INSIGHT PAPER / CRITICAL INFRASTRUCTURE & COUNTER-UAS

The Air Above the Fence

Why counter-drone protection is becoming a corporate security responsibility

From perimeter defence to layered resilience for critical infrastructure and high-risk commercial sites

CENTRAL JUDGMENT

Companies must own awareness, hardening, personnel protection, continuity and state integration. Jamming or kinetic defeat should remain with legally authorised authorities.

Critical infrastructure | Corporate security | Counter-UAS | Resilience

ADG CONSULT NZ

AUGUST 2026

EXECUTIVE ASSESSMENT

Executive Summary

The attempted use of an explosives-laden drone against an aircraft supporting Ukraine at Leipzig/Halle Airport on 4 August 2026 is a warning that the drone threat is moving beyond recognised war zones. France's domestic intelligence chief subsequently told business leaders that defence, technology, energy and communications infrastructure must consider the possibility of more direct and violent hybrid action. The warning was important not simply because of the device involved, but because the intended target sat at the junction of military logistics and civilian commercial infrastructure.[1]

CENTRAL ASSESSMENT This paper supports the hypothesis that counter-drone protection is becoming a corporate security responsibility. That assessment requires an important qualification. Private companies should not attempt to become private air forces, and in many jurisdictions they cannot lawfully jam, seize or destroy an aircraft. Corporate responsibility instead begins with recognising the air above a facility as part of the security environment: assessing the threat, establishing airspace awareness, distinguishing authorised from unauthorised activity, reducing physical vulnerability, protecting personnel, maintaining operations, preserving evidence and connecting the site to authorities capable of lawful intervention.

The policy direction is already visible. In July 2026 the European Commission issued critical-infrastructure resilience guidance that expressly includes drone attacks and hybrid threats within the risks that critical entities should prevent, withstand and recover from.[2] The European Union's February 2026 Action Plan on Drone and Counter Drone Security is organised around preparedness, detection, coordinated response and defence readiness, including a proposed deployment initiative for critical infrastructure and a more integrated air picture.[3] NATO has committed more than USD 40 billion to counter-drone capabilities over five years, reflecting the scale of the military problem and the likelihood that governments will prioritise national and military assets when demand exceeds available protection.[4]

The underlying security imbalance is severe. Commercial drones are inexpensive, widely available, rapidly modifiable and difficult to classify in crowded low-altitude airspace. More capable systems can operate autonomously, use non-standard communications or employ fibre-optic control that defeats radio-frequency jamming. The defended asset may be a refinery, warehouse, substation, airport or data centre worth hundreds of millions of dollars; the attacking system may cost a tiny fraction of that amount. Even where a drone causes no physical damage, its presence can force an airport closure, evacuation, safety shutdown or interruption of work.

The correct corporate response is therefore not to purchase a single counter-drone product and declare the problem solved. Detection does not establish hostile intent. Jamming does not defeat every drone. A weapon that brings down a drone may create greater danger from falling debris, fire or interference with civil aviation. The appropriate solution is a layered **Corporate Counter-Drone Resilience Framework** that combines governance, threat assessment, multi-sensor detection where justified, passive protection, operational continuity, rehearsed response and formal integration with state authorities. This aligns with the UK's National Protective Security Authority, which treats counter-UAS as a site-specific strategy and plan rather than a stand-alone device.[5]

The recommended endstate is a facility that can detect and assess abnormal drone activity early; continue safe operations where possible; move personnel and processes into a protected posture when necessary; hand off reliable information to police, aviation or military authorities; and recover quickly if an incident occurs. Active defeat should be added only at the highest-risk sites, under explicit legal authority and within a government-integrated command arrangement. For most companies, resilience will deliver more protection than an expensive but isolated interception system.

The Security Perimeter Has Become Three-Dimensional

For most of modern corporate security, the protected site has been treated as a two-dimensional problem. Fences, gates, guards, vehicle barriers, lighting and CCTV were designed to control movement across the ground boundary. Rooftops and elevated structures mattered, but the volume of low-altitude airspace above the site was rarely monitored continuously. Small drones have invalidated that assumption.

A drone does not need to breach a gate, defeat a guard or approach along a road. It can observe shift changes and patrol patterns, inspect roofs and process areas, record sensitive activity, deliver contraband, generate a false alarm, support an intrusion or carry an explosive payload. It can also remain outside the property boundary while collecting information that would once have required physical trespass. In security terms, the fence has not disappeared; it has acquired an unprotected vertical flank.

This does not mean every drone near a facility is hostile. The airspace also contains legitimate commercial operators, public-safety aircraft, survey teams, media, hobbyists and a company's own maintenance drones. Some events are accidental or negligent. Others are deliberate but non-violent, including protest, nuisance, voyeurism and competitive intelligence collection. A smaller number involve organised crime, terrorism, proxy activity or state-directed sabotage. The central operational challenge is therefore not merely detecting an object. It is detecting, tracking, identifying and assessing it quickly enough to make a proportionate decision.

