

Drones: The Emerging Threat Not Only to a Country's Internal Security but Also to Its Critical Infrastructure

A strategic risk and resilience analysis



Author: Chief Commissioner Pedro Barrueco Perez, MSc. Criminology | Bachelor's / Higher University Technician in Police Sciences | Postgraduate Degrees: Management – Project Management – Organizational Change – Strategy and Strategic Planning | Diploma Courses: Criminalistics / Forensic Expert – Criminal Profiling – Human Rights – Intelligence – Strategic Intelligence – National / Global Security – Organized Crime | Risk Management – ISO 31000.

September 2026

Contents

Abstract

Executive assessment

1 Introduction

2 From battlefield technology to internal security threat

3 Threat actors and missions

3.1 State actors and proxies

3.2 Terrorist and extremist actors

3.3 Organized crime and transnational criminal organizations

3.4 Lone actors and insiders

3.5 Mission categories

4 Why critical infrastructure is exposed

4.1 Energy

4.2 Transportation and aviation

4.3 Communications and data infrastructure

4.4 Water, chemical, and hazardous material facilities

4.5 Nuclear facilities

4.6 Public venues and government facilities

5 The economics of asymmetric attack

6 Detection, identification, and the limits of technology

7 Countermeasures against drones

7.1 Detection and identification measures

7.2 Electronic and cyber countermeasures

7.3 Kinetic interception and physical capture

7.4 Passive physical countermeasures

7.5 Obscuration, deception, and signature management

7.6 Operational countermeasures

7.7 Recovery as a countermeasure

7.8 Countermeasure selection

8 The legal and governance gap

9 Rigid protective cages and other passive defenses

8.1 Advantages

8.2 Limitations

10 A layered protection model

10.1 Intelligence and threat assessment

10.2 Airspace and perimeter awareness

10.3 Multisensor detection and command and control

10.4 Hardening, obscuration, and dispersion

10.5 Operational response

10.6 Recovery and continuity

11 A risk-based implementation framework

12 Performance measures and warning indicators

13 Strategic implications

Conclusion

Abstract

The rapid diffusion of commercial, first-person-view, one-way attack, autonomous, and increasingly networked drones has created a security problem that no longer belongs only to military air defense. Small, unmanned aircraft can conduct surveillance, move contraband, interfere with aviation and emergency operations, deliver explosives, support cyber or electronic attacks, and strike exposed components of critical infrastructure. Their low cost, availability, precision, and capacity to approach from above give state and non-state actors a means to impose consequences far greater than the price of the platform.

This paper examines drones as a converging threat to internal security and critical infrastructure. It draws on governmental guidance, academic literature, law-enforcement assessments, documented incidents, and operational lessons from recent conflicts. *Particular attention is given to energy, transportation, communications, water, chemical, nuclear, manufacturing, and public-assembly environments. The analysis also considers the United States legal-authority gap: most private operators can detect or report a suspicious drone but cannot lawfully jam, seize, or destroy it.*

The central finding is that no single counter-drone technology can provide reliable protection. *Effective risk reduction requires a layered system combining intelligence, detection, classification, physical hardening, obscuration, perimeter awareness, operational procedures, lawful response options, redundancy, crisis management, and rapid recovery. Rigid protective cages and netting can be valuable against defined threats, especially when selectively applied to critical components, but they are one layer of protection rather than a complete defense.*

Keywords: drones, UAS, counter-UAS, internal security, critical infrastructure, terrorism, organized crime, hybrid warfare, resilience, protective cages

Executive assessment

The drone threat has crossed an important boundary. A capability once concentrated in state militaries is now available to commercial operators, criminals, extremist groups, proxies, and individuals. The same systems that inspect power lines, support firefighters, map disaster damage, and deliver medical supplies can be repurposed for hostile surveillance, disruption, smuggling, sabotage, or attack. This dual-use character complicates detection and response because the presence of a drone does not by itself establish hostile intent.

The security problem is driven by asymmetry. A relatively inexpensive aircraft can reach a target from an angle that conventional fences, guards, and vehicle barriers were not designed to cover. It can expose security routines before an attack, deliver a small payload with precision, force an airport shutdown without firing a weapon, or damage a single component whose failure interrupts an entire service. The 2019 attack on Saudi oil facilities demonstrated the strategic effect of striking concentrated energy infrastructure: approximately 5.7 million barrels per day of production were temporarily disrupted, representing more than five percent of global supply at the time (CRS, 2019; Reuters, 2019). The strategic lesson is broader than the details of attribution or weapon mix. Infrastructure can be physically large yet functionally dependent on a small number of vulnerable nodes.

Conflict in Ukraine has accelerated adaptation on both sides. Radio-frequency jamming has encouraged the use of autonomous navigation and fiber-optic control. Protective nets and barriers have led attackers to exploit openings, ventilation points, sequential strikes, and alternative approach paths. This cycle shows why a static procurement solution will fail. Defense must be organized as an adaptive risk-management process.

The United States faces an additional constraint. Federal law reserves important counter-drone authorities to a limited number of federal departments under defined circumstances. State, local, tribal, territorial, and private security organizations generally lack authority to jam radio links, take control of aircraft, or employ destructive measures. GAO has warned that counter-drone systems can also create unintended consequences, including interference with communications, privacy concerns, falling debris, and collateral damage (GAO, 2022). A facility therefore needs both a technical architecture and a legally coordinated response plan.

The practical objective cannot be perfect interception. It must be to reduce the probability of successful attack, protect the components that matter most, limit cascading consequences, preserve essential functions, and restore service quickly. As the director of Joint Interagency Task Force 401 states, “There is no silver bullet to address the C-UAS challenge” (JIATF 401, 2026, p. 2). That is the correct starting point for national policy and corporate security.

