nuclear-capable Russian Air Force bombers in four separate locations hundreds of miles inside Russian[2]; and Israel's "Operation Rising Lion" which was a massively complex attack on a host of Iranian air

1 "Spectacular Drone Strikes and the Future Sanctuary of the U.S. Homeland." 2025. War on the Rocks. August 27, 2025. https://warontherocks.com/2025/08/spectacular-drone-strikes-and-the-future-sanctuary-of-the-u-s-homeland/.

2 Dahlgren, Masao, and Lachlan MacKenzie. 2025. "Ukraine's Drone Swarms Are Destroying Russian Nuclear Bombers. What Happens Now?" Csis.org. June 4, 2025. https://www.csis.org/analysis/ukraines-drone-swarms-are-destroying-russian-nuclear-bombers-what-happens-now.

defense and command and control systems as a prelude to Israel's more conventional air offensive against Iran[3]. The specific details of these operations have been discussed in other venues and publications at length, but it is worth noting a few similarities between them for the purposes of this analysis:

- Both attacks were vastly successful; achieved virtually complete surprise; and caused direct damage to high-value targets.
- Both attacks required extensive planning by highly capable military organizations and involved the preparation and staging of both materials and personnel across international borders.
- Both attacks utilized commercial logistics and publicly available services from providers in the enemy nation that had no idea they were assisting in an attack on their home soil.
- Both attacks caused billions of dollars in damage by attaching relatively small yields of explosives to commercially purchased and modified drones.

The Rise of Drone Use in America

21 Dec. 2015: FAA's online system for recreational small drones begins[4]

July 2025: 822K[5] total registered drones in the United States

10,300 monthly average of new owner registrations in 2021[6]

1.9 million recreational drones projected by 2029[7]

These two attacks provide a rough inspirational blueprint for similar, potential attacks on military installations in the United States. Granted, the attacks conducted by both Ukraine and Israel were incredibly well-planned, well-resourced, executed by the highest level of military and intelligence professionals, and required months, if not years, of preparation. However, these attacks were also strategic in scope, striking multiple geographically separate targets simultaneously. Non-state actors, homegrown terrorists, or agents of competitor states could utilize the same general model of attack against a single, less complex target within the Continental United States (for example, a single installation's flight line or headquarters) or merely utilize drones to surveil military installations, setting conditions for a larger, more conventional attack. This smaller scope of incursion or attack could still yield potentially devastating and expensive results for U.S. military readiness at a comparatively low cost with a far lower logistical burden. Given the successful examples demonstrated to high acclaim, it would be naïve to think that America's enemies are not planning similar attacks against military installations within the Continental United States.

3 Walla, Katherine. 2025. "By Fusing Intelligence and Special Operations, Israel's Strikes on Iran Are a Lesson in Strategic Surprise." Atlantic Council. June 14, 2025. https://www.atlanticcouncil.org/blogs/new-atlanticist/by-fusing-intelligence-and-special-operations-israels-strikes-on-iran-are-a-lesson-in-strategic-surprise/.
4 "Unmanned Aircraft System." n.d. https://www.faa.gov/sites/faa.gov/files/2022-06/Unmanned_Aircraft_Systems.pdf.
5 Federal Aviation Administration. 2022. "Unmanned Aircraft Systems (UAS) | Federal Aviation Administration." Faa.gov. 2022. https://www.faa.gov/uas.
6 *Ibid.*
7 "Unmanned Aircraft System." n.d. https://www.faa.gov/sites/faa.gov/files/2022-06/Unmanned_Aircraft_Systems.pdf.

Cyber Threats

Cyber threats are abstract, boundary-defying, and asymmetrical, but without the same kinetic aspects as drone threats. They are commonly recognized to be more problematic for civilian infrastructure as opposed to military targets because of the high level of cybersecurity protection across critical military systems. However, civilian infrastructure and military readiness are intrinsically linked concepts and have become[8] a focus[9] area for military threat planners and communities. Military installations primarily receive their power, water, and other utilities from commercial or public providers through physical infrastructure and systems that are overseen by local authorities and administered by local networks with much lower cybersecurity standards than those required by the DoW. These networks have already proven vulnerable to cyber-attacks. In 2023 and 2024, the Cyber Threat Intelligence Integration Center documented dozens of cyber-attacks on water,[10] power, telecommunications, food, and healthcare networks[11] across the nation from sources affiliated with Russia or the Iranian Republican Guard. These vulnerable networks provide routes that our adversaries can utilize to strike indirectly at military installations on US soil–perhaps in a manner that is not as visibly devastating as a kinetic attack, but in one that is still significantly impactful to readiness.

