FLASH REPORT 23

COUNTER-UAS CAPABILITIES IN THE EU: TECHNOLOGIES, PROJECTS AND OPERATIONAL CHALLENGES

Main Authors

Marialuna De Tommaso (ENG)

Filipe Rodrigues (PJ)

André Alegria (PJ)

June 2026

ENACT.
European Network Against Crime and Terrorism

03

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.

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

Funded by the European Union

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.

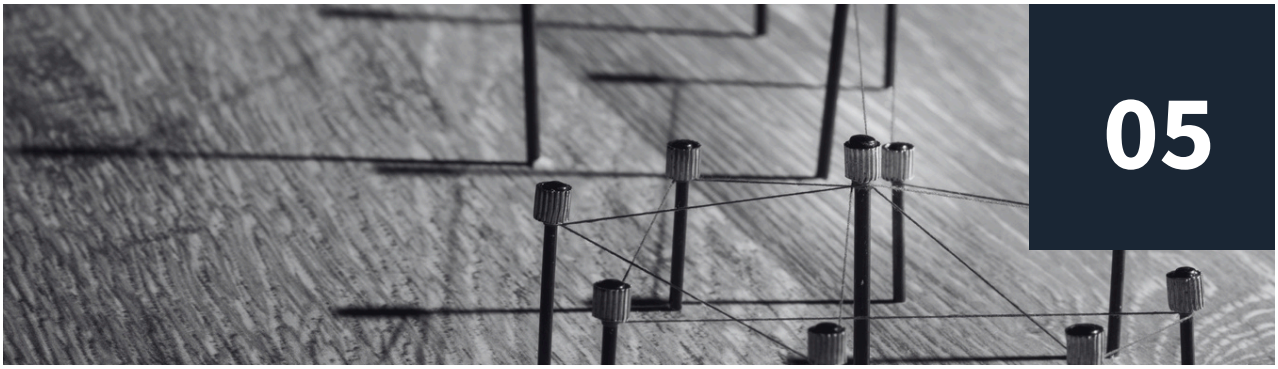
Copyright

Acknowledgement

This report was requested by PRESERVE Protecting euRopean public spaces against Emergent hoStile drone thrEats thRough an adVanced multidimensional shield and cross-border intelligEnce). We are grateful for the request, engagement and feedback throughout the development of the report. PRESERVE brings together 16 partners, including four LEAs, to tackle the so far threat of weaponised recreational/consumer drone swarms through open-source knowledge by non-state actors. https://preserve-he.eu/

Acronyms

AI	Artificial Intelligence
C-UAS	Counter-Unmanned Aircraft Systems
C2	Command and Control
DTI	Detection, Tracking and Identification
EO/IR	Electro-Optical/Infrared
EU	European Union
EU R&I	European Union Research and Innovation
GNSS	Global Navigation Satellite System
H2020	Horizon 2020 Framework Programme
HE/Horizon Europe	Horizon Europe Framework Programme
ISF	Internal Security Fund
JRC	Joint Research Centre of the European Commission
LEAs	Law Enforcement Authorities
RF	Radio Frequency
SOP	Standard Operating Procedure
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle



05

Executive Summary

The rapid proliferation and increasing sophistication of unmanned aerial systems (UAS) are reshaping the European Security landscape and blurring the boundary between Defence and internal Security. While drones provide significant benefits for law enforcement, civil protection, emergency response, border surveillance and critical infrastructure monitoring, their misuse by criminals, terrorist groups, and other non-state actors is creating new operational risks for European Law Enforcement Agencies (LEAs).

In response to this evolving threat environment, counter-UAS (C-UAS) capabilities have become a strategic priority at both the EU and Member State levels. Recent policy initiatives, including the EU Action Plan on Drone and Counter-Drone Security and the broader EU Defence Readiness agenda, reflect the growing recognition that C-UAS is a dual-use capability, requiring stronger synergies between Security and Defence, as well as closer cooperation between public authorities, industry, research organisations and operational end users, including the systematic integration of lessons learned from recent Defence developments and conflicts.

This report analyses the current state of C-UAS capabilities in Europe from a law enforcement and security perspective. It examines the evolving and increasingly complex threat landscape, including emerging challenges such as autonomous, RF-silent and GNSS-denied drone operations, the operational concepts required for C-UAS deployment by LEAs, the main technological layers and deployment models, and the role of EU-funded projects, testing initiatives and cooperation mechanisms in supporting capability development.