The consequences can be disproportionate even when hostile intent is never established. During the Gatwick Airport incident of 19-21 December 2018, repeated reported sightings caused approximately 1,000 flights to be cancelled or diverted and affected about 140,000 passengers. The perpetrator was never established and later analysis questioned how many sightings represented actual drones, but that uncertainty reinforces the lesson: weak verification and the absence of a trusted operating picture can itself produce strategic disruption.[6]

The Threat Is Broader Than an Explosive Drone

Observation and preparation

The most accessible hostile use is surveillance. Stabilised cameras and thermal sensors allow a small platform to observe entrances, guard routines, high-value equipment and staff movements without exposing an operator at the fence. Repeated flights may support theft, kidnapping, sabotage, protest planning or a later attack. A single apparently harmless overflight may be difficult to interpret; a pattern of flights at similar times or over the same asset is an intelligence indicator.

Sites should therefore treat drone reporting as security data rather than isolated nuisance complaints. Time, direction, altitude estimate, behaviour, sensor detections, imagery and any Remote ID information should be retained and compared. The objective is not to criminalise lawful aviation. It is to distinguish the normal local air picture from activity that is persistent, evasive, concealed or closely associated with sensitive operations.

Delivery and support to ground activity

Drones can bypass walls and controlled entrances to deliver prohibited or dangerous items. The prison threat is the clearest established example, but the same method can support intrusion at industrial sites, storage areas and compounds. A drone may also act as overwatch for people on the ground, distract guards from another boundary or test response times through repeated low-level incursions.

The UK's national counter-UAS strategy identifies terrorism, serious and organised crime, disruption of critical national infrastructure and hostile-state activity as the principal high-harm categories.[7] In February 2026, a joint UK government competition sought low-collateral solutions against drones used for contraband delivery, surveillance and disruption around prisons, sensitive sites and critical infrastructure. The requirement demonstrates that even governments with mature security institutions do not regard the problem as technically solved.[8]

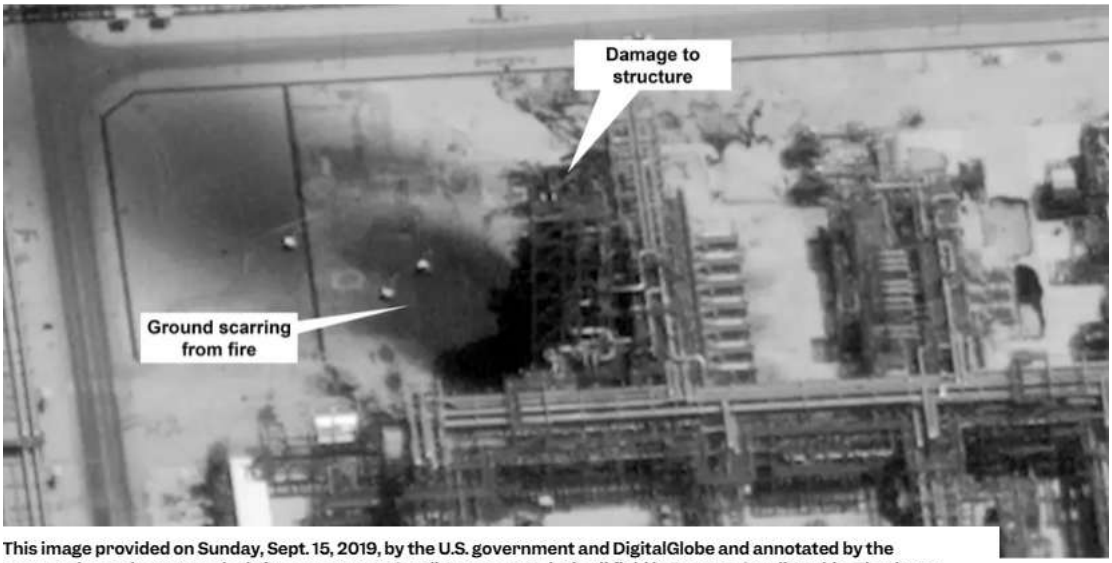
Disruption as the objective

A drone does not need to hit anything to succeed. An airport, refinery, chemical plant or public event may halt activity because the operator cannot determine whether a detected object is harmless, conducting surveillance or carrying a payload. For a hostile actor, the cost of generating uncertainty may be far lower than the cost imposed on the defender through shutdown, delay, inspection, evacuation and reputational damage.

This makes continuity planning part of counter-drone security. A facility that has only two choices - continue normally or stop completely - gives an intruder substantial coercive power. A more resilient site can restrict exposed activity, isolate a process area, move personnel under cover, protect a control room and maintain essential functions while verification and state response proceed.

Direct attack

The 14 September 2019 attacks on Saudi Aramco's Abqaiq and Khurais facilities demonstrated the strategic effect available from relatively small aerial systems used with precision. A United Nations panel assessed that weaponised UAVs and land-attack cruise missiles were used against the two facilities.[9] Approximately 5.7 million barrels per day of Saudi crude production were initially taken offline, although production recovered rapidly.[10] The enduring lesson is not that every corporate facility faces a state-level strike. It is that complex industrial systems contain a limited number of components whose temporary loss can interrupt output far beyond the size of the damaged area.



