ANALYTICAL REPORT 07

UAV DETECTION TECHNOLOGIES FOR LAW ENFORCEMENT: OPERATIONAL READINESS AND REGULATORY FEASIBILITY AGAINST RF-SILENT TARGETS AT BOUNDED, RESOURCE-CONSTRAINED SITES

An External Expert Report prepared for ENACT

Main Authors
Eduardo Cermeño
Almudena Aguilera
Ana Pérez
Jorge Abrines

ENACT. European Network Against Crime and Terrorism

August 2026

ABOUT ENACT

ENACT is a knowledge network focused on the fight against crime and terrorism (FCT). The network is funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society. The project addresses the call topic HORIZON-CL3-2022-SSRI-01-02 ‘Knowledge Networks for Security Research & Innovation’, aiming to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area.

The project aims to satisfy two major ambitions,

- Provide evidence-based support to the decision-makers in the EU research and innovation (R&I) ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the fight against crime and terrorism.

- Act as a catalyst for the uptake of innovation by enhancing the visibility and reliability of innovative FCT security solutions.

Funded by the European Union

REPORT FEEDBACK

We’re collecting feedback on this report through the EU Survey Platform, if you’d like to share your thoughts anonymously please click on the link below.

https://ec.europa.eu/eusurvey/runner/enact-report-feedback

COPYRIGHT

DISCLAIMER

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

This report was prepared by external experts outside of the ENACT consortium. The report does not represent the views or opinions of the ENACT project, and all content remains the sole responsibility of the authors.

USE OF AI

Generative AI tools were used to support translation from Spanish into English, improvement of the English-language writing, editorial revision and checks for consistency between figures, references and the main text. All substantive claims, references, interpretations and recommendations were reviewed and verified by the authors, who retain full responsibility for the report's accuracy, originality and integrity. No confidential, sensitive or non-public information was entered into the tools during the preparation of this public version.

CONFLICT OF INTEREST DECLARATION

The authors of this report are affiliated with Vaelsys, whose business includes camera-based computer vision for perimeter protection and smart cities. Vaelsys has a commercial technology-licensing relationship with Liquen Consultoría Ambiental S.L., developer of the DTBird® camera-based system cited in Annex A. Evidence from that source is treated as related-party vendor evidence and is used only as an illustrative case, not as independent proof of comparative superiority or operational readiness. The report's principal findings and recommendations rely on independent scientific, standards and institutional sources. Unpublished internal prototype results are excluded from the evidentiary basis of this public report.

ACRONYMS

AI	Artificial Intelligence	**HD**	High Definition
C-UAS	Counter-Unmanned Aircraft Systems	**HUMINT**	Human Intelligence
C2	Command and Control	**HW**	Hardware
CBO	Congressional Budget Office (USA)	**INS**	Inertial Navigation System
CNN	Convolutional Neural Network	**JRC**	Joint Research Centre
COP	Common Operational Picture	**LEAs**	Law Enforcement Agencies
DRI	Direct Remote Identification	**LOS**	Line of Sight
EASA	European Union Aviation Safety Agency	**MALE**	Medium Altitude Long Endurance
EMI	Electromagnetic Interference	**NATO**	North Atlantic Treaty Organization
EO/IR	Electro-optical/Infrared	**NLOS**	Non-Line of Sight
EU	European Union	**PTZ**	Pan-Tilt-Zoom
EW	Electronic Warfare	**px**	Pixels (image resolution, vertical count)
FAR	False Alarm Rate	**RBI**	Remote Biometric Identification
FCT	Fight against Crime and Terrorism	**RCS**	Radar Cross Section
FoV	Field of View	**RF**	Radiofrequency
FPV	First Person View	**RGB**	Red-Green-Blue
FRIA	Fundamental Rights Impact Assessment	**SDR**	Software Defined Radio
GCS	Ground Control Station	**SIGINT**	Signals Intelligence
GDPR	General Data Protection Regulation	**SVM**	Support Vector Machine
GNSS	Global Navigation Satellite System	**SWaP**	Size, Weight, and Power
GPU	Graphics Processing Unit	**TRL**	Technology Readiness Level
HALE	High Altitude Long Endurance	**UAVs**	Unmanned Aerial Vehicles

06

EXECUTIVE SUMMARY

Non-cooperative drone operations are now a routine problem for LEAs at bounded civil-security sites. A growing share falls outside the assumption on which passive radio-frequency (RF) detection rests because it flies pre-programmed GNSS waypoints, is guided by onboard vision, or is controlled through a physical link. RF silence removes one detection route; it does not make the aircraft invisible to radar, EO/IR or acoustic sensing. The operators most exposed to that gap are frequently those least able to close it.

This report asks a narrower question than which modality is superior: what detection capability a budget-constrained operator obtains, over what distance, and where that distance suffices. It is a comparative review of literature, EU law, standards and public deployment evidence completed to 27 July 2026; it conducts no new trials and assesses readiness for defined configurations at defined sites, not for modalities.

Reach is primarily governed by target size. Wingspan-scaling of a related-party field evaluation gives indicative camera-only median detection distances of approximately 32–41 m for a 0.35 m platform, rising to 130–164 m for the 1.42 m object actually measured (Table 10). The source used a non-representative target and cameras tuned for avian detection; the figures bound the pattern indicatively and are not independent validation.

Converted into time, these radii define the capability. At a 40 m visible-band perimeter, a 0.35 m platform transiting at 15 m/s is exposed for under three seconds and a fast FPV platform at 35 m/s for under two. In barrier-coverage terms [47], such a field delivers weak, probabilistic coverage of constrained approach corridors, not strong coverage of an airspace volume. Fast approach needs a different geometry, based on acoustic nodes in depth; neither its range nor its cost is evidenced here, and characterising both, with thermal, is the principal research recommendation.

On cost, an author-supplied scenario puts the equipment allowance at approximately €16,650–€21,800, or €1,700–€2,200 per node, equipment only (daylight-hours, visible band). They are arithmetic combinations of stated line items, not validated costs, and exclude lifecycle items and the fixed wide-field cameras the pattern requires. The evidential burden differs by site: where the comparator is no capability at all, a deployment must be better than nothing; at designated critical infrastructure, where EU policy calls for multi-sensor architectures [37], it must demonstrate what it adds.

Three author-defined patterns are distinguished. Autonomous Optical pairs a fixed wide-field camera with an internally cued PTZ and can complete the optical search-to-classification chain unaided. Light Hybrid retains that core and adds only the modality the site's threat model justifies. Heavy Hybrid integrates radar, passive RF, EO/IR and, where justified, acoustic sensing within a common C2 environment. No pattern is universally optimal; the report recommends comparative trials, configuration-specific acceptance testing and an RF-silent stratum in the CEN Workshop Agreement (CWA) 18150 counter-UAS test methodology [52] before any is relied upon in procurement.

1 - INTRODUCTION

The rapid democratisation and technological evolution of UAVs in European airspace has transformed non-cooperative drone operations from an emerging security challenge into a critical operational threat for LEAs.

In urban and peri-urban environments, the misuse of these UAVs can pose a threat, compromising the safety and operational capacity of critical infrastructure and border management, as well as public safety at mass events.

Radar, passive RF, acoustic and optical sensors are all used for UAV detection. Their suitability depends on what the target emits or reflects, the site geometry, environmental conditions, the required operational outcome and the integration of the complete system.

A growing share of non-cooperative flights falls outside the assumption on which passive RF detection rests, namely that the aircraft is in radio contact with an operator. This report uses the term “RF-silent” for a UAV that exposes no command, telemetry or identification signal detectable by a deployed passive RF sensor. Silence can arise in three ways: the aircraft navigates autonomously between pre-programmed GNSS waypoints; it is guided by onboard vision and AI; or it is controlled through a physical link such as a cable or an unspooling optical fibre. NATO Allied Command Transformation records that fibre-optic-controlled FPV drones entered battlefield use from late 2024 and that electronic-warfare counter-UAS systems are ineffective against them [24]. RF silence removes one detection route; it does not make the aircraft invisible to active radar, optical or acoustic sensing.

UAVs flying in this mode operate without emitting radio frequency signals that can be intercepted. These UAVs can fly via autonomous navigation based on pre-programmed GNSS waypoints, using onboard artificial vision algorithms and AI, or guided by cables or fibre optics.

In this type of scenario, RF technology is ineffective, as it relies on intercepting radio frequency signals. The deployment of active radars in an urban environment is also accompanied by a series of operational limitations: interference (clutter) from unwanted echoes originating from fixed structures, a high false alarm rate, and the high cost of deployment and maintenance.

Acoustic sensors in public spaces can suffer from ambient-noise interference, which may mask UAV signatures. If intelligible speech or other personal data are processed, the applicable data-protection regime and safeguards depend on the purpose, controller, technical design and national law; microphones do not automatically breach the GDPR, and consent is not a universal legal basis for LEA processing.

These differentiated limitations justify a comparative assessment of alternative and multimodal architectures. The relevant question is not which modality is universally superior, but which defined configuration meets the protected site's operational requirement with proportionate cost, legal risk and residual blind spots.

This report evaluates the operational, technical, economic and regulatory feasibility of UAV-detection technologies adapted to RF-silent threat environments. Its central proposition is one of complementarity: no modality is universally sufficient in RF-silent conditions, although a single-modality configuration may meet a limited requirement at a specific site where site-specific acceptance testing demonstrates that it does. The practical question is therefore not which modality wins but which configuration meets the requirement of a given site, and how short-range, low-cost modalities can be combined where none does so on its own, trading coverage, exposure time and cost against one another. Within that frame the report examines how far an optical architecture combining fixed wide-field search with internally cued PTZ tracking can carry the detection chain on its own, where that reach ends, and which complementary modalities close the resulting gaps at acceptable cost. The relevant benchmark is not a full layered architecture, which is beyond the reach of many operators, but the capability those operators would otherwise have, which is frequently none.

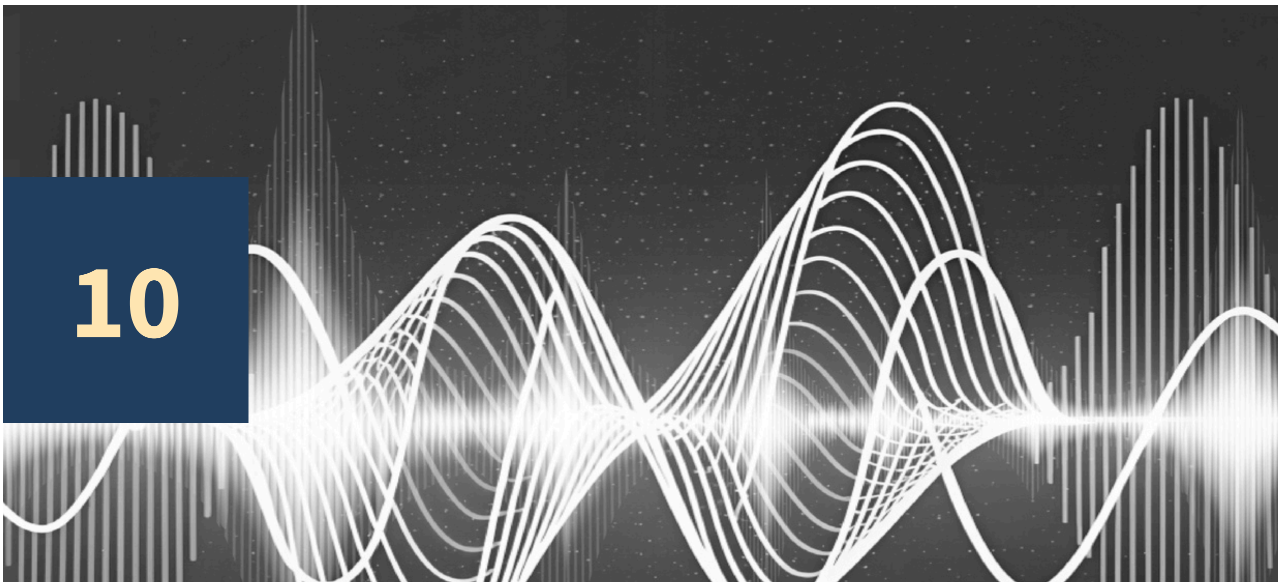
1.1 - THREAT MODEL ADDRESSED

The conclusions of this report are bounded by an explicit threat model, stated here so that a reader can judge whether they transfer to a particular site. The report addresses small non-cooperative UAVs with a maximum horizontal dimension of roughly 0.25 m to 1.5 m, corresponding to groups G1 to G3 of Table 4: consumer and prosumer multirotors, racing and FPV airframes, and small fixed-wing platforms. These are assumed to be RF-silent, that is autonomous on pre-programmed waypoints, vision-guided, or controlled through a cable or optical fibre.