1 Introduction

Drones have become part of ordinary economic and public life. They support agriculture, surveying, infrastructure inspection, media production, emergency response, law enforcement, border security, and logistics. The Federal Aviation Administration treats their integration into national airspace as a permanent transportation and safety issue rather than a temporary technological novelty (FAA, 2026a). Joint Interagency Task Force 401 similarly recognizes legitimate missions including firefighting, search and rescue, disaster relief, border security, and critical-infrastructure assessment (JIATF 401, 2026, p. 7).

The same accessibility that produces legitimate value creates a security vulnerability. The aircraft, navigation components, cameras, batteries, communications links, and software required to assemble a capable system are widely available. Modifications can be learned through online communities and transferred rapidly from conflict zones to criminal environments. The operator does not need to defeat a perimeter fence or remain physically close to the target. In some configurations, the aircraft can fly a programmed route without a continuous command link. In others, fiber-optic control makes conventional radio-frequency detection and jamming far less useful.

This paper uses the term drone broadly, while recognizing the technical distinction between an unmanned aircraft and the larger unmanned aircraft system, which includes the control station, communications link, payload, navigation, software, and supporting elements. That system perspective matters. Defenders often concentrate on the aircraft even though the operator, launch site, data link, supply chain, software, and recovery procedures may present more practical points of intervention.

The argument developed here is that drones should be incorporated into internal-security planning and critical-infrastructure resilience as a persistent threat category. They are not merely another airborne weapon. They are platforms that can combine observation, communication, cyber access, payload delivery, deception, and psychological pressure. The threat also cannot be assessed only by counting attacks. Surveillance flights, incursions, tests of response time, and unexplained activity near sensitive sites may be preparatory or coercive even when no immediate physical damage occurs.

2 From battlefield technology to internal security threat

Modern drone proliferation reflects the convergence of several developments: inexpensive sensors, improved batteries, satellite navigation, compact processors, commercial autopilots, digital video links, open-source software, additive manufacturing, artificial intelligence, and mass-produced components. Economies of scale have lowered the financial and technical barriers that once restricted aerial surveillance and precision strike capabilities to governments.

JIATF 401 describes the change directly: small drones have evolved from state-sponsored intelligence platforms into versatile systems used by state militaries, proxies, non-state armed groups, transnational criminal organizations, and lone actors (2026, p. 5). Europol reaches a parallel conclusion from the law-enforcement perspective. Criminals already employ drones to move illicit goods, monitor police activity and drug-production sites, and in some cases attack law-enforcement personnel (Europol, 2025).

This diffusion does not mean that every actor has the same capability. A recreational user organized criminal group, terrorist cell, state proxy, and military intelligence service differ in training, access, payload, targeting information, and tolerance for failure. A sound assessment therefore asks four separate questions: Who has the motivation? Who has access to the necessary platform and payload? Who can obtain target intelligence? Who can operate without being identified before or after the event?

Internal-security agencies must also distinguish between unsafe, unlawful, suspicious, and hostile activity. An inexperienced pilot near an airport may create consequences comparable to deliberate disruption, but the response and investigative framework will differ. A drone over a refinery may be conducting an authorized inspection, recreational filming, hostile reconnaissance, or attack preparation. Classification must be based on behavior, location, timing, payload indicators, flight profile, intelligence, and the protected site's operating context.

The security implications extend beyond kinetic attack. Persistent aerial observation can reveal shift changes, guarding routines, loading patterns, alarm responses, vulnerable roof structures, temporary construction openings, or the location of emergency equipment. In this role, a drone is an intelligence-collection tool that can support a later ground assault, theft, sabotage, kidnapping, or cyber intrusion. The first hostile act may therefore be information collection rather than payload delivery.

3 Threat actors and missions

3.1 State actors and proxies

States can use drones overtly in armed conflict or covertly through intelligence services, proxies, criminal facilitators, and deniable commercial networks. The platform supports reconnaissance, target development, sabotage, coercion, and influence operations. Attribution is difficult when components are commercially available and the aircraft can be assembled far from the sponsoring state. This ambiguity makes drones useful in the space between routine competition and open conflict.

Hybrid pressure against infrastructure may seek disruption more than destruction. Repeated incursions can force airports to suspend operations, compel security expenditures, test detection coverage, generate public anxiety, and expose decision-making delays. The September 2025 disruption at Copenhagen Airport was treated by Danish leadership as a serious incident involving critical infrastructure, although responsibility had not been established at the time of reporting (The Guardian, 2025). The evidentiary caution is important: an unexplained incursion can be operationally significant without proving state attribution.

3.2 Terrorist and extremist actors

Terrorist use can range from propaganda filming and reconnaissance to assassination attempts, attacks on crowds, delivery of improvised explosives, or release of hazardous material. The 2018 attempted attack against Venezuelan President Nicolás Maduro illustrated how commercially derived multicopters could be adapted for a politically symbolic attack in an urban environment. RAND observed that the event showed both the accessibility of the technology and the difficulty of defending public officials and gatherings against small aircraft (Clarke, 2018).

The capability should not be exaggerated. Payload, range, weather, navigation, operator skill, and reliability remain constraints. Yet terrorism measures success through fear, publicity, and political consequence as well as casualties. A technically unsuccessful drone attack may still expose a protective-security failure, interrupt a national event, or produce widespread alarm.

3.3 Organized crime and transnational criminal organizations

Criminal groups use drones because they reduce exposure of personnel and extend surveillance beyond line-of-sight positions on the ground. Documented missions include moving contraband into prisons, scouting law-enforcement activity, monitoring borders, supporting drug trafficking, and surveilling rival groups. JIATF 401 specifically identifies drug smuggling, observation of border checkpoints and patrols, and prison contraband as homeland hazards (2026, p. 8).