This image provided on Sunday, Sept. 15, 2019, by the U.S. government and DigitalGlobe and annotated by the source, shows damage to the infrastructure at Saudi Aramco's Kuirais oil field in Buqyaq, Saudi Arabia. The drone attack Saturday on Saudi Arabia's Abqaiq plant and its Khurais oil field led to the interruption of an estimated 5.7 million barrels of the kingdom's crude oil production per day, equivalent to more than 5% of the world's daily supply. (U.S. government/Digital Globe via AP) Associated Press

The Russia-Ukraine war has since normalised long-range drone attacks on economic infrastructure. Reuters calculated that Ukrainian attacks affected about 700,000 barrels per day of Russian refining capacity across 16 refineries between January and May 2026, alongside strikes on pipelines and storage facilities.[11] The campaign illustrates a central strategic development: commercial and industrial assets can be targeted as part of a sustained effort to weaken economic capacity, state revenue and public confidence, even when located far from a conventional front line.

Why Existing Defences Are Being Overtaken

The attacker can change faster than the site

Corporate security systems are normally procured through multi-year capital cycles. Drone design changes in months or weeks. Consumer components, open-source software and combat innovation can be recombined quickly, while approval, budgeting, installation and training for the defender proceed slowly. A system purchased against a known commercial quadcopter may perform poorly against an autonomous aircraft, a modified frequency, a low-signature fixed-wing platform or several drones arriving together.

Fibre-optic controlled drones provide a current example. In July 2026 Reuters verified attacks on Ukrainian high-voltage substations in which small drones controlled through fibre-optic cable bypassed electronic-warfare defences. In some cases one drone breached protective netting and a subsequent drone penetrated toward critical transformer equipment. The attacking drone could cost about USD 2,000 while the targeted autotransformer was valued at approximately USD 3.5 million.[12] The incident shows both the cost imbalance and the danger of relying on a single protective measure.

Autonomous navigation creates a similar problem. A drone that does not depend on a continuous radio link may continue along a pre-programmed route after conventional jamming. Satellite navigation interference may reduce accuracy but can also affect legitimate systems and does not necessarily defeat inertial, terrain-referenced or vision-based guidance. Defensive planning must assume that any one detection or mitigation technology will have blind spots.

Commercial facilities are designed for efficiency, not aerial attack

Energy, logistics and communications sites often contain exposed roofs, ventilation openings, antennas, cooling systems, storage tanks, electrical yards and long internal pipelines. Warehouses combine large roof areas with combustible contents and concentrated inventory. On 26 August 2026 a drone attack caused a fire that destroyed a Wildberries logistics centre in Russia's Tambov region; Reuters reported that roughly 100,000 square metres burned and that more than 20 Wildberries and Ozon warehouses had been attacked since mid-July.[13]

The vulnerability is not confined to physical destruction. Production may stop automatically when sensors, power, communications or safety systems are disrupted. Emergency services can be delayed by continuing drone activity. Employees may film and distribute confused scenes before verified information is available. Insurers and regulators may examine whether reasonable protective measures were in place. A modest strike can therefore create operational, financial, legal and reputational effects simultaneously.

Remote field operations face a different version of the same problem. A seismic camp, mine, construction site or pipeline project may have lower strategic value than a national refinery, but it also has fewer public-security resources, longer response times and a large open perimeter. The credible threat may be reconnaissance, intimidation, theft support or observation of foreign personnel rather than aerial attack. The appropriate response is correspondingly lighter, but the vertical approach still needs to appear in the security risk assessment and emergency plan.

The Transfer of Responsibility Is Already Underway

The emerging division of responsibility can be seen in policy, regulation and market behaviour. States retain sovereignty over airspace and the coercive powers needed to interfere with aircraft. At the same time, governments are increasingly expecting operators of critical or economically important facilities to understand their own vulnerabilities, maintain continuity and invest in site-level protection.

Russia made this expectation explicit on 24 August 2026 by authorising temporary state control of fuel, energy, industrial, communications, transport and logistics facilities deemed poorly protected or too slow to repair after drone attack. The measure reflects Russia's wartime political system and should not be treated as a universal governance model. It nevertheless provides unusually direct evidence that failure to manage aerial vulnerability is being reframed as a failure of corporate stewardship.[14]

In Western jurisdictions the shift is more likely to occur through critical-infrastructure resilience duties, licensing expectations, insurance requirements and corporate-governance standards. The European Commission's 2026 guidance emphasises risk assessment, physical protection, mitigation, recovery and employee security. It does not transfer military air defence to private companies. It transfers responsibility for preparedness and resilience.

The market is responding. In August 2026 a private air-defence venture announced that it would design and operate customised systems for data centres, energy installations and military bases. The significance is not the merits of one company; it is that commercial demand is now considered sufficient to support an industry positioned between traditional guarding and national air defence.[15] This market will expand, but it also creates a procurement risk: organisations may purchase impressive technology without a lawful concept of operations, trained operators or a realistic understanding of what the system cannot detect.