The analysis highlights that effective C-UAS capability depends not only on individual technologies but on their integration into a broader operational ecosystem. Detection, tracking, identification, situational awareness, decision-making, mitigation, recovery and forensic exploitation must be supported by clear legal authorisations, standard operating procedures, trained personnel, interoperable command and control (C2) tools and mechanisms for deconfliction with legitimate drone operations.

The report also identifies several persistent capability challenges. These include reliable detection in complex environments, identification and attribution of malicious drone activity, interoperability between systems and agencies, lawful and proportionate mitigation, selective response options, cross-border coordination, and preparedness for emerging threats such as autonomous drones, coordinated operations and RF-silent systems, including recent threats related to fibre-optic FPV drones.

For LEAs and the broader European Security community, C-UAS represents a key capability area for countering crime and terrorism in technologically complex environments. Future efforts should focus on mission-specific concepts of operation, dual-use knowledge exchange between Security and Defence domains, layered and interoperable architectures, realistic testing and validation, clear legal frameworks, and the translation of research outcomes into deployable capabilities for LEAs and Security practitioners.

06

07

Evolving threat landscape and dual-use strategic context

The increasing availability and technological advancement of UAS are contributing to a rapidly evolving threat landscape in Europe, with implications for both internal Security and Defence domains. Drones have evolved from relatively simple remotely piloted platforms into increasingly capable systems that can support autonomous navigation, real-time data processing, coordinated operations and, in some cases, weaponisation. At the same time, their decreasing cost, commercial availability and ease of modification have lowered the barriers for malicious use by criminals, terrorist groups and other non-state actors.[1]

This evolution creates a dual-use challenge. On one hand, drones provide substantial benefits for LEAs, civil protection, border surveillance, emergency response, search and rescue, reconnaissance and real-time situational awareness. On the other hand, the same technological characteristics that make drones attractive for legitimate users, namely affordability, mobility, persistence, precision, rapid deployment and reduced risk to human operators, also make them suitable tools for hostile surveillance, smuggling, disruption, intimidation or attack. As a result, C-UAS capabilities can no longer be understood only as a Defence requirement since they are becoming a core component of public security, critical infrastructure protection and law enforcement preparedness.[1,2]

This dual-use dimension is increasingly recognised at the EU level. The European Commission's **Action Plan on Drone and Counter-Drone Security** focuses on the civilian internal security dimension, while explicitly complementing work carried out in the Defence domain and reinforcing civil-military synergies.[1] In parallel, the **EU Defence Readiness Roadmap 2030** identifies drones and counter-drone systems as a key capability area for strengthening Europe's strategic autonomy and operational readiness, including through flagship initiatives such as the **European Drone Defence Initiative** and **Eastern Flank Watch**.[2] Together, these initiatives show that C-UAS is becoming a cross-domain capability linking internal Security, Defence readiness, border protection, critical infrastructure protection and crisis response.

Recent conflicts, in particular the war in Ukraine, have accelerated innovation in both UAS and C-UAS technologies and provided important lessons for internal security actors. The extensive use of low-cost FPV drones, one-way attack drones, electronic warfare, GPS spoofing, jamming, autonomous functions and fibre-optic tethered drones demonstrates how rapidly the threat environment can evolve. Some of these developments are already relevant beyond the battlefield.

[1]European Commission (2026), *Action Plan on Drone and Counter-Drone Security*, policy page. Available at: https://digital-strategy.ec.europa.eu/en/policies/drone-security
[2]European Commission / DG DEFIS (2025), *Drones and Counter-Drone Systems,* factsheet. Available at: https://Defence-industry-space.ec.europa.eu/system/files/2025-12/Factsheet-Drones-and-C-UAS.pdf

For example, fibre-optic FPV drones can maintain C2 and video transmission without relying on conventional RF wireless links, reducing their vulnerability to jamming and challenging C-UAS architectures that depend heavily on RF detection or RF-based mitigation.[3] This reinforces the need for layered and adaptable C-UAS approaches combining radar, electro-optical/infrared, acoustic, RF, data fusion and, where legally authorised, selective mitigation or physical interception.

