Physical Protection of Critical Infrastructure:

Reframing Critical Infrastructure Security for the Drone Threat

For decades, physical security for public venues and critical infrastructure has focused on controlling access. Fences, cameras, screening checks, and controlled entry points are designed to address threats from individuals seeking physical proximity to inflict damage.

Small unmanned aircraft systems (sUAS) change that assumption. Today, individuals outside a facility, with no intent to gain access, can surveil or threaten facilities and events from significant stand-off distances. Security is no longer defined solely by who gets in, but by how effectively threats from outside the facility are mitigated.

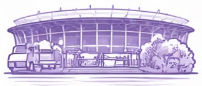
> *"Countering the drone threat is about more than exquisite systems. You can take steps now to prepare and protect critical infrastructure."*

This shift requires local authorities to think about physical protection in new ways that include solutions that are layered, outward-looking, and focused on denying access, visibility, and opportunity, well beyond the entry gate or perimeter. Importantly, many of these measures do not require specialized counter-UAS systems.

The considerations below highlight practical, non-technical actions that local authorities can implement now to reduce drone risk across a range of critical infrastructure and public facilities, often at modest cost and with immediate benefit.

Determining Vulnerabilities – Seeing the Facility from the Outside In:

Effective protection begins with identifying where a UAS operator would see opportunity. Unlike traditional threats, drone operators look for stand-off locations, exposed assets, lines of sight, and predictable patterns to have the greatest impact.



Concentrations of People and Public Activity: Event venues, transit hubs, pedestrian corridors, parking areas, and other publicly accessible spaces create predictable concentrations of people that are exposed from above. These areas often sit outside hardened perimeters and may receive less security attention than core facilities, yet they remain attractive targets due to density or disruption potential.

Critical Systems and Enabling Infrastructure: Power generation equipment, substations, backup generators, pumps, signaling and switching equipment, communications nodes, and the systems that control them are often distributed across a site and located outdoors or in lightly protected structures. Whether physically prominent or low-profile, disruption or surveillance of these assets can have cascading effects on operations, safety, and public confidence.

Movement Nodes and Access Routes: Ingress and egress routes such as facility gates, rail platforms, transfer points, service roads, and loading areas create predictable movement patterns. These chokepoints are vulnerable to aerial observation or interference and deserve as much protection planning as steady-state operations.

Enduring Government and Public Institutions: Facilities such as prisons, courthouses, government complexes, and other institutions face persistent exposure. Their fixed locations, routine schedules, and surrounding public access create enduring vulnerabilities that drones can exploit over time.

Natural Resources and Public Goods: Reservoirs, water treatment facilities, environmental assets, and other public goods are often geographically expansive and difficult to enclose. While traditionally protected through access control and monitoring, these sites are increasingly exposed to aerial interference.

Physical Protection of Critical Infrastructure:

Reframing Critical Infrastructure Security for the Drone Threat

Physical Protection Measures – HOP: Harden, Obscure, Perimeter

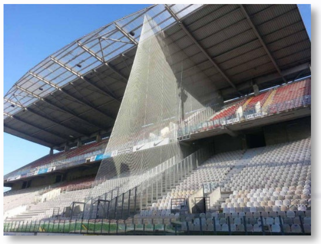
Military force protection emphasizes shaping the environment so the adversary struggles to achieve their objective. The same logic applies to drone threats. Physical measures can deny flight paths, reduce visibility, complicate targeting, and increase operator risk, often without employing exquisite counter-UAS technology.

Hardening: Creating Physical Obstacles to Flight

Hardening does not mean enclosing an entire facility, but selectively introducing obstacles that disrupt predictable aerial access. Examples include:

- **Permanent or semi-permanent structural shielding**, including concrete walls, enclosures, or hardened roofs designed to protect critical systems from overhead approach, observation, or objects released from a UAS.
- **Overhead netting or tensioned cables** above high-risk areas such as entrances, power equipment, and event venues.
- **Closing or covering retractable roofs** or partial roof openings when operationally feasible.
- **Lightweight wire, mesh, or fishing line** in limited zones to create unpredictable flight hazards.