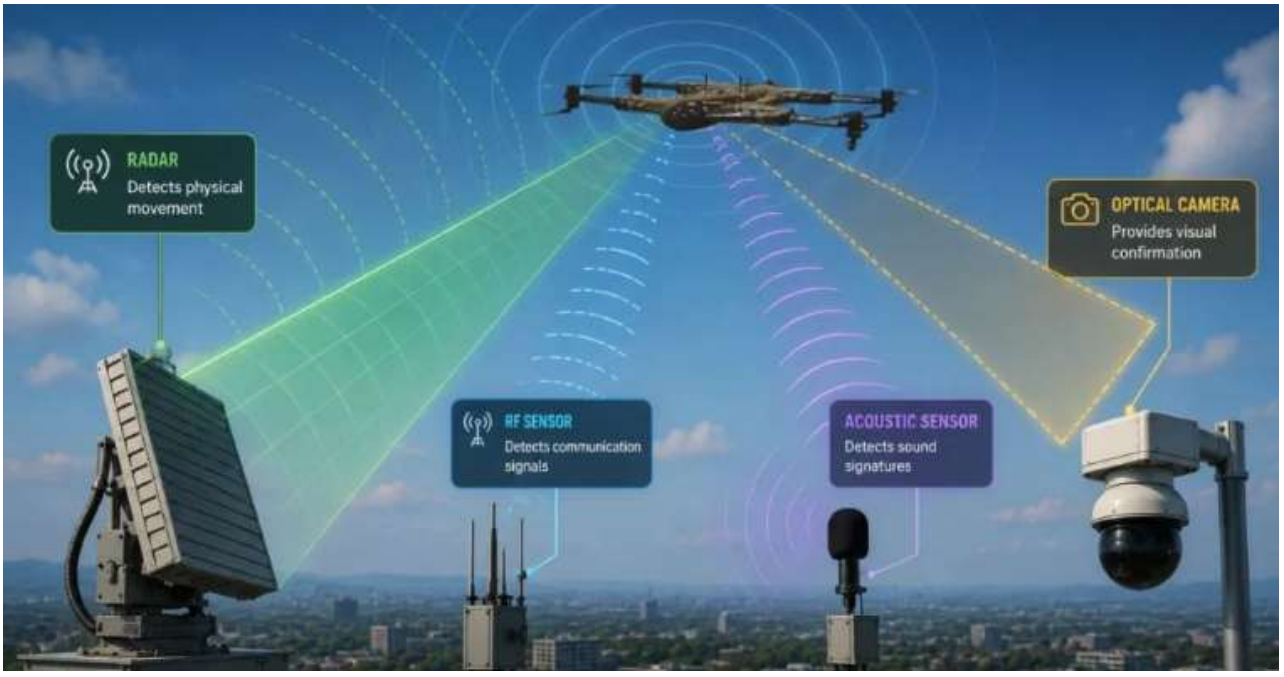
Detection Is Not the Same as Protection

No single sensor provides the answer

Radar can detect an aircraft that emits no radio signal, but small low-flying objects are difficult to separate from birds, vehicles, machinery and terrain clutter. Radio-frequency sensors can identify known control links and may help locate an operator, but they are ineffective against silent autonomous systems or fibre-optic control and can create legal issues if communications are intercepted. Electro-optical and infrared cameras provide visual verification and evidence but need line of sight and are affected by distance, weather, background and lighting. Acoustic detection can add a low-cost cue in quiet environments but performs poorly around industrial machinery, traffic and wind.

Remote ID can help distinguish compliant traffic. The FAA describes it as a digital licence plate broadcasting identification and location information for the aircraft and, depending on the system, the control station or take-off point.[16] It is useful for an allowlist and for ruling out known activity, but it is not a security barrier. A hostile operator may disable, omit or falsify identification. Equally, the absence of Remote ID does not prove hostile intent because exemptions, technical failure and regulatory differences may apply.

The practical answer is sensor fusion: two or more complementary sources presented through a single operating picture, supported by trained human judgment. Even then, the system can establish presence, movement and characteristics more reliably than intent. The FAA explicitly notes that detection systems do not determine the intent or threat level of a drone.[17] A security operation therefore needs decision rules based on behaviour, proximity to protected assets, persistence, payload indicators, compliance, external intelligence and the wider incident context.



False alarms are a security risk

A system that generates frequent unexplained alarms will eventually be ignored or switched off. It may also cause unnecessary shutdowns, exposing the organisation to the same disruptive effect that an adversary seeks. Procurement trials should therefore measure false alarms in the actual environment, including birds, cranes, roof fans, vehicles, rain, dust, heat and legitimate drones. Demonstration performance on a clear test range is not sufficient.

Every alert should have an operator action attached to it. If a system detects an object but the control room cannot verify it, cannot communicate with authorities and has no graduated protective action, the technology has produced awareness without protection. The operating concept, people and communications are at least as important as the sensor.

Active Defeat Has Legal and Operational Limits

Counter-drone technology is commonly divided into detection and mitigation. Mitigation may include taking control of the drone, interrupting communications, spoofing navigation, capturing it with another system or physically destroying it. These options are attractive because they appear decisive. They are also where corporate security encounters the strongest legal and safety constraints.

In the United States, federal guidance warns that private entities and most state or local bodies have not been granted the statutory authority held by selected federal departments. Detection may implicate surveillance law, while mitigation may engage laws protecting aircraft, radio communications and computer systems.[18] The Government Accountability Office similarly identifies risks from errant projectiles, falling drones, privacy intrusion and the limited number of authorised agencies.[19]

The United Kingdom also distinguishes lawful authority from technical capability. Interference with the link between an aircraft and its controller may constitute an offence under the Wireless Telegraphy Act 2006, while kinetic measures may amount to unlawful interference with property unless properly authorised.[20] Australia states even more directly that possession, supply or operation of drone jammers is generally illegal, with exemptions reserved for specified authorities.[21] Other jurisdictions vary, but the corporate rule should be constant: no active measure should be procured, tested or used without written legal review covering aviation, spectrum, privacy, property, safety and liability.