For LEAs, however, the translation of Defence lessons into internal security practice is not straightforward. Military C-UAS operations are often designed for environments where the priority is rapid neutralisation of hostile systems. By contrast, LEA operations usually take place in populated, legally constrained and politically sensitive environments, where proportionality, public safety, privacy, data protection, spectrum management and evidence preservation are central considerations. The presence of legitimate drones, including police, emergency services, media, infrastructure operators or authorised commercial users, further increases the complexity of the response. C-UAS systems must therefore support not only detection and neutralisation, but also discrimination, attribution, deconfliction and legally accountable decision-making.[1,4]

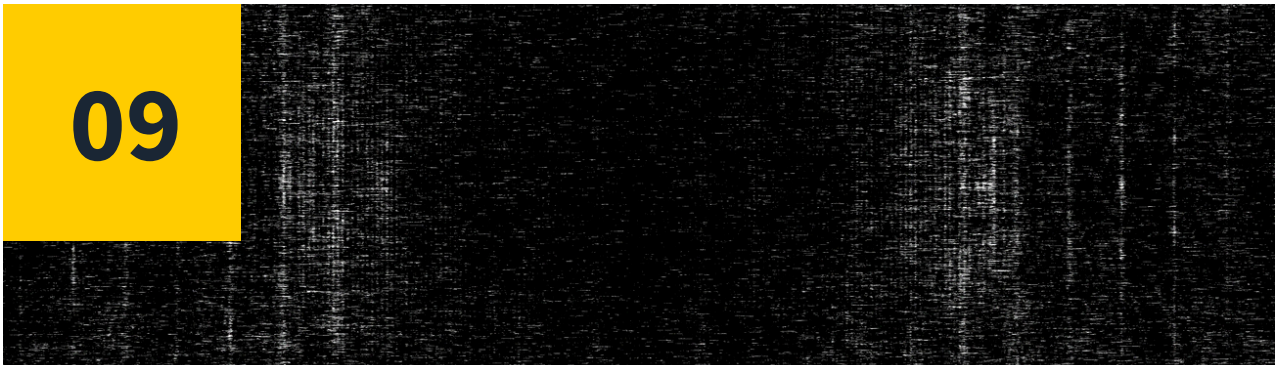
The threat spectrum relevant to European LEAs and related networks such as ENACT is broad. It includes nuisance and unauthorised flights over restricted areas, smuggling into prisons, hostile surveillance of police or border operations, disruption of airports and major public events, reconnaissance against critical infrastructure, trafficking and cross-border illicit activities, and potential terrorist use of drones as delivery or attack platforms. In more complex scenarios, malicious actors may deploy multiple drones simultaneously, use pre-programmed routes, exploit GNSS-denied environments, or combine drones with cyber, electronic or physical actions as part of hybrid threat campaigns.[1,4]

In this context, C-UAS should be approached as an operational ecosystem rather than as a single technology. Effective capability depends on the integration of sensors, C2 tools, standard operating procedures, legal authorisations, inter-agency coordination, training, testing and post-incident exploitation. For LEAs, this means developing concepts of operation that cover the full incident cycle: preparation, detection, tracking, identification, decision-making, mitigation, recovery, forensic exploitation and lessons learned. Such an approach is essential to ensure that counter-drone responses are effective against malicious actors while preserving the ability of law enforcement and emergency services to use drones safely and legitimately.

The development of integrated, AI-enabled and interoperable C-UAS ecosystems is therefore emerging as a critical enabler for European internal security. It can support local operational effectiveness, EU-wide coordination, cross-border information sharing and resilience against technologically advanced threats. At the same time, lessons learned from C-UAS may inform broader future approaches to countering multi-domain unmanned systems, including unmanned ground, surface and underwater vehicles, as these technologies become increasingly relevant for crime, terrorism and hybrid threat scenarios.

[3]U.S. Army / Center for Army Lessons Learned (2025), *Fiber Optic Drones: Posing a Significant C-UAS Challenge*. Available at: https://www.army.mil/article/287737/fiber_optic_drones_posing_a_significant_c_uas_challenge
[4]Europol (2025), *The Unmanned Future(s): The impact of robotics and unmanned systems on law enforcement*. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The-Unmanned-Future-Report.pdf

09



Concepts of Operation for Law Enforcement C-UAS

For LEAs, C-UAS capabilities must be operationalised through an integrated approach that goes beyond individual technological assets. Effective response depends not only on sensors and mitigation tools, but also on risk assessment, C2, legal authorisation, trained personnel, inter-agency coordination and post-incident exploitation. This is particularly relevant in civilian environments, where counter-drone incidents may involve legitimate drone users, privacy and data protection considerations, spectrum management constraints, public safety risks and the need to preserve evidence.[4, 5, 6]