The transition from support tool to weapon is operationally plausible. A group already capable of acquiring drones, modifying payloads, protecting communications, and conducting counter-surveillance has several of the prerequisites for targeted violence. Security planning should therefore examine criminal drone activity as a capability-development indicator, not only as an isolated aviation violation.

3.4 Lone actors and insiders

Commercial availability allows a technically competent individual to operate without the organizational signature associated with a larger plot. An insider creates an additional problem because authorized knowledge can identify the exact component whose disruption would have the greatest effect. Insider-risk programs should consider access to flight schedules, facility drawings, inspection imagery, control-system layouts, maintenance windows, and counter-drone coverage.

3.5 Mission categories

Threat missions can be organized into six categories:

- 1. intelligence, surveillance, reconnaissance, and target development;**
- 2. direct attack, one-way attack, or payload release;**
- 3. smuggling and logistical support;**
- 4. disruption of aviation, emergency response, or public events;**
- 5. communications relay, electronic interference, or support to cyber intrusion;**
- 6. deception, harassment, coercion, and testing of defensive reactions.**

These missions may occur sequentially. A drone can first map a facility, then test its response, and later support or conduct an attack. Incident records should therefore be analyzed across time rather than closed as unrelated events after each flight.

4 Why critical infrastructure is exposed

CISA defines critical infrastructure through the consequence of its loss: assets, systems, and networks are critical when their incapacitation would have a debilitating effect on security, economic security, public health, or safety (CISA, 2026). The United States framework identifies sixteen sectors, including energy, communications, water, transportation, chemical, nuclear, emergency services, financial services, food and agriculture, healthcare, critical manufacturing, and information technology.

Many facilities were designed against fire, weather, trespass, vandalism, vehicle intrusion, theft, and in some cases blast. Their protective architecture often assumes a threat moving horizontally through controlled space. Small aircraft exploit the vertical dimension. Rooftop systems, transformers, antennas, tank vents, control cabinets, cooling equipment, outdoor process areas, and emergency generators may be visible and accessible from above.

Infrastructure is also vulnerable because function is unevenly distributed. A large site may depend on a few components with long replacement times or limited redundancy. The most important target may not be the most visually impressive structure. It may be a transformer bushing, a pump controller, a telecommunications link, a safety instrument, or an exposed connection between otherwise protected systems.

The risk is therefore systemic. Damage to electricity can interrupt water treatment, telecommunications, healthcare, transportation, fuel distribution, banking, and emergency services. *A drone attack does not have to destroy an entire facility to produce cascading consequences. It only has to disable the node that other services require.*

4.1 Energy

Energy systems combine dispersed geography with high-value components. Generation plants, substations, pipelines, storage sites, compressor stations, and distribution assets cannot all receive the same level of protection. The 2019 Abqaiq and Khurais attack temporarily removed approximately 5.7 million barrels per day from Saudi production. Although the operation reportedly involved both drones and cruise missiles, its strategic effect demonstrates the vulnerability of concentrated processing capacity (CRS, 2019; Reuters, 2019).

Ukraine provides a different lesson. Repeated attacks on electrical infrastructure have produced an adaptation cycle involving concrete protection, electronic warfare, netting, deception, dispersal, and rapid repair. Reporting reviewed in the source material describes fiber-optic FPV drones used against substations and sequential attacks intended to breach netting before a following aircraft entered through the opening (Hunder, 2026; Barrueco Perez, 2026). The broader conclusion is that passive barriers work only when their geometry, stand-off distance, anchoring, inspection, and repair cycle correspond to the actual threat.

4.2 Transportation and aviation

Airports are exposed to both accidental and deliberate incursions. A small drone can create collision risk, force runway closures, divert aircraft, delay passengers, and consume police and air-traffic resources. The economic effect can be severe even when the aircraft carries no weapon. This makes disruption an attractive mission for activists, criminals, coercive actors, or hostile services seeking deniable impact.

Transportation risk also includes ports, rail systems, bridges, tunnels, pipelines, and logistics hubs. Drones can observe cargo movement, locate hazardous materials, monitor

security patrols, or interfere with emergency operations. During wildfires and other disasters, unauthorized drones can force response aircraft to withdraw from an area, turning irresponsible or malicious flight into an operational-safety threat.

4.3 Communications and data infrastructure

Antennas, microwave links, satellite ground equipment, data-center cooling systems, backup generators, and cable landing facilities present different combinations of visibility and criticality. A drone can support physical attack, collect imagery, carry a rogue communications device, or position equipment close enough to exploit wireless networks. Defenders should therefore integrate physical security, radio-frequency monitoring, cybersecurity, and supply-chain controls rather than treating them as separate disciplines.

4.4 Water, chemical, and hazardous-material facilities

Water and chemical facilities raise consequence-management concerns beyond equipment loss. A payload striking a tank, valve, pipe, control point, or treatment process could cause release, contamination, fire, or shutdown. Claims involving chemical, biological, radiological, or nuclear payloads require careful assessment because feasibility varies considerably. Nevertheless, JIATF 401 includes CBRNE hazards among evolving drone payload possibilities (2026, p. 8). Planning should consider credible material, delivery efficiency, weather, dispersion, and detection rather than relying on worst-case labels alone.

4.5 Nuclear facilities

Nuclear sites generally have stronger security and federal support than ordinary commercial facilities, but drone incidents still create surveillance, payload, distraction, and response challenges. The principal risk may be less a catastrophic reactor breach than reconnaissance, interference with security operations, attack on supporting infrastructure, or simultaneous use of drones to distract from a ground event. Protective planning must remain consequence-based and avoid unsupported assumptions about what a small payload can penetrate.

4.6 Public venues and government facilities

Stadiums, political events, public celebrations, and government buildings combine symbolic value with dense populations. Even a false alarm can trigger evacuation, crowd movement, or panic. Federal resources cannot cover every event. Reporting to the U.S. Senate in 2025 indicated that federal counter-drone teams could support only a very small fraction of potentially eligible special events (Reuters, 2025). Local planning must therefore emphasize detection, rapid assessment, crowd procedures, evidence collection, and pre-established federal notification.