Operational limitations remain even where authority exists. Jamming works only if it affects the relevant control or navigation signal; it may fail against autonomy, non-standard frequencies or fibre-optic control. It can interfere with communications and navigation used by the site, emergency services or nearby aviation. It may cause the drone to hover, land, return to its launch point or continue unpredictably. UK maritime guidance consequently warns that jamming effectiveness depends on the frequencies, power, geometry and navigation method involved.[22]

Kinetic defeat introduces a different hazard. A bullet, interceptor or damaged drone must fall somewhere. At a refinery, airport, crowded event or dense urban site, the debris and secondary fire may be more dangerous than the original flight. Directed-energy and high-power systems can reduce ammunition costs but require line of sight, power, trained operators, safety controls and substantial capital support. These tools may be appropriate for a military base or nationally critical facility; they are not a default corporate purchase.

The Corporate-State Boundary

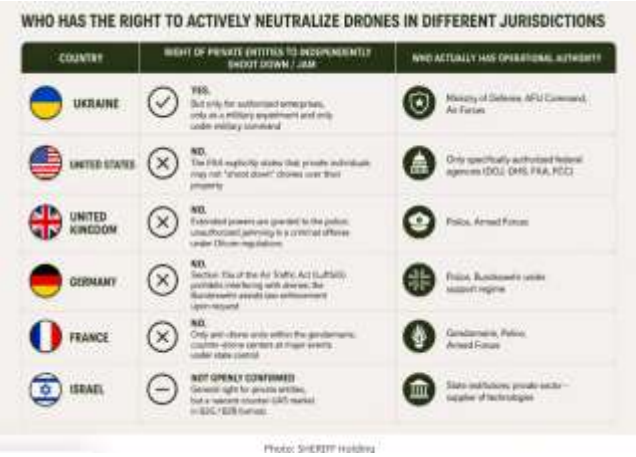
The workable model is shared security with a clear boundary of authority.

Corporate operators should own: site-specific threat and vulnerability assessment; control of authorised company drones; detection and evidence systems where proportionate; protective intelligence; physical hardening; personnel safety; graded operational response; business continuity; training; incident logs; vendor cybersecurity; and pre-agreed liaison with police, aviation regulators, emergency services and national-security bodies.

The state should retain: airspace regulation; access to national surveillance and intelligence; attribution; law-enforcement investigation; authorisation and control of jamming or kinetic effectors; military air defence; cross-border response; prosecution; and the legal framework governing private detection and data collection.

Joint responsibility should cover: protected-airspace arrangements; information sharing; incident thresholds; notification formats; exercises; temporary deployment of authorised countermeasures; evidence preservation; public communication; and recovery of hazardous devices or debris.

This division prevents two opposite errors. The first is corporate passivity - assuming government will detect and stop every threat. The second is corporate overreach - purchasing an active system that is unlawful, unsafe or poorly integrated with national airspace management. The objective is not to erase the boundary between public and private security. It is to make the handover across that boundary fast, informed and rehearsed.



Recommended Solution: Corporate Counter-Drone Resilience Framework

The proposed solution is a six-layer framework designed for critical infrastructure, major logistics nodes and high-risk overseas sites. Each layer is useful independently, but the protective effect comes from their integration. Technology is introduced only after governance, threat and operational requirements have been established.

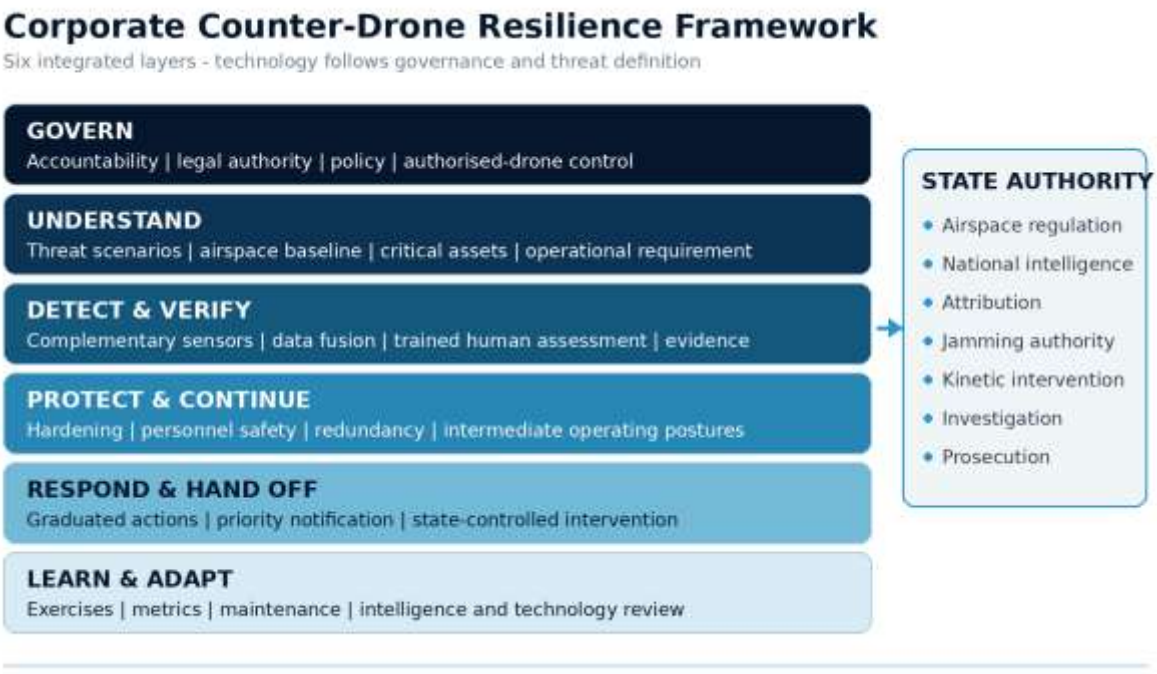


Figure 1. Corporate responsibility should integrate six resilience layers and hand active intervention to the legally authorised state authority.