Building on this approach, LEA-oriented concepts of operation should encompass the full incident cycle, including preparation, detection, tracking, identification, decision-making, mitigation, recovery and lessons learned. Preparation includes defining protected areas, assessing drone-related risks, clarifying roles and legal authorities, establishing standard operating procedures and ensuring that operators can act under time pressure. Once an incident occurs, detection and tracking should provide an actionable operational picture, combining information from RF monitoring, radar, electro-optical/infrared sensors, acoustic detection and other relevant sources where available.[7]

Identification and assessment are also critical in law enforcement contexts since, unlike in military environments, civilian airspace may include drones operated by police units, emergency services, media organisations, infrastructure operators or authorised commercial users. C-UAS systems must therefore support discrimination between legitimate, careless, non-compliant and malicious drone activity, integrating technical data with operational information such as flight authorisations, event security plans, intelligence inputs and, where available, remote ID or other identification mechanisms.[4, 7]

Decision-making and mitigation should be guided by proportionality, necessity and operational risk. Possible responses may range from monitoring and attribution to warning, evacuation, selective mitigation, interception or physical neutralisation. In populated areas, immediate neutralisation may not be the safest or most legally appropriate option.

[5]European Commission – Joint Research Centre (2023), *Countering the threat of civil drones: Commission presents new measures*. Available at: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/countering-threat-civil-drones-commission-presents-new-measures-2023-10-19_en

[6]INTERPOL (2020), *Framework for Responding to a Drone Incident – For First Responders and Digital Forensics Practitioners*. Available at: https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf

[7]European Commission – Joint Research Centre (2025), *Technical developments in counter-drone technology: C-UAS detection, tracking and identification technology – Annual report*. Available at: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC140692/JRC140692_01.pdf

RF jamming may interfere with nearby communications, navigation systems or friendly drones, while kinetic options may create risks from falling debris or uncontrolled impacts. This reinforces the need for controlled and selective mitigation, especially when LEA or emergency-service drones are operating in the same airspace.[8]

Post-incident recovery and forensic exploitation are also essential. The drone, payload, controller, media storage, communication logs and associated digital traces may all constitute evidence. C-UAS operations should therefore include procedures for securing the scene, safely handling the drone or debris, preserving digital evidence, documenting the incident and maintaining the chain of custody.[6]

Ultimately, concepts of operation should be tailored to distinct mission profiles that may fall under the security domain. For example, protecting a prison from smuggling drones requires persistent monitoring and rapid attribution; securing a stadium or public event requires coordination with organisers, emergency services and authorised drone operators; protecting critical infrastructure may require fixed 24/7 detection integrated with a security operations centre; and supporting counter-terrorism or border operations may require mobile systems, rapid decision-making and strong coordination between tactical, intelligence and airspace authorities. For LEAs, this framing links C-UAS capability development with broader law enforcement priorities, including **Terrorism and Radicalisation, Organised Crime**, **Public Space Protection**, **Border Security,** and **Resilience of Critical Infrastructure**. Figure 1 below summarises the LEA-oriented C-UAS operational cycle and its main cross-cutting enablers.

Figure 1: LEA-Oriented C-UAS Operational Cycle and Cross-Cutting Enablers

[8]EUROCONTROL (2024), *Presentation: Communication from the Commission on countering potential threats posed by drones*. Available at: https://www.eurocontrol.int/sites/default/files/2024-11/eurocontrol-2024-cuas-workshop-s4-liberatori.pdf

11

C-UAS Technological Framework and Deployment Models

C-UAS technologies have evolved from isolated detection or jamming tools into integrated systems that combine sensing, data fusion, command-and-control (C2), and mitigation capabilities. From an operational perspective, the objective is not only to detect the presence of a drone, but to support a complete response chain: detection, localisation, tracking, classification, identification, assessment and, where legally authorised, mitigation or neutralisation of the threat.[7] This operational chain provides a common reference framework for structuring C-UAS technological components in law enforcement contexts.

Figure 2 provides a schematic overview of the main C-UAS technology layers and deployment models relevant for LEA-oriented operations. It links sensing, situational awareness, mitigation, and enabling functions to fixed, mobile, man-portable, and emerging drone-versus-drone or robotic-carrier concepts.