Two mission profiles are considered, because they load the detection problem very differently. The first is approach or delivery: the aircraft transits towards the protected site, typically at low altitude to exploit terrain and structure masking and to keep a physical link intact, and its exposure to any sensor is brief. The second is observation: the aircraft loiters over or near the site because the mission requires dwell time, and its exposure grows with the duration of that dwell. Section 3.7 shows why these two profiles behave differently under a distributed sensor field. The two profiles are not equally covered here. The evidence assembled in this report characterises the observation profile, in which exposure accumulates with dwell time. For fast approach it shows only that a visible-band perimeter gives too little exposure to be useful, without establishing what would replace it.

Three things are outside the scope of this report and its conclusions should not be read as applying to them. First, larger platforms: groups G4 to G8 of Table 4, including MALE, HALE and other strategic aircraft, appear in Table 6 only for geometric comparison. Second, standoff observation from high altitude, where a target may accomplish its mission entirely outside the sensing volume of a short-range field. Third, coordinated multi-aircraft or swarm operations, and mitigation or neutralisation of any kind, which raise separate legal and technical questions.

The report applies to two classes of protected site, and the burden of proof it places on a deployment differs between them. The first class is bounded civil-security sites operated under constrained budgets: perimeters of installations, event venues, custodial and judicial facilities and comparable locations for which a full layered counter-UAS architecture is not financially or organisationally attainable. At these sites a low-cost non-RF field may constitute the primary detection capability, and the benchmark against which it should be judged is the capability the operator would otherwise have, which is frequently none. The second class is designated critical infrastructure, where EU policy sets a higher bar: the Action Plan on Drone and Counter-Drone Security calls for a multi-sensor approach integrated through command-and-control software [37]. At these sites the patterns examined here are not offered as a substitute for a layered architecture, and their role is narrower: extending coverage along approach corridors that a layered core does not reach, densifying detection at low altitude where radar performs poorly against small targets, or providing proportionate cover for secondary assets within an operator's estate that do not individually justify full layered instrumentation. The distinction is material for procurement, because the same equipment carries a different evidential burden in each case: at a non-critical site it must be demonstrably better than nothing, whereas at critical infrastructure it must demonstrably add something a layered system does not already provide.



2 - APPROACH

2.1 - REVIEW APPROACH

This report is a targeted, evidence-informed comparative review, not a registered systematic review or meta-analysis. Source identification and checking were completed to 27 July 2026 through publisher databases, EU and national institutional repositories, standards catalogues and citation tracing. Search combinations covered counter-UAS, drone detection, RF detection, radar, EO/IR, acoustic sensing, sensor fusion, law enforcement, Europe, testing, interoperability, GDPR, the Law Enforcement Directive and the AI Act.

Sources were included when they addressed the detection, tracking or classification of small or non-cooperative UAS; described a relevant test, operational constraint, standard or legal rule; and provided sufficient provenance to assess the claim. Sources were excluded from the comparative evidentiary basis when they concerned mitigation only, lacked traceable methods, or relied on confidential or unpublished information. Evidence was prioritised in this order: EU and public institutional sources; peer-reviewed studies; official standards; transparent field evaluations; and vendor documentation used only for product context. For illustration, excluded categories included studies addressing UAV mitigation or neutralisation rather than detection (e.g., jamming and spoofing techniques), commercial vendor material without independently verifiable methodology, and publications addressing platforms or scenarios outside the threat model defined in Section 1 (e.g., MALE/HALE aircraft, coordinated swarm detection).

2.2 - ANALYTICAL METHOD

The comparison considers observability of RF-silent targets, detection and classification function, range dependencies, false-alarm mechanisms, environmental resilience, integration needs, cost and legal conditions. Results are synthesised qualitatively because the reviewed sources use different targets, ranges, datasets, test geometries and metrics. Readiness is assessed for a defined configuration and scenario rather than assigned to an entire sensing modality.

2.3 - LIMITATIONS

The review is not exhaustive, no LEA interviews were conducted, and the authors did not independently reproduce published performance results. Statements in this report about the relative range of different modalities rest on physical reasoning and should not be read as measured comparisons. Heterogeneous evidence prevents a defensible numerical ranking across modalities. Public vendor material and the related-party DTBird® case are clearly identified and are not treated as independent comparative evidence. The budget scenario is illustrative and omits site survey, civil works, integration, communications, training, maintenance and other lifecycle costs. These limitations mean that procurement decisions should be supported by representative site-specific acceptance testing under operationally relevant conditions.

3 - CURRENT CHALLENGE

3.1 - CURRENT CHALLENGE: RF-SILENT

Driven by recent technological advancements, there is a proliferation of link -jamming -resistant, "RF-silent" UAV systems [1][24]. These platforms are designed to operate without a radio link between the aircraft and the ground control station. With that link absent, the emissions on which passive RF detection depends are not present, so the aircraft is not observable by that method. This is a statement about one detection route and not about the platform as a whole: onboard electronics, a video downlink to an onboard recorder or a payload emitter may still radiate, and the aircraft remains observable in principle to active radar, optical, thermal and acoustic sensing.

Among these new types, we highlight the following:

- **Fibre-optic guided FPVs.** These UAVs replace wireless links with a microfibre that unrolls during flight. NATO Allied Command Transformation records that a new generation of fibre-optic-controlled FPV drones entered battlefield use from late 2024 and states that electronic-warfare counter-UAS systems are ineffective against this class, whose combination of high manoeuvrability, jamming immunity and low visual and radar signature is identified as the core of the problem [24]. The operational requirement set issued for the corresponding NATO Innovation Challenge is a useful external benchmark, although a military rather than a civil one: detection of small drones at up to 500 m, operation at night and in poor weather, modular open architecture and a unit price of €50,000–€100,000, with thermal and optical target recognition among the approaches invited [24][25].

- **UAVs with automatic or GPS flight.** They follow pre-programmed routes using INS or GPS waypoints.

- **UAVs with AI navigation.** Innovations in computer vision allow UAVs to navigate autonomously through visual terrain matching.

Because these models do not rely on an RF command link, they can evade passive RF detection of that link and resist link jamming [8]. Their navigation resilience must be assessed separately: a platform using GNSS waypoints may remain vulnerable to GNSS jamming or spoofing, whereas onboard vision, inertial navigation or physical guidance may reduce or remove that dependency.

In addition to innovations in UAVs, the manufacture of these devices has become less expensive, leading to the development of saturation and deception tactics. Attackers deploy standard radio-controlled UAVs alongside fibre-optic or autonomous UAVs. This forces security forces to deploy wide-area jammers, which neutralise conventional UAVs but have no effect on fibre-optic platforms; these take advantage of the defenders' distraction to penetrate the security bubble and strike critical infrastructure. Documented experience from recent conflict zones illustrates these saturation and electronic warfare dynamics in practice [22][23]. The sources cited here concern situational awareness and software-defined command systems rather than counter-UAS test data, and are used only to describe the operational pattern; they are not evidence of detection performance.

3.2 - RADAR

Radar (Radio Detection and Ranging) technology is the most established and traditional method of aerial surveillance, designed for national security and defence [7]. This technology works by emitting radio waves that bounce (echo) off aerial objects (aircraft, birds, UAVs, etc.), and upon receiving them back, we can determine the following characteristics: their spatial coordinates, relative speed and direction of flight. [7] [11].

Radar can provide long-range and wide-area coverage, including against non-emitting targets. Reported range is target- and configuration-dependent and is strongly influenced by radar cross-section, altitude, clutter, power, waveform, antenna geometry and processing; it should not be presented as universally greater than every RF, acoustic or EO/IR configuration [11][42].

Furthermore, unlike optical cameras, radar performance is independent of lighting conditions and remains effective under low-visibility conditions such as fog. Although radar systems can operate at greater distances and under adverse weather conditions, heavy rain, hail, or snowfall can reflect and scatter radio waves, potentially saturating the receiver and significantly reducing the system's effective range and sensitivity. [7]

In urban and peri-urban environments, radar performance can be materially degraded by multipath clutter from surrounding structures and by false alarms from birds and other non-target returns; the extent of that degradation is site- and configuration-dependent and should be established by site testing rather than assumed [11][42].

Radar detection depends on the energy a target reflects back to the receiver. Small airframes present a low radar cross-section, and airframe materials with low electromagnetic reflectivity reduce it further, so returns from such targets may fall close to the clutter floor and be suppressed by the filtering that a radar applies to reject background. This is a general property of the detection principle rather than a finding of any single study. To contextualise the difficulty of UAV detection, Table 4 shows the standard sizes for different types of UAVs, as well as their group classification.

From a logistical standpoint, radar procurement, siting, integration and maintenance can present significant barriers for LEAs.

3.3 - RADIO FREQUENCY (RF)

Along with radar, RF technology is one of the most widely used technologies in UAV detection [12]. Unlike radar, RF sensors operate passively, intercepting and analysing signals from the electromagnetic spectrum that UAVs use to communicate with their controllers or GCS [12].

Many commercial UAVs use recognisable command or telemetry signals in common bands, although frequencies and protocols vary. Spectrum-analysis and RF-fingerprinting methods can support detection or classification when a sufficiently strong, covered emission is present [9][12].

They offer a broad detection range (standoff range), operating even beyond non-line-of-sight conditions by capturing signals that bounce off structures. Furthermore, they can easily be integrated with other security and surveillance technologies, such as cameras, infrared sensors, acoustic sensors, etc., to provide a more comprehensive solution.

The structural vulnerability of RF lies in the emergence of RF-Silent threat vectors. When a UAV operates using pre-programmed GNSS waypoints, guided autonomously by AI, or via physical fibre-optic links they do not emit the command or telemetry signals on which passive RF detection depends, so that detection route does not apply to them.

RF performance can also be affected by interference from communications, industrial equipment and other emitters. The resulting detection and classification impact is configuration- and environment-dependent and should be measured during site testing [10][12][13].

3.4 - ACOUSTIC SENSORS

A 2019 study [14] reported classification results above 90% for a defined audio dataset and model. This is a controlled classification result and does not establish a general operational detection rate or a modality-level TRL.

This technology is based on passive detection. It captures and analyses the acoustic signatures generated by the engines and propellers of UAVs during operation. Directional or omnidirectional microphones are used for capture (with directional microphones being particularly useful for filtering out background noise and focusing on specific areas). [4]

To distinguish a UAV from other noises, these systems rely on training machine learning algorithms (standard pattern-recognition algorithms) to develop a recognition system.

Once the sound has been captured, a spectral analysis is carried out to break down the signal into its frequency components, and this is then fed into the previously trained recognition system. Using a single microphone, we can determine whether or not a UAV is present; however, by deploying multiple microphones, it is possible to determine the UAV's location using triangulation techniques based on the times at which the sound is received by each acoustic sensor.

The main advantage of this system is that it emits neither signals nor radiation, making it undetectable to both UAVs and their operators, thus allowing for discreet operation. Because the sensed quantity is acoustic rather than electromagnetic, the detection principle itself is not degraded by radio-frequency congestion or jamming, which can be an advantage in electromagnetically saturated environments. This concerns the sensing principle and not the equipment: the microphones, digitisers and processing hardware remain electronic and require the usual electromagnetic-compatibility measures.