Existing and new partnerships between military installations and their local communities must play a key role in developing answers to these questions. Because these emergent threats will not respect an installation's fence line nor the boundaries between tiers of civil-military authorities, installation and community stakeholders must be prepared to counter emergent threats at the local level with proactive, coordinated actions that surmount the logistical and practical barriers to cooperation. These barriers to cooperation are difficult and frustrating to neutralize, and countering threats that exist simultaneously outside and inside military installations is a complex problem. Still, the criticality of these emergent threats is clear: These are problems that must be solved to protect our nation's national defense resources.

Evolution of Cyber Threats in the United States

At least 35 attacks by[12] Russian- or Iranian-affiliated actors in a 5-month period (Nov 23 – Apr 24)

Ransomware attacks rose 74% from 2022-2023[13]

Cyber-attacks on critical infrastructure worldwide increased 30% in 2023[14]

House Homeland Security Committee estimates 500K vacant cybersecurity jobs in the United States[15]

8 "U.S. Army North Highlights New Concept to Protect Critical Infrastructure." 2024. www.army.mil. September 23, 2024.
9 "Secure Cyberspace and Critical Infrastructure | Homeland Security." 2024. U.S. Department of Homeland Security. 2024. https://www.dhs.gov/archive/secure-cyberspace-and-critical-infrastructure.
10 CISA. 2023. "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities | CISA." www.cisa.gov. December 1, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.
11 Office of the Director of National Intelligence. 2024. "Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems." https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf.
12 Office of the Director of National Intelligence. 2024.
13 Homeland Security Committee. 2024. "NEW: House Homeland Releases 'Cyber Threat Snapshot' Highlighting Rising Threats to US Networks, Critical Infrastructure – Committee on Homeland Security." House.gov. 2024. https://homeland.house.gov/2024/11/12/new-house-homeland-releases-cyber-threat-snapshot-highlighting-rising-threats-to-us-networks-critical-infrastructure/.
14 *Ibid.*
15 *Ibid.*

The Role of the Defense Community

Installation–community partnerships are well-positioned to address emergent threats for two significant reasons: first, emergent threats to installations develop outside the boundaries of an installation, necessitating cooperation by military and civil authorities to effectively combat; second, local-level partnerships can attack local problems with flexibility and alacrity that federal organizations do not always possess. Of course, locally developed actions alone will not defeat emergent threats, but local partnerships can develop innovative solutions and the initial response plans that can be expanded and further resourced from higher-level state and federal agencies should a major threat be identified.

This locally driven innovation should focus on answering the following key questions:

How can defense communities and installations construct joint methods to enable swift identification of hostile incursions? This includes the capability to distinguish between a deliberate incursion (hostile) and an unintended incursion (non-hostile / accidental).

Once identified, how do defense communities and installations assist each other to rapidly engage and neutralize deliberate, hostile incursions with an appropriate response? Answers to this question will undoubtedly entail multiple lines of effort with an emphasis on calculating appropriate responses to designated levels of threat. For example, there should be an escalation-of-force process that treats a single drone attempting to surveil at the edge of installation airspace differently than a swarm of drones heading toward a flight line. For the greatest effectiveness and efficiency of resources, defense communities, installations and their respective partners must establish engagement strategies that appropriately match the aggressiveness of an incursion.

And, perhaps most importantly, how can defense communities work with installations to proactively deter incursions? Ideally, suspicious behavior, online warning signs, or other threat indicators in the vicinity of an installation should be detected and perpetrator(s) intercepted before hostile drones are in the air or a computer virus is activated. This concept, dubbed "left of launch", should be the preferred approach for defense community stakeholders as it provides a less expensive approach and a higher chance of success to combat the threat than relying on expensive interception tools that may not be entirely effective. Although this proactive approach will be difficult to establish and implement, it is by far the best long-term option for the safety and security of defense assets within the Continental United States.