The detection, tracking and identification phases rely on complementary sensing technologies. Radio frequency (RF) monitoring can detect and analyse communication links between a drone and its controller, and may also support localisation of the operator. Radar can provide wide-area detection and tracking, including against drones that do not emit RF signals. Electro-optical and infrared sensors support visual confirmation, classification and evidence collection, while acoustic sensors may provide additional cues in specific environments. However, each sensor type has limitations related to range, terrain, urban clutter, weather, background noise or electromagnetic interference. For this reason, current C-UAS architectures increasingly rely on multi-sensor fusion rather than on a single detection technology.[7]

Situational awareness and C2 tools are essential for transforming sensor outputs into actionable information. These tools correlate alerts, tracks and visual feeds, support operator decision-making, and help create a common operational picture. In law enforcement contexts, this layer is particularly important because operators must distinguish between legitimate, careless, non-compliant and malicious drone activity, while coordinating with other authorities, emergency services, airspace stakeholders and, in some cases, private infrastructure operators. It also supports the transition from detection and identification to decision-making and response.

Mitigation and neutralisation capabilities are commonly divided into soft-kill and hard-kill measures. Soft-kill measures include non-kinetic techniques such as RF disruption, GNSS interference, protocol manipulation, spoofing or cyber takeover.

Hard-kill measures include physical interception, capture or destruction of the drone. In civilian security contexts, both approaches raise important operational and legal constraints. From a technological perspective, these limitations have direct implications for system design and deployment. RF disruption may affect surrounding communications, navigation systems or authorised drone operations, while kinetic options may introduce safety risks due to falling debris or uncontrolled impacts. As a result, C-UAS solutions for LEA contexts increasingly prioritise selectivity, controllability and the minimisation of collateral effects.[8]

The deployment of C-UAS solutions should be tailored to different mission types and operational requirements. Fixed systems are suitable for permanent or semi-permanent protection of airports, prisons, government buildings, ports, energy facilities and other critical infrastructure. Mobile and deployable systems can support temporary operations such as public events, VIP protection, border deployments or high-risk police operations. Man-portable systems, including anti-drone "gun" concepts, may provide tactical response options for specialised units, but require clear rules of engagement, training and spectrum-management safeguards. Commercial examples, such as Swatter's C-UAS solutions, illustrate the growing market for mobile and deployable systems aimed at defence and security applications, including public security and critical infrastructure protection.[9]

A further trend is the emergence of more selective mitigation approaches. Instead of relying only on broad jamming, some systems aim to target specific communication channels or protocols in order to reduce collateral interference. DroneWall, for example, is presented as a C-UAS system using channel-specific denial-of-service and denial-of-access techniques rather than conventional wide-area radio jamming, with the objective of neutralising hostile drone communications while limiting interference with neighbouring networks.[10] While such systems still require legal authorisation and operational validation, they illustrate an important direction for LEA use cases where friendly drones and public communications may be operating in the same environment.

Emerging C-UAS concepts also include drone-versus-drone interception, net capture systems, autonomous interceptors and robotic platforms carrying C-UAS payloads. These concepts may be particularly relevant where fixed infrastructure is insufficient, where the threat is mobile, or where responders need to operate at a distance from hazardous areas. In the longer term, integration between C-UAS, robotics, AI-enabled perception and common operational picture tools may support more adaptive responses to complex scenarios, including multiple drones, autonomous flight paths and RF-silent threats such as fibre-optic FPV drones.

Overall, the technological framework for LEA C-UAS should be layered, modular and mission-driven. No single technology can address all scenarios. Effective capability depends on combining complementary sensors, interoperable C2 tools, selective mitigation options, trained operators and clear operational procedures. This is especially important for LEA-relevant scenarios where C-UAS must support public security and counter-crime objectives without compromising lawful drone operations, public safety or evidentiary requirements.