Because acoustic detection depends on the sound the airframe produces rather than on any transmission, it remains applicable to the RF-silent platforms described in Section 3 on RF Silent, whose navigation by pre-programmed waypoints, onboard vision or physical link places them outside the reach of passive RF scanning [4].

These systems can use comparatively simple microphone hardware and can be integrated into hybrid architectures, but the cost of a deployable acoustic subsystem also includes array geometry, weatherproofing, synchronisation, processing, calibration, integration and maintenance. The reviewed evidence does not support a universal cost advantage over other sensing modalities.

Despite the advantages of this system, it has some critical disadvantages and limitations worth highlighting. The first of these is that, whilst it is not sensitive to environments with a high volume of electromagnetic signals, it is sensitive to ambient noise: urban traffic, wind, human voices and other types of noise can mask the acoustic signatures of UAVs. Furthermore, adverse weather conditions (rain, wind, snow, etc.) not only add noise but also distort the original signal. [4][12]

Sound intensity falls with distance through geometric spreading and atmospheric absorption, and the higher frequencies that carry much of a rotor signature attenuate fastest, so acoustic detection is inherently a short-range method [4][12]. This report does not quantify that range. Within the search scope of this review, no acoustic field evaluation was located reporting detection probability as a function of distance under conditions comparable to those of Table 9; the acoustic sources identified here report classification performance or localisation accuracy rather than distance-resolved detection. The comparative statement that acoustic range is shorter than that of other modalities is therefore made on physical grounds rather than on measured evidence.

UAV acoustic and radio-frequency signatures vary across models and operating conditions. Signature-based systems therefore require maintained datasets and representative validation.

Finally, acoustic deployment in public spaces requires a case-specific privacy and data-protection assessment. Where intelligible speech or other personal data are processed, the applicable framework may be the GDPR, the Law Enforcement Directive and national law, depending on purpose and controller. Appropriate measures may include edge feature extraction, avoidance of speech recording, short retention, access controls and audit logging; consent and licensing are not automatic requirements in every LEA use case [16].

3.5 - OPTICAL SENSORS

EO/IR sensing may not be characterised solely as a confirmation or fallback layer. At bounded sites with suitable visibility, lines of sight and camera coverage, a fixed wide-field detector combined with an internally cued PTZ can provide an autonomous, RF-independent chain for search, detection, tracking, magnification and classification [40]. In this report autonomous denotes the functional autonomy of the optical chain, meaning that it requires no cueing from another sensing modality, and not operational sufficiency, meaning that it meets the detection requirement of a given site. The two properties are assessed separately throughout. RGB and thermal imaging may be used separately or together, with computer vision and deep-learning algorithms supporting the required functions [6][40].

PTZ cameras can act as trackers, automatically pointing towards a target and providing detailed tracking and magnification [40]. Cueing may come from radar or passive RF in a hybrid architecture, but it need not depend on a non-optical sensor: a fixed wide-angle camera can perform continuous area-wide detection and cue the PTZ internally within the same optical layer. Unlu et al. demonstrate this autonomous multi-camera architecture.

Monocular imagery can support approximate range estimation when target dimensions or other scene constraints are known. For a non-cooperative UAV, however, uncertainty in size, pose, calibration and image quality can materially affect the estimate. An optical architecture may therefore remain autonomous for search, detection, tracking and classification without necessarily providing the precise three-dimensional location or range required for every tactical response [7][42].

Stereo or multi-view systems can estimate depth from disparity without assuming the target's actual size, but they require calibrated geometry, overlapping views, reliable correspondence and sufficient target detail; accuracy typically degrades with distance. Procurement and acceptance testing should therefore treat precise localisation and ranging as a separate performance requirement from autonomous optical detection [7][42].

Table 6 gives the upper geometric bound on the distance at which a UAV of each size group of Table 5 subtends 125 pixels. This value is well above what a detector typically requires to register the presence of an object. The approach follows the pixel-density method of the video-surveillance application standard [28], adapted to a pixel count on the target because the platforms of concern are sub-metre. Here, 'subtend' refers to the angular size the target occupies in the camera's field of view at a given distance, expressed as a pixel count: the number of pixels the target's largest dimension (wingspan) would span on the sensor, calculated using the sensor's vertical pixel density as a proxy for angular resolution. A larger pixel count corresponds to a closer or larger target; a smaller one to a more distant or smaller target. It is a bound set by optics alone; lens quality, focus, target aspect and motion, compression, background, weather, illumination and detector performance all reduce it, and Annex A states the assumptions in full.

As an empirical complement to the theoretical figures in Table 6, Table 9 presents field-measured detection distances obtained using a GPS-tracked avian-mimic drone (1.42 m wingspan) flown under controlled conditions to evaluate a commercial camera-based detection system developed by Liquen [34], which has collaborated in R&D projects with some of the authors of this report. Unlike Table 6, these figures are not calculated from optical specifications alone but derived from actual recorded detection events, synchronised with GPS ground-truth positioning, and modelled statistically to estimate detectability thresholds as a function of distance. It should be noted that the reference object was designed to mimic the morphology of a medium-sized bird of prey rather than a typical threat-representative UAV; the figures are therefore indicative of camera-only detection performance for a similarly-sized flying object, not a validated UAV-specific trial.

Like acoustic sensors, optical sensors do not emit radiation or signals, which allows for discreet operation and safe use in urban environments. Furthermore, as this approach does not rely on the reception of electromagnetic signals, it does not require radio spectrum licences, which makes its adoption by LEAs easier and more cost-effective (see Section 4.1.1).

Despite these technical advantages, optical sensors are dependent on visibility in the environment; in adverse weather conditions, their effective range may be reduced as image clarity diminishes. Obstructions within the field of view, such as vegetation, buildings and other types of structures, can create blind spots where the system is unable to detect airborne objects, and lens contamination (dirt, condensation) is a further practical limitation documented in EU testing frameworks [43] [7].

Illumination is a distinct constraint from weather and is treated separately here because it bears on the configuration costed in Annex A. A visible-band RGB camera, including one with a day/night IR-cut filter, depends on ambient or artificial illumination; comparative testing of passive imagers for counter-UAS use reports that long-wave infrared gave the best target-to-background contrast, with the visible band second and short-wave infrared performing poorly against the UAS tested [41]. Since a substantial share of non-cooperative incursions may occur at night, an autonomous optical configuration intended to operate around the clock requires either a thermal channel or controlled site illumination. Neither is included in the illustrative equipment scenario of Table 7, which is therefore a daylight-hours configuration; adding a thermal layer would raise both the equipment cost and the integration effort, and the comparison in Section 5.2 should be read with that exclusion in mind.

The ability to identify objects is limited to the distance at which the object still occupies a sufficient number of pixels for analysis. To achieve greater distances, cameras must have a longer focal length, which results in a loss of the field of view that can be covered.

For LEAs, an all-optical configuration may be proportionate where a bounded site's threat model, lines of sight, wide-field coverage and acceptance tests support it. The fixed camera provides continuous search and initial detection; the internally cued PTZ provides tracking, magnification and classification. Consistent with the position taken throughout this report, such a configuration is presented as an entry point into a combination rather than as a self-sufficient answer: thermal, acoustic or passive-RF nodes address the conditions under which a visible-band chain degrades, principally darkness, poor visibility and targets outside optical line of sight, and the design question is which of them a given site needs and at what density. Procurement should compare complete configurations against common performance and lifecycle criteria.

3.6 - HYBRID SYSTEMS

No reviewed source supports a complete and reliable single-modality solution across all operational environments. In this report we narrow the aim to which combination of modalities a given site requires, and which viable starting point the available evidence best supports. At bounded sites, a wide-angle camera combined with internally cued PTZ tracking can provide an RF-independent optical search-to-classification chain [40], the chain for which this report assembled both a demonstrated end-to-end implementation and distance evidence, and which remains available when the target emits nothing. Its acceptability remains conditional on visibility, coverage, target size, required warning time and representative field validation. An autonomous optical core remains available when the target emits nothing and is the component of a non-RF combination whose capability this report is able to state rather than assume, on the basis of a demonstrated end-to-end chain and the distance evidence of Table 10; it is proposed as a bounded partial capability, not as a substitute for a layered architecture.

To address modality-specific gaps, C2 platforms can integrate multiple sensors. Commercial examples include SkyCtrl [30][31], UAS Sentry [32][33], AARTOS [26] and ELI-4030 Drone Guard [27]. For the purposes of this report, the terms Autonomous Optical, Light Hybrid and Heavy Hybrid are author-defined deployment patterns rather than an established industry or academic taxonomy.

Author-defined deployment patterns

Architecture	Configuration and functional role	Appropriate use and principal trade-off
Autonomous Optical	Fixed wide-field camera performs continuous search and initial detection; internally cued PTZ performs tracking, magnification, classification and evidence collection.	Bounded partial capability, not a substitute for a layered architecture, for sites with suitable line of sight, visibility, coverage and warning time. Optical degradation and precise 3D localisation must be assessed separately.
Light Hybrid (Selective Modular)	Autonomous optical core plus only the site-justified complementary sensor, often passive RF. The added sensor can cue or corroborate; the optical layer retains its own search-to-classification chain.	Threat-driven modular option where incremental observability or resilience justifies added cost and complexity. It is not simply a smaller Heavy Hybrid.
Heavy Hybrid (Full-Spectrum Layered)	Broad integration of radar, passive RF, EO/IR and, where justified, acoustic sensing or effectors through an advanced C2/common operational picture.	Suited to high-criticality sites requiring maximum layered coverage and resilience; carries the greatest integration, calibration, legal, lifecycle and operator burden.

The functional flow would be:

- Passive RF can add an early cue, protocol information or geolocation where a detectable emission exists; active radar can add wide-area warning for emitting and non-emitting targets through reflected energy, subject to radar cross-section and clutter. A wide-field camera continues its own optical search and can also accept external cues. The PTZ then provides tracking, magnification, classification and evidential imagery, while C2 time-stamps, associates and presents the observations with sensor provenance for the operator.

In Autonomous Optical, the wide-field camera cues the PTZ internally. In Light Hybrid, the selected complementary sensor adds observability without removing that internal optical path. In Heavy Hybrid, the C2 platform coordinates a wider set of layers. In all cases, computer-vision models support detection, tracking and classification, and the optical chain can continue when a passive RF cue is unavailable [40].

Hybrid systems can combine observations from different modalities, but complementary sensors do not automatically eliminate blind spots. Fusion quality, calibration, time synchronisation, correlated environmental failures and operator workload must be tested as part of the complete configuration.
In radar-plus-optical systems, cross-checking observations may reduce some false alarms and support classification. The benefit depends on sensor calibration, association logic, target visibility and representative validation; correlated failures or poor fusion can preserve or create errors.

A selective modular combination of passive RF and AI-assisted EO/IR may be a proportionate candidate for some LEA sites. Passive RF can add an external cue when a detectable emission exists; the optical wide-field-plus-PTZ layer can still perform its own search, tracking and classification chain. The combination does not eliminate the limitations of either modality and must be compared with an autonomous optical configuration and other credible alternatives under equivalent site and test conditions.

In an RF-plus-optical configuration, passive RF may provide an additional cue and, in favourable cases, support protocol identification or geolocation when a detectable signal exists. The optical layer retains its internally cued search-to-classification function and can also exploit the RF cue. Achievable RF range is configuration-dependent; no generic numerical range is assumed.

These models can provide visual evidence required by human operators (human-in-the-loop) to make tactical and legal decisions.

Within this framework, a selective modular system may provide broader coverage than an individual sensor and lower cost than some full-spectrum infrastructures. This is a design hypothesis to be demonstrated through site-specific comparison and acceptance testing, not a general finding of optimality.