5 The economics of asymmetric attack

Drone risk is shaped by an unfavorable exchange ratio. Defenders may need radar, passive radio-frequency sensors, electro-optical cameras, command-and-control software, trained operators, legal review, maintenance, and multiple effectors. An attacker may need only

one modified aircraft and accurate knowledge of a critical component. Even when a drone fails, the defender incurs costs from investigation, shutdown, inspection, and heightened readiness.

This imbalance is not captured by comparing the cost of the drone with the market value of the damaged equipment. Consequence includes service interruption, safety exposure, regulatory reporting, environmental response, reputational damage, customer loss, and cascading effects on dependent sectors. A risk assessment should therefore use business-impact analysis and system dependencies, not replacement cost alone.

The same logic explains why saturation matters. Active systems have detection limits, engagement timelines, ammunition constraints, interference risks, and operator workloads. Multiple drones can approach from different directions, mix decoys with attack platforms, or arrive after an initial strike has damaged sensors. JIATF 401 defines a swarm as multiple systems coordinating their actions toward a common objective, while distinguishing it from an uncoordinated group of individual aircraft (2026, p. 9). That distinction matters for capability assessment, but either form can overload a poorly designed response.

6 Detection, identification, and the limits of technology

Counter-UAS detection commonly combines radar, passive radio-frequency sensing, electro-optical and infrared cameras, acoustic sensors, Remote ID information, and data fusion. Each method observes a different signature and carries limitations.

Radar can provide range and track information but may struggle with small, slow targets, clutter, terrain, buildings, birds, and regulatory constraints. *Passive radio-frequency systems* can detect or locate common control links without transmitting, yet they may fail against autonomous routes, unfamiliar protocols, low-probability-of-intercept links, or fiber-optic control. *Cameras provide visual confirmation* but depend online of sight, lighting, weather, range, and operator attention. *Acoustic sensors* can help at short range but are affected by wind, machinery, traffic, and urban noise. *Remote ID can support identification* of compliant aircraft, but it is not proof that an aircraft is safe, and a hostile operator may disable, alter, or spoof the signal.

Academic reviews consistently support multisensor fusion. Wang, Liu, and Song (2021) identify acoustic, visual, passive radiofrequency, radar, and fused detection approaches, while emphasizing that no method performs reliably across all environments. Nassi et al. (2021) similarly identify weather, ambient light, background clutter, birds, and permitted drone traffic as persistent challenges. The operational implication is simple: detection architecture must be designed for the site, not selected from a generic product demonstration.

Detection is only the first decision. The facility must track and classify the aircraft, determine whether it is authorized, evaluate behavior and payload indicators, and decide what action is lawful and proportionate. JIATF 401 organizes military counter-UAS activity as a continuous cycle of detect, track and identify, defeat, and report (2026, p. 49). Civilian operators should adapt the sequence but recognize that “defeat” may mean warning personnel, stopping a process, moving people, protecting a critical component, or requesting federal support rather than physically interfering with the aircraft.

False positives and uncertain classification can produce their own risk. A defensive action that disrupts legitimate communications, damages a lawful aircraft, or causes debris to fall into a crowd may be worse than continued observation. Sensor confidence, escalation

thresholds, decision authority, and logging requirements should be established before an incident.

7 Countermeasures against drones

Countermeasures should be understood as a system of measures rather than a weapon or device. In practical terms, they include every action that reduces the probability that a drone will locate, reach, damage, or disrupt a protected function. Some measures detect and classify the aircraft. Others interfere with its control, physically intercept it, obstruct its route, protect the target, reduce the consequences of impact, or accelerate recovery. The appropriate combination depends on the threat, operating environment, legal authority, and potential consequences of the defensive action itself.

Table 1 Countermeasure categories and principal limitations

<i>Category</i>	<i>Examples</i>	<i>Primary limitations</i>
<i>Detection and identification</i>	Radar, RF sensing, EO/IR cameras, acoustic arrays, Remote ID, data fusion	False alarms, clutter, weather, line of sight, autonomous or fiber-optic aircraft
<i>Electronic and cyber</i>	Command-link disruption, GNSS interference, spoofing, protocol takeover	Legal restrictions, collateral interference, encryption, autonomy, uncontrolled landing
<i>Kinetic and capture</i>	Firearms, interceptors, nets, projectiles, missiles, directed energy	Falling debris, missed shots, fire, fragmentation, airspace and public-safety risk
<i>Passive physical</i>	Cages, netting, cables, overhead cover, shielding, protected openings	Threat-specific design, secondary hazards, maintenance, access, repeated strikes
<i>Obscuration and deception</i>	Visual screening, signature reduction, camouflage, decoys, dispersion	Public imagery, pattern exposure, false confidence, limited value without redundancy
<i>Operational and recovery</i>	Shutdown, isolation, shelter, relocation, spares, redundancy, rapid restoration	Decision delays, production impact, training needs, dependence on rehearsed coordination

The military model described by JIATF 401 uses a continuous cycle of detect, track and identify, defeat, and report (2026, p. 49). Civilian critical-infrastructure operators can use the same logic, but the defeat phase requires modification. *A private operator may have authority to change site operations, move personnel, isolate hazardous processes, activate physical barriers, or provide tracking data to law enforcement, while lacking authority to jam, seize, or destroy the aircraft. For this reason, countermeasure planning must connect technology with pre-established decisions and authorized actions.*

7.1 Detection and identification measures

Detection is the first layer of an active counter-drone system. *Radar, passive radio-frequency sensors, electro-optical and infrared cameras, acoustic arrays, Remote ID receivers, and data-fusion platforms can provide warning and support classification.* No sensor should be treated as independently decisive. A radio-frequency detector may not see an autonomous or fiber-optic aircraft. Radar may confuse small drones with birds or lose them in clutter. Cameras require line of sight and favorable environmental conditions. Remote ID identifies compliant broadcasts but cannot be relied upon against a hostile operator.