[9]Swatter Company (2025), *About – Advanced Defense & Security Solutions*. Available at: https://swattercompany.com/about/

[10]Unival Group (2025), *DroneWall cUAS Counter-UAS System*. Available at: https://unival-group.com/en/products/counter-monitoring/spectrum-monitoring-and-the-unival-approach/unival-spectrum-guard/dronewall-cuas

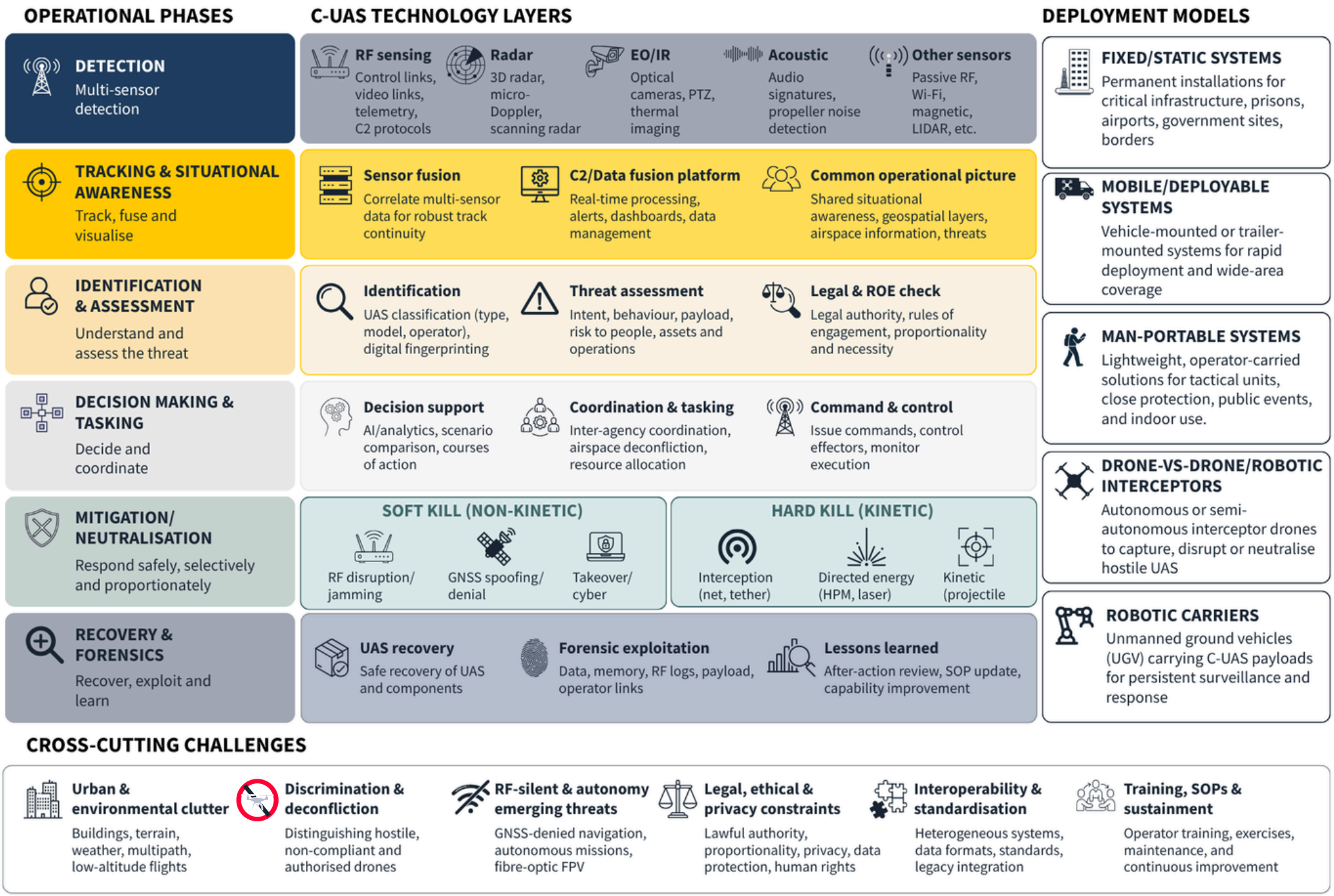


Figure 2: C-UAS Technology Layers and Deployment Models for LEAs

14

EU-Funded Solutions and Policy Initiatives Supporting C-UAS Capabilities

The development of C-UAS capabilities in Europe is supported by a combination of policy initiatives, EU-funded research and innovation projects, testing and standardisation activities, and operational cooperation mechanisms. Together, these elements contribute to strengthening preparedness, enhancing detection and response capabilities, reducing fragmentation across Member States, and fostering closer alignment between technological development and the operational needs of LEAs, security practitioners and critical infrastructure operators. However, their impact ultimately depends on the ability to ensure coherence between technological development, operational needs and deployment constraints in law enforcement contexts.