3.7 - DEPLOYMENT GEOMETRY AND BARRIER COVERAGE

The preceding subsections characterise each modality at the level of a single sensor. Whether the resulting detection distances are sufficient is not a property of the sensor but of the deployment geometry, and that question has an established formal treatment in the sensor-network literature under the heading of barrier coverage [47]. Introducing that vocabulary here allows the limitations of short-range non-RF modalities to be stated precisely rather than qualitatively, and it supplies the analytical basis for the complementarity argument developed in Sections 5 and 6.

Kumar, Lai and Arora define k-barrier coverage of a belt region as the property that any intruder crossing the belt is detected by at least k sensors, and distinguish strong barrier coverage, in which detection holds regardless of the crossing path, from weak barrier coverage, in which it holds only for paths crossing the belt orthogonally; the same work develops probabilistic barrier coverage, deriving the sensor density needed to reach a stated detection probability rather than a guarantee [47]. That distinction is the appropriate way to state the principal limitation of a low-cost non-RF sensor field. Given per-node detection distances of the order reported in Table 10, such a field can realistically be designed for weak, probabilistic barrier coverage of constrained approach corridors. It cannot provide strong barrier coverage of an airspace volume: a target with sufficient altitude and standoff crosses above the field without entering any node's sensing region.

Two refinements of the classical model are material here. First, cameras and directional microphones are not omnidirectional disc sensors but cones of limited field of view, for which a separate body of results exists [48]; PTZ cameras in particular have been modelled explicitly as directional sensors for border and critical-infrastructure surveillance, with instantaneous detection, tracking continuity and sensor cost treated as joint and partly conflicting objectives [50]. Second, classical barrier coverage treats the intruder as a point. Si et al. reject that idealisation for camera networks and introduce a resolution criterion derived from a three-dimensional sensing model, in which coverage requires the target to subtend sufficient pixels rather than merely to fall inside a geometric sector [51]. The pixel-density geometry of Table 6 is an instance of that criterion; read together, Tables 3 and 10 supply the per-node sensing model that a barrier-coverage design for this application would take as input.

Within that framework two asymmetries favour the defender, and in the authors' assessment they are the strongest argument available for low-cost non-RF deployments. The first is transit: where an approach corridor is constrained, cumulative detection probability across successive nodes rises quickly even when the probability at any single node is modest, so that node count partially substitutes for node range. The second is dwell: a UAV conducting reconnaissance or surveillance must remain within or near the protected volume in order to be useful, and cumulative detection probability rises with exposure time, so the more valuable the mission is to its operator the more exposed it becomes.

Complementarity follows from the same framework rather than from preference. Barrier coverage has been extended to hybrid directional networks in which nodes of differing type and capability jointly achieve a coverage guarantee [49], which is the formal counterpart of mixing visible cameras, thermal or dual-sensor PTZ units and acoustic arrays within a single deployment. It also makes the cost trade-off explicit. The evidentiary basis for the two non-visible components of such a layout is weaker than for the visible-band core: this review did not locate, within its search scope, thermal or acoustic evidence comparable to that of Table 9, so the case for including them rests on the physical complementarity described in Sections 3.4 and 3.5 rather than on comparable performance data. Characterising those two modalities to the same standard as Table 10 is accordingly one of the priorities in Section 6. Because thermal and dual-sensor units carry a unit cost several times that of a visible-band PTZ, a tiered layout , a majority of low-cost visible nodes for corridor coverage, with thermal or dual units placed on the approach axes where night and adverse-weather performance is decisive, offers a more favourable coverage-per-euro profile than either a uniform visible deployment, which is blind at night, or a uniform thermal one, which is unaffordable at density. The scenario costed in Table 7 is a uniform visible configuration and should be read as the lower bound of that design space rather than as a recommended layout.

Finally, the comparator matters, and it differs between the two classes of site defined in Section 1.1. At designated critical infrastructure the comparator is a layered multi-sensor architecture, and a non-RF field must justify itself by what it adds to that architecture rather than by what it replaces. At a site that is not so designated, and for a resource-constrained agency, the realistic alternative is frequently no detection capability at all, because the cost of a layered architecture places it beyond the reach of many such operators. Assessed against that comparator, a non-RF sensor field providing weak, probabilistic barrier coverage of likely approach corridors is not a substitute for a layered architecture and is not offered as one. It is a proportionate partial capability whose value lies in raising the cost, the risk and the required sophistication of an incursion rather than in guaranteeing its interception.

4 - ANALYSIS

4.1 - REGULATORY FRAMEWORK

The deployment of UAV detection systems is not only constrained by technical capabilities, but is also strictly conditioned by a complex legal framework governing airspace use, the radio-frequency spectrum, and citizen privacy. The operational viability of any solution for LEAs depends directly on its ability to integrate into this framework without creating unmanageable legal conflicts. The body of regulations presented below ensures the deployment and operational functionality of these technologies within a framework of legal and technical rigour, securing interoperability between the various air defence systems across Europe:

1. Commission Implementing Regulation (EU) 2019/947 and Commission Delegated Regulation (EU) 2019/945. The Implementing Regulation establishes rules and procedures for UAS operations and makes direct remote identification a condition of specified classes and operations; the technical requirements for the DRI function and the C0–C6 class marking are laid down in the Delegated Regulation [46]. The two must be read together. DRI is not universal: applicability depends on the aircraft, class, category, operation and applicable transitional or national provisions. A DRI receiver can assist with compliant broadcasts but does not replace broader detection of non-cooperative or exempt aircraft [17].

2. Royal Decree 517/2024 (Spain). This decree develops the national legal regime for the civil use of UAS, exercising the margin left to Member States by the EU framework: it governs activities excluded from the Basic Regulation, national standard scenarios (STS-ES) and remote-pilot training, and it creates a register of unmanned aircraft held by the Ministry of the Interior together with reporting duties on commercialisation, sale and transfer (Articles 53–57). For a detection deployment, the operative consequence is that the identification data an LEA may lawfully obtain, and from which register, is a matter of national law rather than of the detection technology; the precise obligations must be confirmed against the consolidated text and any subsequent amendments. Processing by surveillance systems remains subject to the applicable Spanish and EU data-protection or law-enforcement regime [18][19].

3. Action Plan on Drone and Counter-Drone Security. In light of current regulations and the present scenario, the European Commission has since launched the Action Plan on Drone and Counter-Drone Security (published 11 February 2026), a strategic document bridging technological requirements with the regulatory framework. Its objective is to coordinate Member States in developing UAV detection capabilities that are both effective and proportionate, enabling LEAs to protect critical infrastructure and public events within a unified legal environment. [37]

4.1.1 - COMPARISON OF REGULATORY BURDEN BY TECHNOLOGY

The regulatory burden varies significantly across the different UAV detection technologies, making it a decisive factor in their deployment by LEAs. Table 1 summarises the regulatory burden associated with each option:

1. Radar. Spectrum, conformity and authorisation requirements depend on the frequency band, power, equipment and national allocation. An individual transmission licence should not be assumed for every radar configuration, but a site-specific spectrum and safety assessment is required.

2. Radio Frequency (RF). Passive reception avoids transmission authorisation, but lawful monitoring, retention and use of intercepted or DRI-derived data remain purpose- and jurisdiction-specific. DRI compliance by the aircraft is distinct from the legal basis on which an LEA or site operator processes receiver outputs.

3. Optical Sensors (EO/IR). Passive sensors exempt from spectrum licensing. Their regulatory burden stems from compliance with the EU Artificial Intelligence Act (AI Act – Regulation (EU) 2024/1689), including a case-specific assessment of the intended purpose and the provisions on Remote Biometric Identification (RBI). A Fundamental Rights Impact Assessment under Article 27 is not automatic for every high-risk system, but LEAs should not assume it will not apply to them: the obligation attaches to deployers that are bodies governed by public law or private entities providing public services. The exclusion in Article 27(1) covers only the area listed in Annex III, point 2 (safety components in the management and operation of critical digital infrastructure, road traffic or the supply of water, gas, heating or electricity) and does not extend to the physical protection of critical infrastructure generally. Where the system is high-risk, a FRIA should therefore be planned for; Article 27 applies from 2 August 2026. Edge-based anonymisation is recommended as a safeguard rather than separately mandated in all cases [21].

4. Acoustic Sensors. Their legal position depends on whether the design processes intelligible speech or other personal data, the operational purpose and the controller. The GDPR, the Law Enforcement Directive and national law may apply. Privacy risk can be reduced through data minimisation, edge feature extraction, restricted retention, access control and auditability; neither a GDPR breach nor consent is automatic [16].

5. Light Hybrid (Selective Modular System). Combining passive RF and EO/IR may reduce spectrum-authorisation issues compared with some active-radar configurations, but it is not categorically frictionless. The legal assessment still depends on data, purpose, actor, AI functionality, location and national law.

Table 1: Regulatory Burden Summary

Technology	Regulatory burden and legal conditions
Radar	Active sensor. Spectrum, conformity and authorisation conditions depend on band, power, equipment and national allocation.
Radio Frequency (RF)	Passive reception avoids transmission authorisation; monitoring and processing of RF/DRI-derived data remain purpose- and jurisdiction-specific [17][18].
Acoustic Sensors	Passive sensor. GDPR, LED or national rules may apply if personal data (intelligible speech included) is processed; assessment is design and purpose-specific [16]
Optical Detection (AI)	Passive sensor. Data-protection and AI Act obligations depend on captured data, intended purpose, actor and AI functionality [16][21].
Heavy Hybrid (Full-Spectrum Layered System)	Legal and operational burden is the aggregate of the selected sensors, networks, processing and any effectors; military configurations are not direct LEA comparators.
Light Hybrid (Selective Modular System)	May reduce cost or spectrum burden, but requires the same case-specific assessment of data, AI, cybersecurity and operational purpose.

4.1.2 - CONNECTION WITH THE ACTION PLAN ON DRONE AND COUNTER-DRONE SECURITY

The connection between the European Commission's Action Plan on Drone and Counter-Drone Security and the research presented is established through the assessment of the economic and technical viability of defence systems, using the reference report from the CBO, "Options to Counter Small Unmanned Aircraft Systems" [15] as a bridge.

The European Action Plan is structured around four priorities: prepare, detect, respond and strengthen defence readiness, and calls for proportionate security mitigation measures, in particular for the deployment of counter-drone systems around critical infrastructure [37]. The wording quoted here is a paraphrase and not a verbatim citation. The methodology of this document adopts that need as a central axis to document the gap between available technology and its actual deployment by LEAs.

One qualification must be recorded explicitly, because it bears directly on the central proposition of this report. Section 3.2 of the Action Plan states that the detection of malicious drones relies on several sensors and requires a multi-sensor approach integrated through AI-powered command-and-control software, and it lists software-defined radar, acoustic phased-array microphones, LiDAR, thermal infrared and optical sensors among the technologies to be supported [37]. The same emphasis on multi-sensor data fusion is found in the JRC analysis of counter-drone systems [43]. The autonomous optical pattern examined in this report is therefore a narrower proposition than the direction set at EU policy level: it is put forward as a proportionate option for bounded sites under stated conditions, not as a substitute for the layered, fused architectures that the Action Plan and the JRC evidence base advocate for critical infrastructure protection. Where the two diverge, the burden of demonstration rests on the narrower option, and the comparative trials recommended in Section 6 are the means of discharging it.

The CBO estimates that one illustrative option for protecting a US military installation with a complete layered defence, including complementary sensors and effectors, could cost approximately $74 million [15]. This figure is not a radar price and is not directly comparable with the narrower author-supplied equipment scenario. It nevertheless illustrates why civilian buyers should compare proportionate, configuration-specific alternatives using equivalent scope and lifecycle costs.

European initiatives such as the JRC living lab [20] and COURAGEOUS [29][44] provide test infrastructure, methods and trial experience for comparing C-UAS configurations. They do not by themselves prove that the low-cost scenario in this report meets operational requirements; that conclusion requires testing of the actual configuration under the common protocol.