The strongest configuration normally combines complementary sensors. Radar or radio-frequency equipment may provide the initial alert and track, while cameras support visual confirmation. Software can correlate tracks, authorized-flight lists, Remote ID data, restricted areas, and behavioral indicators. The objective is not merely to detect an object. It is to determine whether the aircraft is authorized, careless, suspicious, hazardous, or hostile with enough time to act.

Detection systems also create governance obligations. They may collect images, device identifiers, location data, or communications-related information involving lawful operators and nearby communities. Organizations need rules for collection, access, retention, sharing, deletion, and audit. These requirements should be part of system design rather than added after deployment.

7.2 Electronic and cyber countermeasures

Non-kinetic systems may disrupt the command link, interfere with satellite navigation, deceive navigation inputs, take control of the aircraft, or force it to land or return to a programmed location. These measures can be effective against aircraft that depend on known radio frequencies and predictable protocols. They can also provide a response without the blast, gunfire, or visible debris associated with kinetic interception.

Their limitations are substantial. Jamming may interfere with legitimate communications, navigation, emergency systems, or nearby operations. A drone may enter an uncontrolled flight state, continue autonomously, return to its launch point, or fall into a populated or hazardous area. Spoofing and protocol takeover depend on technical access to the target system and may fail against encrypted, unfamiliar, modified, pre-programmed, or fiber-optic platforms. Electronic defeat should therefore be assessed as a conditional capability, not a universal solution.

Cyber countermeasures introduce additional issues of speed, attribution, system knowledge, and lawful access. The engagement window may last seconds. A defensive tool must identify the correct link and avoid affecting lawful aircraft or unrelated networks. The organization must also preserve logs so the action can be reviewed after the incident.

7.3 Kinetic interception and physical capture

Kinetic measures include firearms, automatic cannon, missiles, interceptor drones, projectiles, and other systems intended to destroy or disable the aircraft. Physical-capture methods include nets launched from the ground or another drone, entanglement devices, and trained interceptor platforms. Directed-energy systems such as high-energy lasers or high-

power microwave systems occupy a separate technical category but share the objective of physically or electronically disabling the aircraft.

These measures may provide the only practical response to an autonomous, radio-silent, or fiber-controlled attack drone. They also create serious secondary risks. Missed projectiles, falling drones, unexploded payloads, fire, fragmentation, electromagnetic effects, and damage to nearby aircraft or infrastructure can turn a successful interception into a separate emergency. A mitigation system suitable for a remote military installation may be unacceptable at an airport, refinery, urban substation, stadium, chemical plant, or densely populated site.

The decision must consider where the intercepted drone will fall, what its payload may do after impact, and whether the defensive action could trigger the device. Engagement zones should be identified in advance wherever possible. Emergency, fire, explosive-ordnance, aviation, and medical consequences must be integrated into the response plan.

7.4 Passive physical countermeasures

Passive countermeasures seek to reduce vulnerability without detecting or engaging each aircraft. They include rigid cages, anti-drone netting, tensioned cables, overhead cover, blast and fragmentation shielding, protected ventilation, relocation of exposed components, visual screening, camouflage, decoys, dispersion, and increased separation between redundant systems.

Their main advantage is persistence. A physical barrier does not require a communications link, engagement authority, or operator reaction. It can retain value against autonomous and fiber-optic drones and cannot be exhausted in the same way as ammunition. Passive protection is particularly useful for components with high criticality, limited redundancy, and predictable aerial approaches.

Passive measures are not automatically safe or effective. They require engineering for aircraft mass, speed, payload, impact angle, mesh size, stand-off distance, anchoring, fire, blast, electrical clearance, grounding, weather, corrosion, ventilation, drainage, maintenance, and emergency access. They must also be inspected after an attempted penetration because a first strike may create a route for a second aircraft.

7.5 Obscuration, deception, and signature management

A drone cannot precisely strike what its operator or autonomous system cannot reliably identify. Obscuration reduces the visual, infrared, electromagnetic, and behavioral signatures that reveal a critical component. Deception presents false indicators, decoys, or misleading patterns intended to divert surveillance or expend an attacker's limited resources.

JIATF 401 identifies hiding, blending, disguising, disrupting recognizable patterns, and decoying as distinct survivability techniques (2026, p. 60). These methods can be adapted to fixed infrastructure. Publicly available imagery, facility tours, contractor photographs, procurement documents, maintenance records, and social-media posts should be reviewed because they may defeat physical concealment by revealing the site's functional layout.

Obscuration is strongest when combined with redundancy and selective hardening. A decoy that does not change the consequences of losing the real component offers limited value.

The goal is to increase targeting uncertainty while ensuring that a successful strike against one visible object does not stop the essential function.

7.6 Operational countermeasures

Operational measures may be the only actions immediately available to a civilian facility. *They include suspending exposed work, moving personnel under cover, closing vulnerable access points, isolating hazardous processes, shutting valves, separating vehicles, relocating critical equipment, activating fire watches, protecting emergency generators, preserving command-and-control communications, and notifying authorized agencies.*

These actions require specific triggers. An unverified detection may justify heightened observation but not a full shutdown. A drone descending toward a tank farm with a visible payload requires a different response. Procedures should define who assesses the event, who can stop operations, what information is reported, and how normal activity resumes after the aircraft departs.