Even modest obstacles can deter low-cost, consumer-grade drones and force higher-risk flight profiles.



Top: Netting used to protect fans from projectiles can be repurposed to disrupt sUAS flight and observation. Bottom: Anti-drone netting installed to protect critical infrastructure from overhead threats..

Top: Temporary tenting obscures backup generators supporting a data center. Bottom: U.S. military camouflage netting used to reduce aerial visibility of critical assets.

Obscuration: Reducing What a Drone Can See or Exploit

If a drone cannot easily identify targets, crowds, or critical systems, its effectiveness drops sharply. Practical obscuration measures include:

- **Temporary walls, scrims, or barriers** that block line of sight into sensitive areas.
- **Visual clutter** that breaks up clear overhead views, making targeting more difficult.
- **Revisiting traffic, workforce, or public flow design** to prioritize dispersion and rapid movement rather than prolonged queuing or static positioning.
- **Decoys or diversions**: structures or equipment that appear important but are not and can draw attention away from truly critical assets.

Obscuration is especially powerful because it reduces risk without escalating response or requiring specialized authorities.

> *"It's not the C-sUAS platform; it's the approach. We have to apply lessons and TTPs from the military and operational environments to counter advanced threats."*

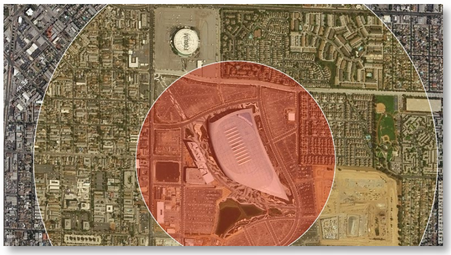
Joint Interagency Task Force 401

Perimeter Thinking: Extending Security Beyond the Fence Line

In counter-UAS defense, the perimeter does not begin or end at the facility fence or property line. The most dangerous drone operator is rarely inside the secured footprint. Key considerations include:

- **Establishing layered perimeters** that extend outward into parking areas, nearby public spaces, and elevated terrain.
- **Patrols at stand-off distance** focused on anticipating ground control stations (GCS), not just access enforcement or crowd management.
- **Temporary checkpoints or screening** in outer zones during high-risk windows.
- **Training security officials** to recognize operator behaviors, such as:
    - Individuals or small groups loitering without a clear purpose
    - Frequent upward scanning or sustained visual focus on a facility
    - Use of handheld controllers, tablets, or unusual antennas
    - Vehicles positioned for extended stationary observation

> *"Sometimes the best defense is making a target harder to see, harder to reach, or harder to understand."*



An aerial view of SoFi Stadium shows the distinction between the traditional inner security zone and a broader outer area where most commercial drones, often operated from 1–3 miles away, are likely controlled. Effective security planning extends into surrounding neighborhoods, not just the fence line.

Pushing the effective perimeter outward forces drones to operate at greater distance, which:

- Strains battery life
- Degrades video and control links
- Increases the chance of operator exposure
- Creates a larger safety buffer if a drone is downed

This approach mirrors military standoff principles and can be implemented with existing personnel and authorities.

Key Takeaways for Local Authorities:

- Drone threats shift risk outside facilities and venues, requiring outward-looking security in depth.
- Physical protection measures can meaningfully reduce risk without relying on advanced counter-UAS systems.
- Hardening, obscuration, and extended perimeters work best when layered together.
- Environmental design choices can deter or disrupt drone operations before technology or force is required.

Training officers to observe human behavior, not just aircraft, is critical.

Additional Resources:

Cybersecurity and Infrastructure Security Agency (CISA) Be Air Aware™:
https://www.cisa.gov/topics/physical-security/be-air-aware

The information in this guide is compiled by JIATF 401 for informational purposes. It outlines best practices and considerations for physical security measures against sUAS threats but is not a comprehensive or universally applicable standard. These recommendations should not replace a professional security assessment tailored to your specific asset and threat environment.