Govern the airspace security problem

Appoint a senior accountable executive and a designated programme owner, normally within security or resilience but supported by operations, safety, legal, information technology, facilities and communications. Define which business units own the drone fleet, approve contractors and maintain the register of authorised flights. Establish a legal matrix for every country of operation covering detection, radio-frequency monitoring, imaging, data retention, jamming, seizure, use of force and reporting.

The organisation should adopt one corporate standard with country annexes rather than allowing each facility to purchase independently. The standard should define risk tiers, minimum reporting, procurement assurance, cyber requirements, data governance and the threshold for government engagement. Local plans can then reflect site geography and law without losing corporate consistency.

Understand the threat and the site's real vulnerability

Conduct a scenario-based threat and vulnerability assessment. It should identify likely actors, intent, capability, approach routes, surrounding launch areas, legitimate air traffic, critical assets, exposed personnel and single points of failure. The assessment should cover surveillance, contraband or payload delivery, disruption, direct attack and drone-supported ground intrusion. It should also examine the consequence of a false report or precautionary shutdown.

The assessment must be operational, not generic. A refinery should identify process components whose loss creates escalation or prolonged shutdown. A warehouse should examine roof access, fire spread and inventory concentration. A data centre should consider cooling, power and communications redundancy. A remote camp should focus on observation, personnel exposure, response time and safe shelter. Sensitive detail should remain controlled, but the security plan must understand what actually matters.

NPSA guidance recommends developing a formal operational requirement that defines the threat scenarios, what the system must detect, track and identify, when it must operate and what performance is required.[23] This approach should precede vendor engagement. Buying a product before defining the operational requirement reverses the security process and encourages dependence on marketing claims.

Build proportionate airspace awareness

Create a baseline of legitimate activity. Register company and contractor drones, planned flight windows, operators, Remote ID details where applicable and emergency-service procedures. Establish one reporting channel for guards, staff and nearby partners. Provide simple recognition training so reports include behaviour and direction rather than only the word "drone".

At higher-risk sites, deploy multi-sensor detection selected against the operational requirement. Radar, radio-frequency, optical, infrared, acoustic and Remote ID sources should feed a single command-and-control view where possible. The system should record tracks and video in a format suitable for evidence and after-action review. A trained operator must verify alerts and apply agreed decision rules. Cybersecurity testing is essential because a connected detection system can itself become an access point into the corporate network.

NATO's 2026 procurement model reinforces the modular approach: a common command-and-control backbone integrates radar, direction finding, electro-optical/infrared and acoustic sensors with electronic or hard-kill effectors where authorised.[24] Corporate systems should adopt the same principle at a smaller scale - open architecture, multiple sensors and the ability to replace a component without rebuilding the entire system.

Reduce consequence through passive protection

Passive protection is the most legally accessible and frequently the most cost-effective layer. It should include protection of critical openings and exposed equipment; control of roof and upper-level access; relocation or shielding of vulnerable control and communications nodes; fire detection and suppression; separation of high-value inventory; redundancy in power and communications; rapid isolation of affected process areas; and protected routes or shelter for personnel.

Measures must be engineered for the site. Netting or grilles can reduce access to an aperture but may create maintenance, fire, wind-load or entanglement hazards. Concrete protection can defeat fragments but still leave ventilation and access routes exposed. Camouflage and concealment may reduce observation at a military location but conflict with industrial safety and emergency identification. Security, process safety and engineering teams must approve the design together.

Operational resilience should provide intermediate postures between normal work and complete shutdown. Examples include pausing outdoor work, moving staff under cover, isolating a loading area, closing roof access, protecting ignition-sensitive operations, transferring control to a secondary room, increasing fire watch and moving critical data or command functions to a remote location. These actions reduce the adversary's ability to impose major disruption through a low-confidence alert.

Establish a graduated response and government handover

Develop four response levels linked to observable behaviour rather than assumptions about intent.

Routine: a known, compliant or non-threatening flight. Confirm authorisation, record as required and continue operations.

Concern: an unidentified aircraft near the site or a repeated flight over non-critical areas. Verify using available sensors, notify security supervision, check authorised activity, begin recording and prepare protective actions.

Threat: persistent, evasive or payload-indicating activity approaching critical assets, or activity coordinated with a wider incident. Protect personnel, restrict exposed operations, initiate pre-agreed safety measures, notify authorities through the priority channel and preserve a continuous incident log.

Attack or impact: an apparent hostile act, detonation, crash or hazardous payload. Activate the emergency-management structure, treat the device and debris as potentially hazardous, control secondary risks, request authorised specialist response, preserve evidence and execute continuity and crisis-communication plans.