7.7 Recovery as a countermeasure

Recovery reduces the value of a successful attack. Spare components, alternate power, redundant communications, manual control, mutual-aid agreements, restoration contracts, pre-positioned repair material, and rehearsed crisis communications can prevent a local strike from becoming a prolonged regional disruption. Recovery planning is especially important for networks with hundreds of geographically dispersed assets that cannot all receive active protection.

A downed or crashed drone must be treated as a potential explosive device, intelligence source, and crime scene. Personnel should not handle it unless trained and authorized. The scene should be isolated, emergency services notified, imagery preserved, sensor logs secured, witnesses identified, and chain-of-custody procedures applied. Technical exploitation may reveal the aircraft's components, route, imagery, operator practices, or links to earlier incidents.

7.8 Countermeasure selection

Countermeasure selection should be based on a site-specific comparison of effectiveness, legality, collateral risk, response time, integration, maintainability, and lifecycle cost. A system that performs well during a controlled demonstration may fail in rain, urban clutter, electromagnetic congestion, or the limited sight lines of an operating facility. Testing must use threat-representative aircraft and conditions while remaining within aviation and safety rules.

The final design should produce defense in depth. Detection provides time. Identification supports a defensible decision. Electronic or kinetic measures may stop an aircraft where legally authorized. Passive barriers reduce the chance that it reaches the critical component. Operational actions protect people and processes. Redundancy and recovery limit the consequences if every preceding layer fails.

8 The legal and governance gap

The United States does not grant general counter-drone authority to private security departments or ordinary state and local agencies. Federal criminal, aviation, communications,

and surveillance laws can apply to jamming, intercepting control links, seizing an aircraft, or damaging it. Congress has provided tailored authority to the Departments of Defense, Energy, Justice, and Homeland Security under specified conditions. GAO summarized the practical consequence in 2022: outside those authorized federal entities, organizations generally cannot deploy many mitigation measures even when responsible for protecting an important facility.

This limitation is not a minor compliance issue. It changes system design. A facility that purchases detection equipment without a response concept may learn that a drone is approaching but have no lawful means to stop it. The organization must know which federal agency has jurisdiction, what information that agency requires, how quickly support can arrive, and what protective actions can be taken independently.

The regulatory framework is evolving. FAA Remote ID requirements improve accountability for compliant operations, while the 2026 federal rulemaking process for unmanned-aircraft flight restrictions near certain fixed-site facilities reflects continuing efforts to protect sensitive locations (FAA, 2026b; Federal Register, 2026). These measures can support deterrence and investigation, but they do not physically prevent a determined attacker from entering restricted airspace.

Privacy and civil-liberties issues must also be addressed. Counter-drone sensors can collect images, location information, radio-frequency data, and information about lawful operators or nearby residents. Programs should define purpose, access, retention, sharing, audit, and deletion requirements. Governance must include legal, security, privacy, cybersecurity, safety, and operational stakeholders.

9 Rigid protective cages and other passive defenses

Rigid cages, tensioned cables, overhead cover, and anti-drone netting are among the most visible lessons transferred from recent conflict. Their purpose is to deny a direct flight path, entangle propellers, change impact geometry, trigger premature detonation, or preserve stand-off distance between a payload and the critical component. Their appeal is understandable: they are passive, continuously present, locally repairable, and potentially less expensive than sophisticated interception systems.

The correct question is not whether a cage provides absolute protection. It does not. The question is whether a properly engineered barrier reduces likelihood or consequence enough to justify its cost and operational burden. Selective hardening can be rational when a facility has a limited number of exposed components whose failure would produce disproportionate consequences.

9.1 Advantages

Passive barriers do not depend on radio-frequency detection, communications, operator reaction, or ammunition. They may retain value against autonomous and fiber-optic systems that bypass conventional jamming. They can be modular, repaired after contact, and combined with visual screening. During a saturation event, a barrier continues to function without requiring a separate engagement decision for every aircraft.

They also support continuity. If stand-off or deflection turns a direct strike into limited external damage, the organization may avoid a prolonged outage. That benefit should be measured through expected downtime and service restoration, not only the physical condition of the barrier.

9.2 Limitations

Barrier performance depends on threat definition, mesh size, material, anchoring, stand-off distance, approach angle, warhead, aircraft mass and speed, and the condition of the structure. Repeated strikes can create an opening. A first drone may deliberately breach the barrier for a following aircraft. A barrier that stops a light quadcopter may have little effect against a heavier fixed-wing system or larger explosive payload.

Poor design can create secondary hazards. Around electrical equipment, conductive structures must account for clearances, grounding, lightning, arcing, and maintenance. Around fuel or hazardous material, impact may produce burning debris, fragmentation, or blast reflection. Barriers can interfere with ventilation, drainage, fire suppression, cranes, inspections, evacuation, and responder access. Wind, snow, corrosion, and seismic loading must be considered by qualified engineers.

Protective structures can also reveal target importance. A conspicuous cage may identify the component that defenders consider decisive. Hardening should therefore be combined with obscurity, concealment, decoys, protection of redundant assets, and control of publicly available imagery.

The strongest conclusion in the supplied rigid-cage analysis should be preserved: “A protective cage is not the defense. It is one layer of the defense” (Barrueco Perez, 2026, p. 8). JIATF 401 reaches the same broader principle by directing planners to combine active and passive measures, identify critical assets, harden positions, use cover and concealment, establish early warning, employ deception, and plan recovery (2026, p. 50).

10 A layered protection model

An effective program should be built in concentric and mutually supporting layers. The layers are organizational as well as physical.

10.1 Intelligence and threat assessment: the program begins with a defined threat, not a vendor catalogue. Intelligence should identify hostile actors, local drone activity, relevant incidents, accessible technologies, probable launch sites, approach corridors, online targeting information, and warning indicators. Security teams should examine how the threat could evolve after controls are installed.