Within this framework, EU-funded programmes, particularly **Horizon 2020**, **Horizon Europe**, and the **Internal Security Fund**, have played an important role in advancing technological solutions, supporting validation in operationally relevant environments, facilitating uptake by law enforcement authorities, and contributing to deployment in real operational contexts. At the same time, recent policy initiatives have increasingly focused on ensuring that research outputs can be translated into deployable capabilities, supported by common testing methodologies, shared operational frameworks and stronger cooperation between civil, security and defence stakeholders.

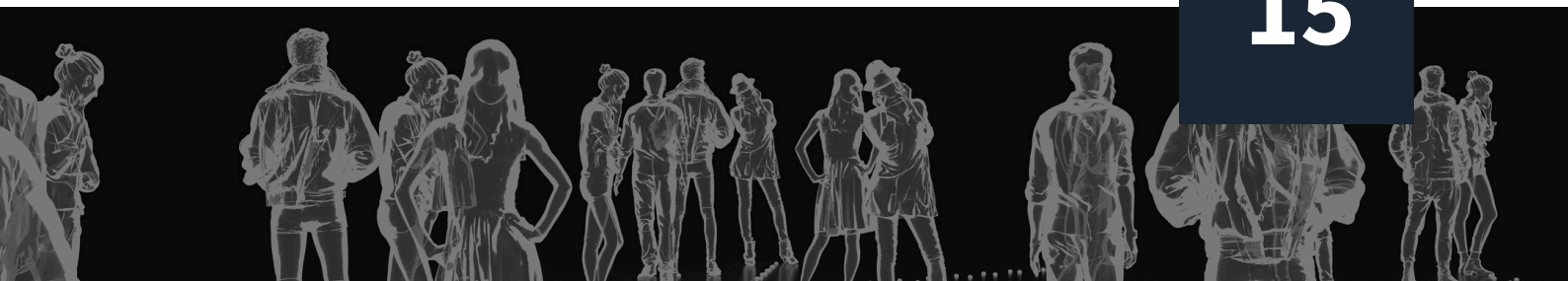
European Research and Policy Initiatives

At the policy level, the European Commission's **Action Plan on Drone and Counter-Drone Security** represents a major milestone towards a more coordinated European response to drone-related security threats. The Action Plan establishes a framework aimed at enhancing preparedness, improving detection capacities, coordinating responses and reinforcing civil-military synergies in the drone and counter-drone domain.[1] It also promotes a more structured European ecosystem for counter-drone technologies, including improved testing infrastructures, coordinated risk assessment and closer cooperation between public authorities, industry, research organisations and defence stakeholders.

This policy direction is complemented by the **EU Defence Readiness Roadmap 2030**, which identifies drones and counter-drone systems as a key capability area for strengthening Europe's strategic autonomy and operational readiness.[2] Although the Roadmap is primarily framed in defence terms, its relevance for internal security is significant.

The same technological developments, supply chains, industrial capabilities and lessons learned from military C-UAS are increasingly relevant for the **Protection of Public Spaces**, **Border Management**, **Resilience of Critical Infrastructure** and high-risk law enforcement operations.

For LEAs, the key implication is that C-UAS should be treated as a dual-use capability. It requires the ability to draw on defence innovation and operational lessons while adapting them to civilian environments, where proportionality, public safety, privacy, data protection, spectrum management and legal authorisation remain decisive factors. This creates a need for EU-level coordination not only in technology development, but also in doctrine, testing, procurement, training and operational interoperability. It also highlights the need to bridge policy ambition with operational implementation, ensuring that EU-level initiatives translate into effective, deployable capabilities for law enforcement authorities.



The EU Portfolio for C-UAS Research: Advancing Counter-Drone Technologies through Horizon Programmes

EU-funded research projects have significantly contributed to the advancement of C-UAS technologies, particularly through the development of integrated systems, multi-sensor architectures, response management tools and validation activities in realistic operational contexts. Over time, these projects show a clear evolution from isolated detection or mitigation components towards more integrated, end-to-end capabilities covering detection, tracking, identification, situational awareness and mitigation.