ENABLING THE EFFORT

A Nucleus for Solutions

The subsequent reports in this series will focus on examples and case studies of successful actions taken by installation – community partnerships to combat emergent drone and cyber threats. These 'deep dives' will serve to illustrate in detail what roles exist for installation – community partnerships to play in countering specific aspects of the threats and what might be replicable for other localities. However, defense community and installation support organizations should not think that they need to drastically revise their usual approach to installation – community cooperation to best action an agenda against emergent threats. Instead, defense community stakeholders should view partnering on emergent threat prevention as a natural evolution of installation – community relationships. Many installation – community partnerships started with the recognition of a need to develop a common response to the BRAC process and then evolved to focus on mutually-beneficial compatibility, resiliency, and cost-savings efforts. The same evolution can occur again to add emergent threat response to existing partnership efforts. This evolution is natural because the process to build responses to shared emergent threats will contain the same nucleus of actions as the process to effectively respond to any other installation – community challenges. Essentially, installation – community partnership organizations should take action on emergent threat responses the same way they have successfully actioned compatibility responses, IGSA creation, and investments for shared infrastructure. These successful actions include:

- **Coordinate stakeholders to build innovative solutions.**
- **Educate stakeholders and the public on the need to proactively counter emergent threats.**
- **Assist in Resourcing Local Projects**

CONCLUSION

The evolving technology associated with drones and cyber warfare means that emergent threats lie in a murky, uncomfortable boundary between the known and unknown. As discussed in this initial report, and expanded upon later in this series, international boundaries and hardened perimeters are not sufficient to eliminate emergent threats, and the nature of their fast-paced technological advances means that the tools and methods being designed to combat them could be outdated before they are even produced. In this atmosphere, the best defense is flexible, scalable, and, most importantly, localized to specific situations and geographic areas.

Expanded installation-community partnerships must play an active part in developing this localized defense against emergent threats. These partnerships are perfectly positioned to align stakeholders, explore possible actions, and coordinate resourcing for the localized solutions that will provide proactive defensive measures to our military installations and their supporting communities. As discussed, these partnerships already have an applicable framework to approach developing solutions to the challenges of emergent threats. All that is necessary is a deliberate widening of the aperture to include emergent threat response as an initiative alongside resilience, compatibility, and economic opportunity.

Defense communities regularly demonstrate the effectiveness of proactive, localized actions in increasing defense industry economic value and military mission compatibility. Furthermore, they are active champions of military installations and the Soldiers, Sailors, Airmen, Marines, Guardians and Guardsmen who live and work on these installations. They have an unmatched ability to advance national defense priorities and unite stakeholders across the spectrum of public and private industry to resolve shared defense-related issues. These defense communities must now add emergent threat response to their portfolios of successful civil-military partnership actions.

ASSOCIATION OF DEFENSE COMMUNITIES

The Association of Defense Communities (ADC) builds resilient communities that support America's military. It is the connection point for leaders from communities, states, the military and industry on community-military issues by enhancing knowledge, information sharing, and best practices. With nearly 300 communities, states, regions and affiliated industry organizations, ADC represents every major defense community/state in the nation.

defensecommunities.org

Matrix
Excellence by Design

Matrix Design Group is an award-winning interdisciplinary firm, providing professional engineering, consulting, environmental and planning and program management for both the public and private sectors. As specialists in sustaining installations, community advocacy and BRAC services, Matrix is a complete provider of innovation and solutions. With the industry's most comprehensive experience, the Matrix team has the necessary expertise to assess installation closure susceptibility and the tools and knowledge to help defense communities remain vibrant.

matrixdesigngroup.com

Developed in collaboration with:

Matrix

Excellence by Design

ASSOCIATION OF DEFENSE COMMUNITIES

1300 Connecticut Ave NW
Suite 200
Washington, DC 20036

defensecommunities.org