10.2 Airspace and perimeter awareness: traditional perimeter security begins at the property line. Drone defense must look beyond it. Likely launch areas, parking structures, rooftops, parks, roads, water approaches, and adjacent properties may determine warning time. Relationships with neighbors and law enforcement can extend observation without expanding technical surveillance beyond lawful limits.

10.3 Multisensor detection and command and control: sensor selection should follow a site survey addressing terrain, electromagnetic environment, legal restrictions, background aviation, weather, and line of sight. Alerts must enter a common operating picture. The command center needs authority to validate authorized flights, classify behavior, record evidence, notify leadership, and trigger protective actions.

10.4 Hardening, obscuration, and dispersion: critical components should be protected according to consequence and feasibility. Measures may include netting, rigid barriers, overhead cover, blast and fragmentation shielding, relocation, visual screens, reduced lighting signatures, camouflage, decoys, and greater separation between redundant components. JIATF 401 emphasizes that survivability includes camouflage, cover, concealment, decoys, and dispersion, not only interception (2026, pp. 60–61).

10.5 Operational response: procedures should define actions for observation, verified incursion, suspected hostile surveillance, payload indicators, attack, crash, and recovery. Options can include sheltering personnel, stopping exposed operations, isolating hazardous processes, moving vehicles, activating fire response, protecting command functions, preserving communications, and requesting authorized federal support.

10.6 Recovery and continuity: complete protection is unrealistic across a dispersed infrastructure network. In 2026, the chief executive of E.ON stated that “complete protection is illusory” and emphasized rapid restoration after a successful attack (Reuters, 2026a). That position is not surrender; it is a resilience principle. Spares, alternate power, manual control, redundant communications, restoration contracts, mutual aid, crisis communications, and rehearsed decision-making reduce the attacker's strategic effect.

11 risk-based implementation framework

The following process translates the threat into an operational program.

- **Step 1 Define the essential function:** identify the service that must continue during and after an incident. The answer may differ from the list of expensive assets. Security priorities should follow mission impact.
- **Step 2 Map dependencies and single points of failure:** document electrical, communications, water, fuel, digital, transportation, vendor, and workforce dependencies. Identify components with long replacement times and limited substitutes.
- **Step 3 Define credible drone scenarios:** assess aircraft size, speed, range, payload, navigation, control method, launch distance, operator skill, number of aircraft, and likely intelligence support. Separate credible scenarios from technically possible but remote extremes.
- **Step 4 Analyze aerial access and signatures:** review roof openings, vents, line-of-sight routes, blind zones, lighting, thermal signatures, publicly available imagery, flight restrictions, likely launch positions, and emergency approaches.
- **Step 5 Evaluate existing controls:** determine what current CCTV, radar, alarms, guards, access control, intelligence, cyber monitoring, fire protection, and business-continuity systems contribute. Avoid building an isolated drone program when existing capabilities can be integrated.

- **Step 6 Select layered measures:** choose detection, physical protection, obscuration, procedures, redundancy, and lawful response options as a system. Evaluate interoperability, staffing, maintenance, training, false alarms, and lifecycle cost.
- **Step 7 Engineer against secondary hazards:** require structural, electrical, fire, blast, environmental, aviation, and emergency-response review for physical modifications. A barrier that obstructs maintenance or redirects blast toward the asset may increase total risk.
- **Step 8 Establish authority and coordination:** define who classifies an event, who can stop operations, who contacts law enforcement, who communicates with regulators and customers, and which agency can employ mitigation technology. Decision thresholds must be understood before the timeline compresses.
- **Step 9 Test and exercise:** use lawful red-team flights, tabletop exercises, sensor testing, communications drills, and recovery exercises. Test night, weather, maintenance, shift-change, and degraded-communications conditions. Record both technical performance and decision time.
- **Step 10 Learn and adapt:** every incursion, false alarm, authorized-flight conflict, exercise, and attack should produce a structured review. JIATF 401 describes lessons learned as a cycle of discovery, validation, resolution, evaluation, and dissemination (2026, p. 84). That cycle is equally applicable to corporate and civilian infrastructure security.

12 Performance measures and warning indicators

A program should be measured by outcomes and readiness rather than by the number of devices installed. Useful indicators include:

- percentage of critical assets covered by validated detection;
- detection probability by aircraft type, altitude, direction, and operating condition;
- average time from detection to classification and notification;
- percentage of authorized flights correctly reconciled;
- false-alarm rate and operator workload;
- percentage of critical components with assessed overhead vulnerability;
- time required to isolate hazardous processes or move personnel;
- time required to notify the agency with legal authority;
- availability of spares and estimated time to restore essential service;
- inspection and repair time after barrier contact;
- completion rate for exercises and corrective actions;
- number of recurring incidents linked through intelligence analysis.

Warning indicators should include repeated flights at similar times, systematic observation of access points, loitering near critical components, flights without expected Remote ID data, unusual antennas or payloads, coordinated ground vehicles, activity near likely launch sites, attempts to provoke security responses, and online publication of detailed site imagery. None of these indicators alone proves hostile intent. Their value comes from pattern analysis and context.

13 Strategic implications

Drone proliferation changes the distribution of power below the level of conventional war. A non-state actor can now obtain aerial observation, precision movement, and limited strike capability without an air force. A state can apply pressure through ambiguous incursions or proxies while complicating attribution. A criminal organization can watch law enforcement from above and move contraband without exposing a courier. An individual can create national-level disruption by operating near a sensitive airport or public event.

The resulting challenge is institutional. Aviation authorities regulate airspace, law enforcement investigates crimes, intelligence agencies assess actors, infrastructure operators manage continuity, communications regulators protect spectrum, and defense organizations possess many of the most capable countermeasures. The threat moves across these boundaries faster than bureaucratic coordination. Responsibility without authority and authority without local awareness are equally dangerous.