4.2 - OPERATIONAL READINESS ASSESSMENT

A single TRL cannot be assigned defensibly to radar, passive RF, EO/IR, acoustic sensing or a broad hybrid category. Each modality contains mature products, research prototypes and novel integrations. Operational readiness must be assessed for a defined hardware-software configuration, target set, site, operating concept and legal basis.

Commercial availability, a high score on a curated dataset or an isolated field demonstration is evidence of maturity, but not proof that an integrated system is ready for a particular LEA deployment. Acceptance evidence should report probability of detection, false alarms per unit time, track continuity, localisation error, classification performance, latency, availability and operator workload under representative weather, clutter and target conditions [42][44].

The related-party DTBird® evaluation in Annex A and the author-supplied cost scenario illustrate optical test reporting and budget assumptions; neither is used to establish comparative superiority or a formal TRL. Likewise, the CBO estimate concerns a complete military layered defence including complementary capabilities and cannot be treated as the price of radar or as a direct comparator for the illustrative modular configuration [15]. Table 2 therefore presents readiness cautions rather than modality-level TRLs.

Table 2: Configuration-specific readiness evidence

Technology	Readiness evidence	Range	Principal constraints	Legal conditions
Radar	Mature commercial components; deployment readiness requires configuration- and site-specific acceptance testing.	Target- and configuration-dependent [11] [42]	Small RCS, low altitude, clutter, birds, siting and weather	Spectrum, conformity and authorisation are case-specific
Radio Frequency (RF)	Mature commercial systems for detectable emissions; no coverage of genuinely RF-silent targets.	Emission- and configuration-dependent [12] [42]	Absent/unknown emissions, protocol coverage, interference and antenna geometry	Passive reception; processing and use of outputs remain purpose-specific
Optical (EO/IR)	Mature sensors and commercial analytics; a wide-field camera plus an internally cued PTZ can form an autonomous optical chain, while deployment readiness remains configuration- and site-specific [40][42].	Optics-, target- and environment-dependent [41] [42]	Field of view, occlusion, weather, illumination/thermal contrast and compute	Data-protection and AI Act assessment depends on use and captured data
Acoustic	Research and commercial configurations exist; representative public-space validation remains limited.	Noise-, signature- and configuration-dependent [3] [4]	Ambient noise, wind, reverberation, attenuation and signature change	GDPR/LED/national-law assessment if personal data are processed

4.2.1 - READINESS EVIDENCE AND INTERPRETATION

Commercial radar, passive-RF, EO/IR and acoustic products demonstrate that their underlying technologies have moved beyond laboratory concepts. This does not justify assigning a single TRL to a modality. A formal TRL claim should identify the exact sensor, software, integration, operating concept, target set and environment that were validated.

The DTBird® material in Table 9 is a related-party public field evaluation using an avian-mimic drone under stated conditions. It illustrates transparent reporting of distance-dependent detectability but does not independently validate threat-representative UAV detection for LEA sites. Four limitations stated in the source must be carried with the figures. The trial was conducted in a single afternoon session at one site under dry, clear and effectively windless conditions, so it does not sample degraded optical conditions. The number of valid detections per model is small (n = 14 for F4, 18 for A6, 47 for A4 and 55 for F6). The source reports no statistically significant difference between camera models (Kruskal–Wallis $\chi^2 = 7.72$, $p = 0.052$; pairwise Wilcoxon $p > 0.05$), so Table 9 must not be read as ranking the models. The two distance columns are also different quantities and must not be read against each other: the median describes the maximum distance recorded at each detection event, computed over detected events only, whereas the ≥ 90% figure is a threshold read from a generalised additive model fitted to theoretical flights, using the mean distance during each flight as the predictor and all such flights, detected or not, as the sample [34]. That is why the ≥ 90% threshold exceeds the median for three of the four models, and it is why neither column should be quoted as a single operating range. The reference object has a 1.42 m wingspan, several times larger than the small non-cooperative UAVs of concern to LEAs; Table 10 applies the source's own wingspan-scaling method to that difference.

5 - IMPACT ON FCT R&I LANDSCAPE

5.1 - OPERATIONAL REQUIREMENTS AND DEPLOYMENT FEASIBILITY

This study identifies several operational challenges and research priorities that are expected to shape future research and innovation (R&I) activities within the Fight against Crime and Terrorism (FCT) domain. For Law Enforcement Agencies (LEAs), protecting critical infrastructure and public spaces against UAV-related threats will increasingly depend on the effective integration of complementary sensing technologies, supported by artificial intelligence and interoperable command-and-control architectures.

For LEAs, the primary operational requirements are to achieve sufficient early warning while maintaining a low false alarm rate. Detection systems must provide enough reaction time to support legal, tactical and operational decision-making without overwhelming operators with irrelevant alerts. Consequently, detection performance cannot be evaluated solely in terms of maximum range but also in terms of reliability, scalability and ease of deployment.

Range becomes an operational requirement only once it is converted into time, and the figures used in this report give three regimes. At a visible-band perimeter with a detection radius of roughly 40 m against a 0.35 m target (Table 10), a platform transiting at 15 m/s is exposed for under three seconds, which supports alerting, cueing and evidence capture but not interdiction. Against a fast first-person-view platform transiting at some 35 m/s, the same radius yields under two seconds, which is below any useful decision time; that class is therefore addressed by a different geometry rather than by a perimeter (Section 3.7). Giving the same platform an exposure of the order of six to ten seconds, still not interdiction, but enough to halt an event, close an access point, move people away and cue a PTZ onto the track, would require several nodes deployed in depth along a constrained approach corridor, with a per-node detection distance that this report does not quantify; establishing it is part of the comparative trials recommended in Section 6. The perimeter figures above are geometric consequences of the stated detection radii and transit speeds, not measured response times.

Each sensing technology offers distinct operational capabilities. Radar remains one of the principal technologies for wide-area surveillance because it provides continuous spatial tracking and is largely independent of lighting conditions. However, its effectiveness against small UAVs with low radar cross-section (RCS) is reduced, particularly under adverse weather conditions where heavy precipitation may degrade detection performance [7].

RF detection can provide passive stand-off coverage and, in some configurations, support location of the UAV or its Ground Control Station. Achievable range varies with emissions, protocol, antenna placement, environment and configuration, so no universal range is inferred from vendor specifications [11][26]. DRI can assist where a broadcast is legally required and present, but the obligation is not universal and does not cover non-cooperative RF-silent targets [17][18].

Acoustic sensors provide complementary short-range coverage and may compensate for radar and RF blind spots, particularly against non-cooperative UAVs. Their operational performance remains strongly dependent on environmental noise and deployment conditions [2][4][12], making them more suitable as supporting sensors than as standalone solutions in perimeter geometry.

EO/IR sensors can provide search, initial detection, tracking, classification and evidence collection. At a bounded site with favourable coverage, a fixed wide-field camera plus an internally cued PTZ can complete the detection chain without radar, RF or acoustic cueing [40]. Completing the chain is not the same as meeting the requirement: operational acceptance still depends on optics, weather, target size, background, line of sight, warning-time requirements and representative end-to-end testing [11][41][42].

Multimodal sensor fusion is the direction set at EU policy level and, as set out in Section 3.7, the complementarity between modalities follows from the coverage analysis rather than from preference. What the evidence does not support is treating fusion as a precondition before any non-RF capability can be fielded: where cost or complexity places a layered architecture out of reach, a narrower optical or acoustic deployment remains a defensible partial capability for a bounded site. Recent research reports results using multimodal AI architectures that combine radar, acoustic and optical information under defined experimental conditions [5][7][38]. These results cannot yet be treated as representative of continuous operational deployments, but they illustrate the potential of fusion to improve resilience and situational awareness.

Equally important is interoperability. Future C-UAS platforms should integrate heterogeneous information sources—including sensor data, SIGINT, video feeds and operator inputs—within common command-and-control environments that provide a unified operational picture. Open and modular system architectures facilitate the gradual incorporation of new sensors and AI capabilities without requiring complete system redesigns, thereby improving scalability, long-term sustainability and adaptability to emerging threats [38]. A real-world example of an adopted open C-UAS architecture standard is SAPIENT, developed by the UK's Defence Science and Technology Laboratory (Dstl) and published as a British Standards Institute standard, which enables interoperability between heterogeneous sensor and effector nodes [39].

From an R&I perspective, several priorities remain insufficiently addressed by current commercial solutions. These include the detection of RF-silent autonomous UAVs, the operational validation of multimodal AI algorithms under real deployment conditions, privacy-preserving integration of optical sensors, trustworthy and explainable AI for decision support, and standardised interoperability between heterogeneous detection platforms. These areas represent promising research directions for future European projects supporting the development of trustworthy, interoperable and operationally deployable C-UAS technologies for civil security applications.

5.2 - COST AND DEPLOYMENT CONSIDERATIONS

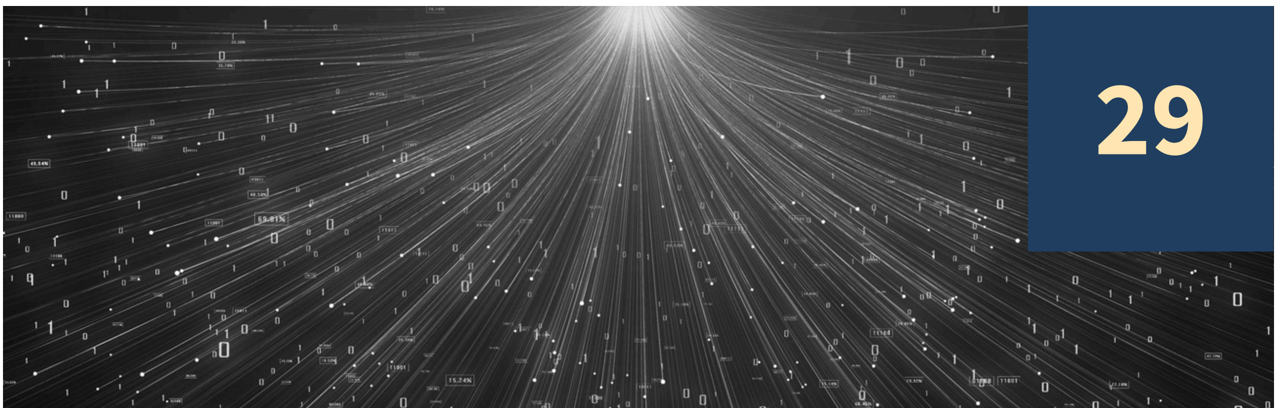
The transition from experimental prototypes to operational C-UAS deployments depends not only on technical performance but also on affordability, life-cycle costs and proportionality. For LEAs, deployment costs must remain compatible with the protection of multiple critical infrastructures and public spaces, making economic sustainability a fundamental design requirement.

Military counter-UAS systems provide useful technological evidence but cannot be directly extrapolated to civilian environments. Their scope, acquisition cost, maintenance and operational concepts may differ substantially. Consequently, this study compares Autonomous Optical and Light Hybrid (Selective Modular) configurations with Heavy Hybrid (Full-Spectrum Layered) alternatives against the capability, deployment and lifecycle requirements of civil-security sites.

To illustrate the budgeting method, the report uses an author-supplied scenario covering an outline of approximately 296,000 m². A layout of ten cameras is adopted solely as an illustrative input to the cost calculation. It was not derived from a documented site survey, three-dimensional occlusion study, lens-by-lens coverage design or field acceptance test, and therefore does not demonstrate that ten cameras provide continuous coverage of that area.

The costed PTZ is a commercially available visible-band unit with a 1/3″ progressive-scan CMOS sensor, 4.7–47 mm optics, a horizontal field of view of 59.1° to 6.5°, 360° continuous pan and 2688 × 1512 native resolution (Table 8) [45]. Table 6 is computed on generic optics rather than on these, and on a pixel count well above what detection requires; it therefore gives a conservative geometric bound rather than a performance prediction for the costed configuration. The achievable radius of the pattern is in any case governed by the fixed wide-field camera that performs the search, which this scenario does not cost.