The thresholds, wording and actions should be agreed with local authorities before an incident. Police and aviation responders need a concise report: site, time, current track, direction, behaviour, imagery, Remote ID if present, actions taken and immediate safety concerns. A company should not wait until a threat is overhead to discover that the emergency number reaches a general call centre unable to interpret the report.

Test, measure and adapt

Counter-drone plans degrade unless exercised. Begin with tabletop exercises that include security, operations, safety, legal, communications and external responders. Progress to controlled field tests where lawful, using approved drones and clearly separated safety management. Test the complete chain from initial detection through verification, executive decision, protective action, authority notification, incident command and recovery.

NATO's Layered Counter-UAS Initiative emphasises connecting sensors, command-and-control systems and effectors rather than testing devices in isolation.[25] Its 2026 technical exercise brought together approximately 300 participants, 40 companies, more than 60 systems and 40 software applications to test interoperability.[26] Corporate programmes should apply the same lesson: integration and operator performance matter more than a vendor's best-case sensor range.

Metrics should include detection and verification performance against approved test scenarios; false alarms per operating period; time from detection to operator assessment; time to authority notification; percentage of authorised flights correctly identified; availability of sensors and communications; completion of training; time to place personnel and processes into a protected posture; continuity of critical functions; and time to restore normal operations. The threat assessment and operational requirement should be reviewed after every incident, major exercise and material change in drone technology.

A Risk-Tiered Implementation Model

Not every facility requires the same investment. A proportionate corporate programme should establish three implementation tiers.

Baseline sites

All sites should include drones in the security risk assessment and emergency plan. Minimum measures are an authorised-drone register, staff reporting procedure, basic observation and recording capability, roof and critical-aperture review, law-enforcement contact plan, incident log, communications template and annual tabletop exercise. Remote camps and ordinary offices may remain at this tier unless threat intelligence or asset criticality justifies more.

Enhanced sites

High-value industrial, logistics, data, maritime and overseas sites should add a formal operational requirement, integrated detection appropriate to the environment, trained control-room operators, protective engineering, alternative operating modes, redundant communications and periodic exercises with authorities. Detection should normally be multi-sensor and able to preserve evidence. A service-level agreement should define maintenance, software updates, data ownership and response support.

Nationally critical or acutely threatened sites

Facilities whose loss would create national, regional or mass-casualty consequences require a government-integrated system. This may include protected airspace, access to national intelligence, continuous multi-sensor surveillance, on-site or rapidly deployable authorised effectors, specialist explosive-ordnance response and joint command arrangements. Corporate management still owns continuity, physical protection and workforce safety, but active defeat remains under the legally designated authority.

Tiering should be dynamic. A site may move temporarily to a higher posture during conflict escalation, a major event, a credible threat, politically sensitive activity or the arrival of high-profile personnel. The organisation should define who can order that change and what additional resources follow it.

Implementation Roadmap

First 30 days: establish control

Name the accountable executive and programme manager. Issue an interim reporting instruction. Inventory company and contractor drones. Confirm local police, aviation, emergency and national-security contacts. Begin a legal review. Identify obvious exposed critical functions and implement no-regret measures such as access control, reporting, camera coverage review and protected muster options. Preserve all previous drone incident records for pattern analysis.

Days 30-90: define the requirement

Complete the threat and vulnerability assessment for priority sites. Assign each facility a provisional tier. Develop the operational requirement and response levels. Map authorised flight procedures and data-retention rules. Conduct the first cross-functional tabletop exercise with at least one external authority. Test the notification path. Produce a costed programme separating governance, passive protection, detection, integration, training and maintenance.

Months 3-12: build and integrate

Pilot detection at one representative high-risk site before fleet-wide procurement. Test performance in the real operating environment and against approved scenarios, including legitimate traffic and common false-alarm sources. Complete priority hardening and continuity measures. Integrate alerts into the security control room and incident-management system. Train operators, supervisors and executives. Exercise day, night, poor-weather and communications-degraded conditions where safe and lawful.

Continuing programme: sustain and adapt

Review intelligence and technology quarterly at corporate level and after any material incident. Revalidate vendor performance, software security and sensor calibration. Repeat tabletop exercises at least annually and field validation according to risk. Track performance metrics, near misses and false alarms. Maintain spare parts, alternative communications and a plan for rapid temporary deployment to a site whose risk has increased.

Procurement Principles

A counter-drone procurement should be treated as a security system integration project, not the purchase of a radar or jammer. The tender must begin with the operational requirement and the legal concept of operations. Vendors should be required to state limitations, not only maximum performance.

Selection should favour modular architecture, open interfaces, auditable decision logic and the ability to combine multiple sensors. Trials must occur at the intended site and measure false alarms, clutter rejection, tracking continuity, weather performance, operator workload, cybersecurity, evidence quality and integration with existing control-room systems. The organisation should retain its own data and ensure that cloud processing, remote maintenance and software updates do not create unmanaged foreign access or operational dependence.

Contracts should cover training, certification, maintenance, calibration, software support, threat-library updates, replacement parts and secure decommissioning. Performance guarantees should relate to agreed scenarios, not a universal detection range. Where active mitigation is contemplated, the contract must identify the lawful authority, rules for activation, aviation coordination, spectrum approval, safety case, liability and who commands the system during an incident.