Governments should therefore build a shared operating model. It should define reporting standards, information-sharing channels, protected-site priorities, evidence requirements, support timelines, privacy rules, and criteria for deploying federal capabilities. Critical-infrastructure operators should be included in planning because they understand process dependencies and restoration requirements that outside responders may not see.

Investment must also balance active defense with resilience. Attempting to protect every component equally is neither feasible nor necessary. The better approach is to identify decisive functions, make them harder to find and reach, provide layered warning, preserve safe operations during an incident, and recover before disruption becomes strategic.

Conclusion

Drones are now a persistent internal-security and critical-infrastructure threat because they combine accessibility, adaptability, precision, and distance. Their danger lies not only in explosive payloads. Surveillance, smuggling, disruption, deception, communications support, and the testing of security reactions can all advance hostile objectives. The platform allows actors with limited resources to reach vulnerabilities that traditional security design often leaves exposed.

The response must avoid two errors. The first is technological overconfidence: the belief that radar, jamming, an interceptor, or a protective cage will solve the problem alone. The second is fatalism: the assumption that because complete protection is impossible, meaningful risk reduction is also impossible. Both are operationally unsound.

A defensible strategy begins with critical functions and credible threats. It integrates intelligence, multisensor awareness, trained decision-makers, legal coordination, selective hardening, obscuration, dispersion, emergency action, redundancy, and recovery. Rigid cages and netting can materially reduce risk when engineered for a defined threat and inspected as degradable controls. They cannot replace the larger system.

The final measure of protection is not whether every drone is intercepted. It is whether an organization can deny easy targeting, prevent a single inexpensive aircraft from causing disproportionate harm, preserve life and essential functions, and restore operations before the attacker achieves a wider political, economic, or psychological objective.

References

- Barrueco Perez, P. (2026). *Rigid protective cages: A low-cost defense for critical infrastructure against drone attacks* [Unpublished manuscript].
- Castrillo, V. U., Manco, A., Pascarella, D., & Gigante, G. (2022). A review of counter-UAS technologies for cooperative defensive teams of drones. *Drones*, 6(3), 65. <https://doi.org/10.3390/drones6030065>
- Clarke, C. P. (2018, August 13). Approaching a “new normal”: What the drone attack in Venezuela portends. RAND Corporation. <https://www.rand.org/pubs/commentary/2018/08/approaching-a-new-normal-what-the-drone-attack-in.html>
- Congressional Research Service. (2019, October 1). *Attacks against Saudi oil infrastructure and U.S. policy* (IN11173). <https://www.everycrsreport.com/reports/IN11173.html>
- Cybersecurity and Infrastructure Security Agency. (2026). *Critical infrastructure sectors*. <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>
- European Commission. (2023). *Communication on countering potential threats posed by drones* (COM(2023) 659 final). Publications Office of the European Union.
- European Union Agency for Law Enforcement Cooperation. (2025). *The unmanned future(s): The impact of robotics and unmanned systems on law enforcement*. Publications Office of the European Union. <https://doi.org/10.2813/0022284>
- Federal Aviation Administration. (2026a). *Unmanned aircraft systems*. <https://www.faa.gov/uas>
- Federal Aviation Administration. (2026b). *Remote identification of drones*. https://www.faa.gov/uas/getting_started/remote_id
- Federal Register. (2026, June 30). Designation: Restrict the operation of unmanned aircraft in close proximity to a fixed site facility. <https://www.federalregister.gov/documents/2026/06/30/2026-13126/designation-restrict-the-operation-of-unmanned-aircraft-in-close-proximity-to-a-fixed-site-facility>
- Government Accountability Office. (2018). *Small unmanned aircraft systems: FAA should improve its management of safety risks* (GAO-18-110). <https://www.gao.gov/products/gao-18-110>
- Government Accountability Office. (2022). *Counter-drone technologies: Technologies addressing an emerging threat* (GAO-22-105705). <https://www.gao.gov/products/gao-22-105705>
- Government Accountability Office. (2024). *Drones: Actions needed to better support remote identification in the national airspace* (GAO-24-106158). <https://www.gao.gov/products/gao-24-106158>
- Hunder, M. (2026, July 10). Russia evades Ukraine electrical substation defences with small, unjamable drones. *Reuters*.

Joint Interagency Task Force 401. (2026). *Counter-small unmanned aircraft systems quick reference guide* (Version 4). U.S. Department of War.

Nassi, B., Shabtai, A., Masuoka, R., & Elovici, Y. (2021). SoK: Security and privacy in the age of commercial drones. In *2021 IEEE Security and Privacy Workshops*. IEEE.
<https://arxiv.org/abs/1903.05155>

National Academies of Sciences, Engineering, and Medicine. (2018). *Assessing the risks of integrating unmanned aircraft systems into the national airspace system*. National Academies Press. <https://doi.org/10.17226/25143>

Reuters. (2019, September 14). Attacks on Saudi oil facilities knock out half the kingdom's supply. <https://www.reuters.com/article/world/attacks-on-saudi-oil-facilities-knock-out-half-the-kingdoms-supply-idUSKCN1VZ01Q/>

Reuters. (2025, July 22). Increasing drone incidents near U.S. airports, stadiums prompt alarm, officials say.

Reuters. (2026a, August 12). Full energy grid protection against drones “illusory,” E.ON CEO says.

Reuters. (2026b, February 25). Ukraine to cover 4,000 km of roads with anti-drone nets by year-end, minister says.

The Guardian. (2025, September 23). Danish PM: Airport drone incursion a “serious attack” on critical infrastructure. <https://www.theguardian.com/world/2025/sep/23/drone-sightings-cause-disruption-delays-norway-denmark-airports>

Wang, J., Liu, Y., & Song, H. (2021). Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends. *IEEE Aerospace and Electronic Systems Magazine*, 36(3), 4–29. <https://doi.org/10.1109/MAES.2020.3015537>