Table 7 separates the autonomous optical and computing core (€16,650–€21,800; daylight-hours, visible-band configuration) from the optional central-server adaptation (€16,950–€23,600 when included) and the optional passive-RF extension; with the RF module alone the illustrative total is €23,350–€37,500, and with all optional items €23,650–€39,300. These are arithmetic combinations of the stated line items, not supplier quotations or validated deployment costs. At the ten-node layout assumed they give approximately €1,700–€2,200 per node, equipment only; because most of the non-camera items are shared infrastructure, that figure does not scale linearly and is not transferable to layouts of a different size. It is also a lower bound: Table 7 costs ten PTZ units, whereas Autonomous Optical as defined in Section 3.6 pairs each PTZ with a fixed wide-field camera, which the scenario does not quantify and which must be added before the figures are used in procurement.



These values illustrate the stated equipment assumptions for Autonomous Optical and an RF-extended Light Hybrid configuration. However, actual costs depend on site characteristics, infrastructure, sensor density, integration, communications, operator training, preventive maintenance, controlled software and model updates, performance-drift monitoring and other operational requirements.

The illustrative scenario allows the autonomous optical core and its optional extensions to be costed separately. It does not demonstrate coverage or establish that either the all-optical or RF-extended configuration is generally optimal. Future FCT R&I should compare these and other architectures using the same threat scenarios, performance metrics, lifecycle costs and legal constraints.

5.3 - ALIGNMENT WITH EUROPEAN RESEARCH AND INNOVATION PRIORITIES FOR CIVIL SECURITY

The research priorities identified throughout this analysis are broadly consistent with the strategic objectives reflected in Horizon Europe Cluster 3: Civil Security for Society and the European Commission's Horizon Europe Strategic Plan 2025–2027. These initiatives emphasise the development of trustworthy artificial intelligence, resilient critical infrastructure, interoperable security systems and innovative technologies capable of supporting public authorities while respecting European legal and ethical principles [35][36].

The growing complexity of UAV threats, particularly those posed by autonomous and RF-silent platforms, reinforces the need for multidisciplinary research combining sensing technologies, artificial intelligence, cybersecurity and operational validation. Future research should therefore focus not only on improving the performance of individual sensors but also on developing integrated C-UAS architectures capable of combining heterogeneous information sources within interoperable command-and-control environments.

The analysis also supports ongoing European efforts to promote trustworthy and human-centric AI. Rather than replacing human operators, AI should provide transparent and explainable decision support, facilitating threat assessment while maintaining meaningful human oversight in accordance with the European regulatory framework established by the AI Act [21].

Another priority emerging from this study concerns interoperability and standardisation. Future C-UAS solutions should adopt open and modular architectures capable of integrating sensors, software components and AI models from different manufacturers. Such approaches would facilitate technology upgrades, reduce long-term costs and minimise vendor dependency while supporting the gradual incorporation of emerging sensing technologies.

Finally, the transition from research to operational deployment will require continued collaboration between research organisations, industry, public authorities and Law Enforcement Agencies. Common testing methodologies, shared evaluation datasets and operational validation under representative deployment conditions will play an important role in accelerating technology adoption while ensuring compliance with European legal, ethical and operational requirements [37].

6 - RECOMMENDATIONS

This section consolidates the recommendations developed across the report into a single implementation agenda. Actions are grouped below by the body that would own them; horizons run from publication of this report and should be adjusted to the governance cycle of the responsible body.

6.1 - EVIDENCE AND TEST METHODOLOGY

Table 3a: Evidence and test methodology

Priority	Action and lead owner	Horizon	Success criterion	Dependency
Critical	ENACT/JRC with LEA users: extend the existing CWA 18150 counter-UAS test methodology [29] with a scenario stratum for RF-silent targets, feeding the Commission Recommendation on voluntary performance requirements (Q4 2026) and the EU counter-drone centre of excellence (Q1 2027) [37].	0-12 months	RF-silent stratum adopted into the CWA 18150 revision, defining targets, weather/clutter strata, Pd, false alarms, latency and track continuity.	CWA 18150 baseline; LEA scenarios; safe test sites
Critical	Test centres and R&I funders: measure detection distance for thermal and acoustic sensing against threat-representative small UAVs, to the reporting standard of Table 9.	12-24 months	Distance-resolved detection probability published for both modalities under stated conditions, with sample sizes and uncertainty reported.	Instrumented ranges; GPS ground truth; common protocol
High	EU R&I funders: run comparative trials of affordable autonomous wide-field-plus-PTZ optical, radar-plus-optical and RF-plus-optical configurations.	12-24 months	Comparable public results and lifecycle costs from at least three representative site types.	Funding; vendors; public datasets
High	Research community: quantify the transit and dwell asymmetries for defined site geometries and sensor mixes, including the per-node acoustic detection distance that a fast-approach corridor requires.	12-24 months	Cumulative detection probability modelled and measured for at least one channelled approach corridor.	Thermal/ acoustic range data; site access
Medium	Research community: operational validation of multimodal AI fusion and of privacy-preserving optical processing under representative deployment conditions.	24 months +	Results reported with false alarms per hour in continuous operation, not dataset metrics alone.	Shared datasets; test infrastructure

6.2 - PROCUREMENT

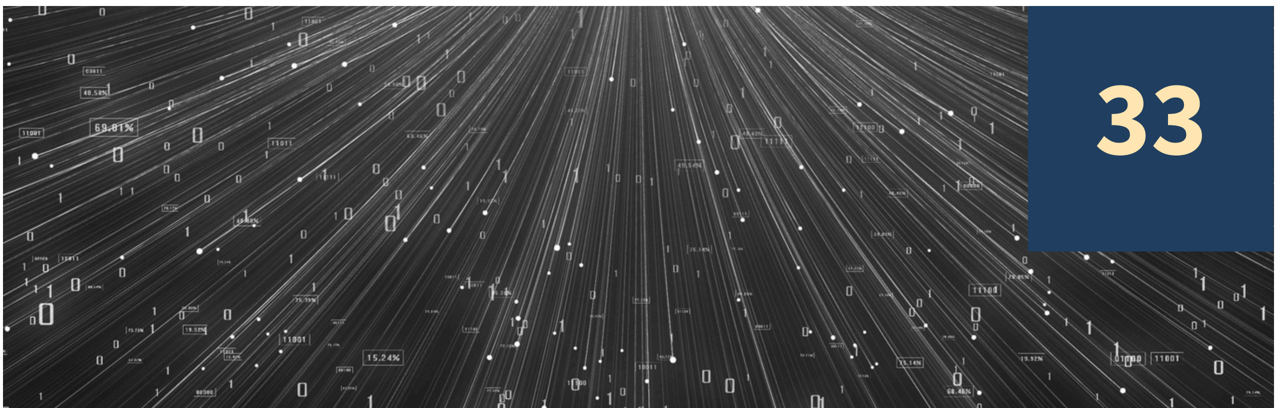
Table 3b:Procurement

Priority	Action and lead owner	Horizon	Success criterion	Dependency
High	National procurement authorities and LEAs: specify acceptance evidence as probability of detection, false alarms per unit time, track continuity, localisation error, classification performance, latency, availability and operator workload under representative weather, clutter and target conditions [42][44].	Next procurement	Every tender contains measurable thresholds, test data and an acceptance plan.	Common protocol; lawful test authority
High	National procurement authorities and LEAs: require configuration-level evidence; a TRL claim must identify the sensor, software, integration, operating concept, target set and environment that were validated.	Next procurement	No modality-level maturity claim accepted as evidence of deployment readiness.	Common protocol; independent test capacity
Medium	Procurement authorities: treat precise localisation and ranging as a performance requirement separate from detection, and require fusion quality, calibration, time synchronisation and correlated environmental failures to be tested on the complete configuration.	Next procurement	Separate, individually verifiable requirements stated in the specification.	Acceptance plan; representative test set
Medium	Procurement authorities: cost complete configurations on equivalent scope and lifecycle terms; equipment allowances are lower bounds and exclude site survey, civil works, integration, communications, training and maintenance.	Next procurement	Award decisions based on lifecycle cost of complete configurations, not equipment price.	Lifecycle cost model; supplier disclosure

6.3 - DEPLOYMENT AND COMPLIANCE

Table 3c: Deployment and compliance

Priority	Action and lead owner	Horizon	Success criterion	Dependency
Medium	Deploying authorities and DPO/legal teams: complete purpose-specific legal and rights assessments before pilot or use, planning for a FRIA where the system is high-risk.	Before pilot/use	Documented legal basis, necessity, data flows, retention, oversight and applicable DPIA/FRIA decision.	Defined purpose, controller and configuration
Medium	Deploying authorities: apply data minimisation, restricted retention, edge processing and access control; confirm national obligations against the consolidated texts in force.	Before pilot/use	Safeguards implemented, auditable and documented.	Legal assessment; national law review
Medium	Deploying authorities and suppliers: establish operator-training, preventive-maintenance, controlled software/model-update and performance-drift monitoring plans.	Before operational acceptance; ongoing	Named responsibilities, training records, maintenance intervals, update controls and periodic re-testing against baseline metrics.	Configuration baseline; support arrangements
Medium	Standards bodies, vendors and public buyers: implement secure, documented sensor interfaces with version traceability, and open modular architectures such as SAPIENT [39].	12-24 months	Interoperability test passed with two vendors; authenticated messages and version traceability.	Interface profile; cybersecurity controls



7 - CONCLUSION

This report has examined the operational, technical, economic and regulatory feasibility of UAV-detection technologies for LEAs, with particular attention to RF-silent autonomous and fibre-linked targets. RF silence creates a specific blind spot for passive RF detection; it does not make a target invisible to active radar, EO/IR or acoustic sensing. Each of those modalities remains subject to different physical, environmental and operational constraints, and none is exempt from being assessed in the configuration and at the site where it will be used.

We claim that sufficiency is not a property of a sensing modality. No modality is universally sufficient in RF-silent conditions, and whether a given detection distance is adequate is settled by deployment geometry and by the comparator rather than by the sensor. In barrier-coverage terms [47], what a low-cost non-RF field can be designed to deliver is weak, probabilistic coverage of constrained approach corridors, exploiting the transit and dwell asymmetries described in Section 3; what it cannot deliver is strong coverage of an airspace volume. What that is worth then depends on the site. Where the realistic alternative for a resource-constrained operator is no detection capability at all, such a field is a proportionate partial capability whose value lies in raising the cost, the risk and the sophistication an incursion requires. At designated critical infrastructure, where EU policy calls for multi-sensor architectures integrated through command-and-control software [37], the same field is a complement that must justify what it adds to a layered architecture rather than what it costs less than.

Within that frame the modalities answer different failure modes rather than competing for a single role. Active radar observes non-emitting targets over a wider area but degrades against small radar cross-sections at low altitude and in clutter. Passive acoustic sensing depends on neither emission nor illumination nor optical line of sight, which makes it the candidate for channelled approach corridors and for targets outside optical view, at short range and subject to ambient noise. Thermal imaging addresses the darkness in which a visible-band chain fails, at several times the unit cost of a visible-band PTZ. Passive RF retains its value wherever a detectable emission exists, a case this report's threat model excludes but real deployments will encounter. A tiered layout follows from that division rather than from preference: visible nodes for corridor coverage, thermal on the approach axes where night and adverse-weather performance decides the outcome, and acoustic where terrain channels the approach.

Autonomous Optical, a fixed wide-field camera plus an internally cued PTZ, is accordingly the component whose capability is bounded quantitatively, and the bound is target size: indicative camera-only median detection runs from approximately 32–41 m for a 0.35 m platform to 130–164 m for the 1.42 m object measured (Table 10). Radii of that order give a few seconds of exposure, which places the pattern at alerting, cueing and evidence capture rather than interdiction. It can therefore carry the detection chain unaided only where a site's geometry, visibility and warning-time requirements make such a radius sufficient, and only where acceptance testing has demonstrated that it does [40].