The cost decision should compare the programme with the consequence of disruption, not with the purchase price of a drone. The relevant calculation includes production loss, safety escalation, evacuation, recovery, regulatory exposure, loss of inventory, reputational damage and the cost of operating without a trusted air picture. A low-risk office may justify only policy and reporting. A refinery, airport or major data facility may justify persistent detection and substantial hardening. Proportionality is achieved through risk analysis, not through buying the same equipment everywhere.

Strategic Outlook

The drone threat will continue to diffuse from battlefields into hybrid conflict, organised crime, activism and commercial coercion. Systems will become more autonomous, less dependent on standard radio links and more capable of coordinated action. At the same time, legitimate commercial drone traffic will grow, making simple exclusion increasingly difficult. The security problem will shift from detecting "a drone" to maintaining a trusted low-altitude operating picture in which lawful, unknown and hostile activity can be separated quickly.

Governments will expand counter-drone powers and capability, but national coverage will remain selective. Military forces will protect military assets; police will respond according to threat and available authority; aviation regulators will prioritise safety and lawful airspace use. Commercial operators will remain closest to their own assets, understand their process consequences best and control the measures that determine whether an incident becomes a catastrophe or a manageable interruption.

The hypothesis is therefore supported. Counter-drone protection is becoming a corporate security responsibility, but the responsibility is principally one of **resilience, awareness and integration**, not independent use of force. The organisation that waits for government to solve the entire problem will retain an unmonitored vertical approach and an unrehearsed response. The organisation that buys an illegal jammer or isolated sensor will create a different vulnerability.

The effective model lies between those extremes: a risk-tiered corporate programme that governs authorised drone use, understands the local threat, fuses appropriate sensors, hardens critical functions, protects personnel, maintains operations, shares reliable information and hands coercive action to the state. The fence remains necessary. It is no longer sufficient.

SOURCE NOTES

References

References are numbered in order of first appearance. Web sources were checked during preparation on 27 August 2026.

[1] Tim Hepher, 'French security chief sees new threats after Leipzig drone attack', Reuters, 26 August 2026. Source

[2] European Commission, 'Commission issues guidance to strengthen resilience of critical infrastructure', 10 July 2026. Source

[3] European Commission, Action Plan on Drone and Counter Drone Security, COM(2026) 81 final, 11 February 2026. Source

[4] NATO, 'NATO Allies invest 40 billion dollars in counter-drone capabilities and drone training', 7 July 2026. Source

[5] UK National Protective Security Authority, 'Counter Uncrewed Aerial Systems (C-UAS)', guidance for national infrastructure security managers, updated 2025. Source

[6] UK Parliamentary Office of Science and Technology, Misuse of Civilian Drones, POSTnote 610, 17 January 2020. Source

[7] UK Home Office, Counter-Unmanned Aircraft Strategy, 2019. Source

[8] UK Defence Innovation and partner departments, 'Countering Illegal Use of UAS Around Prisons and Sensitive Sites', 3 February 2026, updated 24 April 2026. Source

[9] United Nations Security Council, Final report of the Panel of Experts on Yemen, S/2020/326, Annex 14: attacks on the Saudi Aramco facilities in Abqaiq and Khurais, 27 April 2020. Source

[10] US Department of State, Country Reports on Terrorism 2019: Saudi Arabia, 2020. Source

[11] Reuters, 'Ukraine doubles strikes on Russian oil refineries this year', 15 May 2026. Source

[12] Max Hunder, 'Russia evades Ukraine electrical substation defences with small, unjammable drones', Reuters, 10 July 2026. Source

[13] Reuters, 'Fire destroys drone-hit Wildberries warehouse in Russia's Tambov region, governor says', 26 August 2026. Source

[14] Reuters, 'Putin allows Russia to take control of infrastructure deemed vulnerable to drone attacks', 24 August 2026. Source

[15] Heather Somerville, 'Blackwater's Erik Prince Launches Air-Defense Startup', The Wall Street Journal, August 2026. Source

[16] US Federal Aviation Administration, 'Remote Identification of Drones', updated 19 March 2025. Source

[17] US Federal Aviation Administration, 'UAS Detection, Mitigation, and Response on Airports', updated 23 June 2025. Source

[18] US Departments of Justice, Transportation, Homeland Security and the Federal Communications Commission, Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems, 17 August 2020. Source

[19] US Government Accountability Office, Science & Tech Spotlight: Counter-Drone Technologies, GAO-22-105705, 26 May 2022. Source

[20] UK Parliament, Explanatory Notes to the Air Traffic Management and Unmanned Aircraft Act 2021, paragraphs 43-44. Source

[21] Australian Communications and Media Authority, 'Jammers are illegal in Australia', updated 22 July 2026. Source

[22] UK Department for Transport, 'Countering drone threats to shipping', 2023. Source

[23] UK National Protective Security Authority, C-UAS - Making Your Site Ready: Developing an Operational Requirement for C-UAS Technology, 2025. Source

[24] NATO Support and Procurement Agency, 'NSPA establishes several framework contracts for C-UAS', 27 July 2026. Source

[25] NATO Allied Command Transformation, 'Layered Counter-UAS Initiative (LCI-X) is Building NATO's Approach to a Fast-Moving Threat', 18 May 2026. Source

[26] NATO Communications and Information Agency, 'Allies and industry test the latest counter-drone technology during NATO exercise', 21 May 2026. Source