The technologies to detect RF-silent UAVs exist. Radar, electro-optical and infrared imaging and acoustic sensing all observe targets that emit nothing, and this report has set out what each can and cannot do: the ranges they reach, the conditions that degrade them, the regulatory burden they carry and the cost at which they come. Those limits are not obstacles to deployment but the inputs to it. What follows from them is that a protected site cannot be equipped from a catalogue. The smallest target that must be detected bounds the achievable radius; the approach geometry determines whether that radius is sufficient; the operating environment — illumination, noise, clutter, line of sight — determines which modalities remain effective there; and the capability the operator would otherwise have sets the standard the deployment must beat. A combination that answers those four questions, and is then tested at the site and in the arrangement in which it will be used, can be defended. One selected by modality, or by specification sheet, cannot. That is the practical contribution of this report: not a recommended architecture, but the terms on which a proportionate one can be assembled and verified.

8 - REFERENCES

[1] Yu, A., Kolotylo, I., Hashim, H. A., & Eltoukhy, A. E. E. (2025). Electronic warfare cyberattacks, countermeasures, and modern defensive strategies of UAV avionics: A survey. IEEE Access, 13, 68660–68681. https://doi.org/10.1109/ACCESS.2025.3561068

[2] Guvenc, I., Koohifar, F., Singh, S., Sichitiu, M. L., & Matolak, D. (2018). Detection, tracking, and interdiction for amateur drones. IEEE Communications Magazine, 56(4), 75–81. https://doi.org/10.1109/MCOM.2018.1700455

[3] Kang, C., Huang, Q., Sun, F., Liang, X., & Xu, L. (2025). From classical approaches to recent advancements: A holistic review of acoustic detection for unmanned aerial vehicles. AIP Advances, 15(12), Article 120701. https://doi.org/10.1063/5.0304975

[4] Ghenescu, M. T., Ghenescu, V., & Carata, S. V. (2026). Acoustic Source Drone Detection System Using Tetrahedral Microphone Array and Deep Neural Networks. Sensors, 26(6), Article 1778. https://doi.org/10.3390/s26061778

[5] Alla, I., Olou, H. B., Loscri, V., & Levorato, M. (2024). From sound to sight: Audio-visual fusion and deep learning for UAV detection. In Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '24) (pp. 123–133). ACM. https://doi.org/10.1145/3643833.3656133

[6] Wang, G., Jiang, Q., Jin, X., Wozniak, M., Wang, P., & Yao, S. (2024). RTM-UAVDet: A real-time multimodal UAV detector. IEEE Transactions on Aerospace and Electronic Systems, 61(1), 473–489. https://doi.org/10.1109/TAES.2024.3446460

[7] Larrat, M., & Sales, C. (2026). A Multimodal Transformer Approach for UAV Detection and Aerial Object Recognition Using Radar, Audio, and Video Data. ACM Transactions on Cyber-Physical Systems, 10(3), 1–21. https://doi.org/10.1145/3807778

[8] Parihar, R. S. (2026). An overview of anti-drone systems: Technologies, challenges, and future directions. Journal of Transportation Security, 19, Article 23. https://doi.org/10.1007/s12198-026-00334-1

[9] Xiao, W., Gao, F., & Hu, E. (2025). Signal Processing in Counter-UAS: An SDR-Based Spectrum Localization Analysis and Jamming Noise Generation System. In Proceedings of the 2025 2nd International Conference on Virtual Reality, Image and Signal Processing (VRISP '25). ACM. https://doi.org/10.1145/3772128.3772161

[10] Shi, Y., Shan, T., & Dong, H. (2026). Integrated detection of weak drone signals: From parameter estimation to sensitive classification. Digital Signal Processing, 168, Article 105524. https://doi.org/10.1016/j.dsp.2025.105524

[11] Besada, J. A., Campaña, I., Carramiñana, D., Bergesio, L., & de Miguel, G. (2022). Review and simulation of counter-UAS sensors for unmanned traffic management. Sensors, 22(1), Article 189. https://doi.org/10.3390/s22010189

[12] Ezuma, M., Erden, F., Anjinappa, C. K., Ozdemir, O., & Guvenc, I. (2020). Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference. IEEE Open Journal of the Communications Society, 1, 60–76. https://doi.org/10.1109/OJCOMS.2019.2955889

[13] Fu, Y., Zhang, C., & He, Z. (2026). Radio-Frequency-Based Drone Recognition via Variational Mode Decomposition and Multi-Domain Feature Fusion. Drones, 10(2), Article 124. https://doi.org/10.3390/drones10020124

[14] Al-Emadi, S., Al-Ali, A., Mohammad, A., & Al-Ali, A. (2019). Audio based UAV detection and identification using deep learning. In 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 459–464). IEEE. https://doi.org/10.1109/IWCMC.2019.8766732

[15] Congressional Budget Office. (2026, July 9). Options to counter small unmanned aircraft systems. https://www.cbo.gov/publication/62262

[16] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[17] European Commission. (2019). Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft. Official Journal of the European Union, L 152, 45-71. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0947

[18] Royal Decree 517/2024, of 4 June, approving the Regulation on the use of unmanned aircraft systems (UAS) and adopting implementing measures for Commission Implementing Regulation (EU) 2019/947. Boletín Oficial del Estado, (136), 65362-65436. https://www.boe.es/buscar/doc.php?id=BOE-A-2024-11377

[19] Organic Law 3/2018, of 5 December, on Personal Data Protection and Guarantee of Digital Rights. Boletín Oficial del Estado, (294), 119788-119857. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[20] Joint Research Centre (JRC). (n.d.). Drones, counter drones and autonomous systems: the Counter-UAS "living lab" at the JRC Geel site (Belgium). European Commission. https://joint-research-centre.ec.europa.eu/projects-and-activities/drones-counter-drones-and-autonomous-systems_en

[21] European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, 1–144. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[22] Putrenko, V., & Pashynska, N. (2024). Military situation awareness: Ukrainian experience. Applied Cybersecurity & Internet Governance, 3(1), 121-141. https://doi.org/10.60097/ACIG/190341

[23] Bondar, K (2025, May). How Ukraine's War is Reshaping C4ISR for the Modern Battlefield. Hague Centre for Strategic Studies(HCSS). https://hcss.nl/wp-content/uploads/2025/05/02-Kate-Bondar-How-Ukraines-War-is-Reshaping-C4ISR-for-the-Modern-Battlefield-Final-v5.pdf

[24] NATO Allied Command Transformation. (2025). Request for Innovative Participation — Innovation Challenge 2025/June: Countering fiber-optic-controlled FPV drones (RFIP-ACT-SACT-25-48). Headquarters Supreme Allied Commander Transformation. https://www.act.nato.int/wp-content/uploads/2025/05/rfip025048.pdf

[25] NATO Allied Command Transformation. (2025, 24 June). Frontline innovation: NATO's 16th Innovation Challenge counters fibre-optic controlled drone threats. https://www.act.nato.int/article/innovation-challenge-fibre-optic-drones/

[26] Aaronia AG. (n.d.). AARTOS DDS: World's most successful UAV detection system (Data Sheet & Technical Specifications). https://aaronia.com/en/solutions/drone-detection.

[27] Elta Systems. (n.d.). ELI-4030 Drone Guard: Integrated multi-sensor C-UAS system (Product Brochure). Israel Aerospace Industries (IAI). https://www.iai.co.il/p/eli-4030-drone-guard

[28] International Electrotechnical Commission. (2025). Video surveillance systems for use in security applications—Part 4: Application guidelines (IEC 62676-4:2025). https://webstore.iec.ch/en/publication/83425

[29] COURAGEOUS. (2024). Building a common understanding of the effectiveness of counter-UAS solutions [EU-funded project]. Outputs include CEN Workshop Agreement CWA 18150, Counter-UAS testing methodology. European Commission / INTERPOL. https://www.interpol.int/How-we-work/Innovation/Projects/Project-Courageous

[30] Advanced Protection Systems. (n.d.). SkyCtrl: Multi-sensor counter-drone system. Retrieved 22 July 2026, from https://apsystems.tech/en/

[31] Kustra, M., & Nowakowski, H. (2020). Countering unmanned aerial vehicles in the operational area of airports. Scientific Journal of Silesian University of Technology. Series Transport, 107, 77–87. https://www.researchgate.net/publication/342388951_Counteracting_Unmanned_Aerial_Systems_in_the_Operational_Area_of_Airports

[32] UAS Sentry. (n.d.). Advanced Remote ID sensing and drone detection technology. Retrieved 22 July 2026, from https://www.uassentry.com/

[33] DroneShield. (2024). DroneSentry-C2: Integrated counter-UAS command-and-control software [Product specification sheet]. https://www.droneshield.com/c-uas-products/dronesentry-c2

[34] Liquen Consultoría Ambiental, S.L. / DTBird®. (2025). Evaluation Report on DTBird 2025 Models: Detectability and Detection Range (Rev. 01). https://www.dtbird.com/wp-content/uploads/2025/10/Evaluation-Report-on-DTBird-2025-Models-Detectability-and-Detection-Range.pdf

[35] European Commission. (2024). Horizon Europe strategic plan 2025–2027. https://op.europa.eu/en/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1/language-en

[36] European Commission. (2025). Horizon Europe work programme 2025 – Cluster 3: Civil Security for Society. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en

[37] European Commission. (2026). Action Plan on Drone and Counter-Drone Security. https://digital-strategy.ec.europa.eu/en/library/action-plan-drone-and-counter-drone-security

[38] Arapoglou, F., Zacharia, P., & Papoutsidakis, M. (2025). Intelligent Counter-UAV Threat Detection Using Hierarchical Fuzzy Decision-Making and Sensor Fusion. Sensors, 25(19), Article 6091. https://doi.org/10.3390/s25196091

[39] British Standards Institution. (2024). SAPIENT — Network of autonomous sensors and effectors: Interface control document — Specification (BSI Flex 335 v2.0:2024-03; sponsored by the UK Ministry of Defence, lead technical author Dstl). https://www.gov.uk/government/news/new-milestone-as-bsi-publishes-updated-sapient-standard

[40] Unlu, E., Zenou, E., Riviere, N., & Dupouy, P.-E. (2019). Deep learning-based strategies for the detection and tracking of drones using several cameras. IPSJ Transactions on Computer Vision and Applications, 11, Article 7. https://doi.org/10.1186/s41074-019-0059-x

[41] Birch, G. C., & Woo, B. L. (2017). Counter unmanned aerial systems testing: Evaluation of VIS SWIR MWIR and LWIR passive imagers (SAND2017-0921). Sandia National Laboratories / U.S. Department of Energy. https://www.osti.gov/servlets/purl/1342469

[42] Poppinga, G., Anderson, D., & Amendola, D. (2025). Technical developments in counter-drone technology: C-UAS detection, tracking and identification technology—Annual report (JRC140692). Publications Office of the European Union. https://doi.org/10.2760/1517220

[43] Grieco, G., Amendola, D., & Anderson, D. (2024). Counter-drone systems and data fusion (JRC139587). Publications Office of the European Union. https://doi.org/10.2760/6037951

[44] De Cubber, G., Doroftei, D., Petsioti, P., Koniaris, A., Brewczyński, K., Życzkowski, M., Roman, R., Sima, S., Mohamoud, A., van de Pol, J., et al. (2025). Standardized evaluation of counter-drone systems: Methods, technologies, and performance metrics. Drones, 9(5), Article 354. https://doi.org/10.3390/drones9050354

[45] Axis Communications. (2025). AXIS M5526-E PTZ camera [Datasheet, T10194184/EN/M9.2/202504]. https://www.axis.com/dam/public/e6/f0/d1/datasheet-axis-m5526-e-ptz-camera-en-US-480995.pdf

[46] European Commission. (2019). Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. Official Journal of the European Union, L 152, 1-40. https://eur-lex.europa.eu/eli/reg_del/2019/945/oj

[47] Kumar, S., Lai, T. H., & Arora, A. (2007). Barrier coverage with wireless sensors. Wireless Networks, 13(6), 817-834. (Earlier version: Proceedings of MobiCom ’05, 284-298.) https://doi.org/10.1007/s11276-006-9856-0

[48] Tao, D., & Wu, T.-Y. (2015). A survey on barrier coverage problem in directional sensor networks. IEEE Sensors Journal, 15(2), 876-885. https://doi.org/10.1109/JSEN.2014.2310180

[49] Wang, Z., Liao, J., Cao, Q., Qi, H., & Wang, Z. (2014). Achieving k-barrier coverage in hybrid directional sensor networks. IEEE Transactions on Mobile Computing, 13(7), 1443-1455. https://doi.org/10.1109/TMC.2013.118

[50] Darázs, B., Bukovinszki, M., Kósa, B., Remeli, V., & Tihanyi, V. (2024). Comparison of barrier surveillance algorithms for directional sensors and UAVs. Sensors, 24(14), Article 4490. https://doi.org/10.3390/s24144490

[51] Si, P., Wu, C., Zhang, Y., Jia, Z., Ji, P., & Chu, H. (2017). Barrier coverage for 3D camera sensor networks. Sensors, 17(8), Article 1771. https://doi.org/10.3390/s17081771

[52] CEN Workshop Agreement (CWA) 18150:2024. Unmanned aircraft systems — Counter UAS — Testing methodology. CEN, October 2024. https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa-18150.pdf

9 - ANNEXES

ANNEX A — SUPPLEMENTARY TABLES AND DEPLOYMENT SCENARIO

Table 4: UAV sizes by group

Group	Height (m)	Width/ Wingspan (m)	Classification
G1	0.05	0.15	Nano UAV
G2	0.15	0.4	Micro UAV
G3	0.3	1	Mini UAV
G4	0.8	3	Lightweight UAV
G5	2	10	Tactical UAV
G6	4	20	MALE (Medium Altitude Long Endurance)
G7	6	35	HALE (High Altitude Long Endurance)
G8	> 6.00	> 35.00	UAV strategic or high-altitude

Table 5: Grouping of UAVs by size

Group	Type of UAVs	Classification
G. Small	G1 - G2 - G3	Nano UAV, Micro UAV, Mini UAV
G. Medium	G4 - G5	Lightweight UAV, Tactical UAV
G. Large	G6 - G7 - G8	MALE, HALE, UAV strategic or high-altitude

Table 6: Upper geometric bound on the distance at which a UAV subtends 125 pixels, by size group and camera configuration

Focal Length	Sensor	Vertical resolution (px)	G. small estimate	G. medium estimate	G. large estimate
3 mm	1/3"	1080	1.45 - 9.64 m	28.93 - 96.43 m	192.86 - 337.5 m
9 mm	1/3"	1080	4.34 - 28.93 m	86.79 - 289.29 m	578.57 - 1012.5 m
12 mm	1/3"	1080	5.79 - 38.57 m	115.71 - 385.71 m	771.43 - 1350 m
3 mm	1/1.8"	1080	0.97 - 6.45 m	19.34 - 64.46 m	128.93 - 225.63 m
9 mm	1/1.8"	1080	2.90 - 19.34 m	58.02 - 193.39 m	386.79 - 676.88 m
12 mm	1/1.8"	1080	3.87 - 25.79 m	77.36 - 257.86 m	515.72 - 902.51 m
3 mm	1/2.7"	1080	1.29 - 8.62 m	25.86 - 86.19 m	172.39 - 301.68 m
9 mm	1/2.7"	1080	3.88 - 25.86 m	77.57 - 258.58 m	517.16 - 905.03 m
12 mm	1/2.7"	1080	5.17 - 34.48 m	103.43 - 344.77 m	689.54 - 1206.7 m
3 mm	1/2.8"	1080	1.15 - 7.64 m	22.91 - 76.38 m	152.76 - 267.33 m
9 mm	1/2.8"	1080	3.44 - 22.91 m	68.74 - 229.14 m	458.27 - 801.98 m
12 mm	1/2.8"	1080	4.58 - 30.55 m	91.65 - 305.52 m	611.03 - 1069.31 m

Interpretation note for Table 6. Each value is the distance at which the target subtends 125 pixels, obtained as $D = f \times W \times N_v / (h_s \times N_t)$ with $N_t = 125$, where f is the focal length, W the wingspan of the size group, $N_v = 1080$ the vertical pixel count and h_s the vertical sensor dimension assumed for each format (1/3″: 2.688 mm; 1/1.8″: 4.021 mm; 1/2.7″: 3.007 mm; 1/2.8″: 3.394 mm). Bounding a visual task by a pixel-density threshold follows the approach of the video-surveillance application standard [28]. That standard states its thresholds as densities per metre of scene, whereas the criterion is stated here as a pixel count on the target, because the platforms of concern are sub-metre and a per-metre density does not constrain a sub-metre object usefully. One hundred and twenty-five pixels across the target is a demanding requirement, well above the count at which a detector can register presence, so the distances given are correspondingly shorter than a detection-grade bound would yield.

The figures are upper bounds in three further respects. The wingspan is the largest dimension a UAV can present, so a target observed head-on resolves at a shorter distance; the height values of Table 4 are not used. The model carries no term for lens quality and distortion, focus, target contrast and motion, compression, background or detector performance. And the focal lengths, sensor formats and resolution are generic, and do not correspond to the reference camera of Table 8, whose optics (4.7–47 mm) and native resolution (2688 × 1512) differ. Groups G4–G8 fall outside the threat model of this report and are shown for geometric comparison only; for that threat model the governing column is G. small, which places the bound at a few metres to a few tens of metres. Site-specific optical design and representative field testing remain necessary before any figure is used in procurement.

Table 7: Illustrative equipment budget for the autonomous optical core and optional extensions.

	Estimated cost per unit	Estimated cost total
Illustrative AXIS M5526-E reference cameras (10 units)	1.100 € - 1.300 €	11.000 € - 13.000 €
Base server	1.800 € – 2.500 €	1.800 € – 2.500 €
Central server adaptation for processing signals (optional)	300 € - 1.800 €	300 € - 1.800 €
Optional RF receiver compliance, integration and certification allowance (project estimate; not an emission licence)	3.000 € - 8.000 €	3.000 € - 8.000 €
Optional RF receiver hardware (SDR, antenna array, LNA and enclosure)	3.700 € - 7.700 €	3.700 € - 7.700 €
Processor (CPU)	600 € – 900 €	600 € – 900 €
GPU for AI (critical)	1.800 € – 2.800 €	1.800 € – 2.800 €
RAM	250 € – 400 €	250 € – 400 €
Storage	350 € – 550 €	350 € – 550 €
Managed PoE+ switch (Power over Ethernet Plus)	450 € – 850 €	450 € – 850 €
Server network card	100 € – 200 €	100 € – 200 €
Cabling infrastructure	300 € – 600 €	300 € – 600 €
Autonomous optical + compute core (excl. optional items)		16.650 € - 21.800 €
Optical core + optional central-server adaptation		16.950 € - 23.600 €
Optical core + optional RF module (excl. server adaptation)		23.350 € - 37.500 €
Optical core + all optional items		23.650 € - 39.300 €

RF-related amounts are project allowances for receiver hardware, integration, compliance and certification; they are not emission-licence fees. The ten camera units are PTZ elements; the fixed wide-field cameras required by the Autonomous Optical pattern are not costed here. Unit prices are indicative allowances compiled by the authors from published European distributor listings current at the date of this report; they exclude VAT, mounts, midspans and installation hardware, and they are not supplier quotations. Published distributor pricing for the reference camera at the time of writing is of the order of €950 excluding VAT per unit, so the allowance used here carries a margin for mounting hardware and price variation that a site-specific quotation should replace.

Table 8: Specifications of the illustrative AXIS M5526-E PTZ camera (source: official Axis datasheet [45])

Reference camera model	AXIS M5526-E PTZ Camera [45]
Image sensor	1/3" progressive-scan RGB CMOS
Pixel size	1.998 µm
Focal length	4.7–47 mm
Horizontal FoV	59.1°–6.5°
Vertical FoV	35°–3.67°
Pan range	360° endless
Tilt range	0°–90°
Resolution	16:9: 2688x1512 to 320x180 / 3:2: 1920x1280 to 240x160 / 4:3: 1600x1200 to 160x120

Table 9: Field-measured detection distances for a 1.42 m-wingspan avian-mimic reference object, GPS-validated [34]

Camera Model	Median detection distance (m)	Absolute max. detection distance (m)	Distance at >= 90% detectability (m)
DTBird F6	164.36	451.33	274
DTBird A6 (60° lens)	180.64	359.68	197
DTBird F4	132.69	257.35	172
DTBird A4 (60° lens)	129.62	265.41	92

The reference object used in Table 9 is considerably larger than the platforms that dominate the LEA threat model. The source derives estimates for other object sizes by scaling the measured distances linearly with wingspan, and reports those extrapolations in its own appendices. Applying that same method to threat-representative sizes gives the indicative figures in Table 10.

Table 10: Wingspan-scaled indicative distances derived from Table 9 using the linear scaling method applied in the source [34]

Target wingspan / max. dimension	Median (F6)	Median (A4)	Absolute max. (F6)	Distance at ≥ 90% detectability (F6)
0.35 m (consumer quadcopter)	~41 m	~32 m	~111 m	~68 m
0.60 m (small fixed-wing / larger quad)	~69 m	~55 m	~191 m	~116 m
1.00 m (G3 "Mini UAV", Table 4)	~116 m	~91 m	~318 m	~193 m
1.42 m (measured reference object)	164 m	130 m	451 m	274 m

Table 10 estimates how detection distance changes with target size. Scaling the measured 164 m median for a 1.42 m object gives an indicative distance of approximately 40 m for a 0.35 m consumer drone. This is shorter than the source measurement but longer than the values in Table 6 because it states a pixel count on the target well above what detection requires .

These figures suggest that Autonomous Optical is most suitable for compact sites and constrained approach corridors. Using a detection radius of approximately 40 m, each optical node could monitor around 80 m of frontage. Three corridors of about 200 m would therefore require approximately nine nodes, each combining a fixed wide-field camera and a PTZ. This is broadly consistent with the ten PTZs costed in Table 7, although the fixed cameras must also be included. The same layout would not provide continuous coverage of the full 296,000 m² site.

For a fast drone following a channelled approach, passive acoustic nodes could instead be placed in depth along the approach axis. Their practical value would depend on detection range, ambient noise and the availability of suitable locations with power and communications. These factors should be established through the trials proposed in Section 6.

Both examples illustrate limited, corridor-based coverage. They are not final designs and would require site-specific planning and acceptance testing.

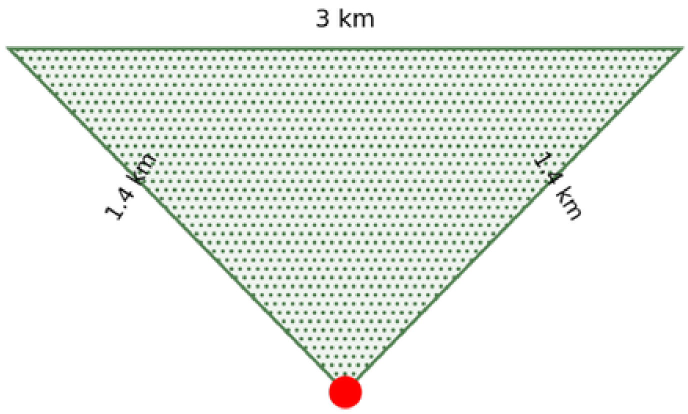


Figure 1: Illustrative outline of the area used for the budgeting scenario (not a validated camera-coverage plan)

ENACT.

European Network Against Crime and Terrorism

@enact-network

enact-eu.net

Scan the QR code to visit ENACT online and read this report in digital format.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.