Within the **Horizon 2020** programme, the **ALADDIN** project focused on the design and validation of a holistic counter-drone solution combining detection, identification and neutralisation capabilities into a unified architecture. The project integrated multiple sensing technologies and advanced data processing approaches, contributing to improved performance in complex operational scenarios.[11]

Similarly, the **DAPS** project explored drone detection and mitigation solutions tailored to urban environments and critical infrastructure. Its relevance lies in addressing the need for scalable protection against unauthorised drones in security-relevant contexts, including environments where rapid deployment and controlled response are required.[12] **KNOX** also contributed to this area by focusing on cost-effective and scalable drone alarm and protection systems, integrating detection and jamming functions for urban and security applications.[13]

In parallel, the **RESPONDRONE** project addressed the management of multi-drone operations and the integration of real-time data for first responders.[14] While not specifically focused on counter-UAS, it provides valuable insights into coordinated drone operations, data fusion and situational awareness. These elements are directly relevant for C-UAS, particularly in scenarios involving multiple drones, complex airspace management, emergency response coordination or swarm-like threat patterns.

More recently, **Horizon Europe** initiatives such as **PRESERVE** have placed stronger emphasis on emerging hostile drone threats in public spaces. PRESERVE focuses on the development of an integrated C-UAS platform combining detection, intelligence analytics, response management and validation in realistic operational contexts, with particular relevance for law enforcement and the **Protection of Public Spaces**.[15] This reflects a broader shift towards solutions that are not only technically advanced, but also aligned with LEA requirements and deployment constraints.

Overall, the EU-funded project landscape demonstrates that C-UAS capability development is increasingly moving towards integrated, modular and operationally validated systems. This evolution is essential for LEA- and security-relevant contexts, where counter-drone capabilities must support public security, counter-terrorism, organised crime response, border security, major event protection and critical infrastructure resilience.

[11]European Commission (CORDIS), *ALADDIN – Advanced hoListic Adverse Drone Detection, Identification Neutralization, Grant Agreement 740859*. Available at: https://cordis.europa.eu/project/id/740859

[12]European Commission (CORDIS), *DAPS – Drone Alarm and Protection System, Grant Agreement 719382.* Available at: *https://cordis.europa.eu/project/id/719382*.

[13]European Commission (CORDIS), *KNOX – Cost advantageous and scalable drone alarm and protection system, Grant Agreement 768242.* Available at: https://cordis.europa.eu/project/id/768242

[14]European Commission (CORDIS), *RESPONDRONE – Novel integrated solution for operating a fleet of drones with multiple synchronized missions, Grant Agreement 833717.* Available at: https://cordis.europa.eu/project/id/833717

[15]European Commission (CORDIS), *PRESERVE – Protecting European public spaces against emergent hostile drone threats, Grant Agreement 101168392.* Available at: https://cordis.europa.eu/project/id/101168392

Testing, Standardisation and Performance Assessment Initiatives

Alongside research and development, increasing attention is being devoted to testing, standardisation and performance evaluation. These activities are critical for ensuring the reliability, comparability and operational usability of C-UAS solutions. In practice, performance may vary significantly depending on the operating environment, drone type, sensor mix, weather conditions, electromagnetic interference, urban clutter and the presence of legitimate airspace users. As a result, laboratory performance alone is insufficient to determine whether a system is suitable for real law enforcement deployment.

The **COURAGEOUS** and **COURAGEOUS²** initiatives, funded through the **Internal Security Fund**, are particularly relevant in this area. They focus on developing standardised testing methodologies and validation frameworks for assessing C-UAS system performance across operational scenarios.[16] By providing structured approaches for evaluating technologies, these initiatives support more informed procurement and deployment decisions by LEAs. They also contribute to building a common understanding of what C-UAS performance means in practice, including detection probability, false alarm rates, tracking continuity, identification reliability, response time and operational safety.

Complementary activities are carried out by the European Commission's Joint Research Centre, which supports technical assessment and experimentation in the field of C-UAS detection, tracking and identification technologies.[7] Such work helps bridge the gap between laboratory testing and operational deployment, while supporting evidence-based policy development and capability planning. This is particularly important given the diversity of available C-UAS solutions and the absence of fully harmonised benchmarks across Member States.

In the Border Management domain, the Frontex C-UAS Prize Contest provides another relevant example of operationally oriented capability assessment. The contest aims to foster innovative solutions to counter unauthorised UAS activity at the EU's external borders and includes live operational trials in a simulated border environment. This is particularly relevant for LEAs and border authorities because it links technical maturity, deployment feasibility and operational needs, including the neutralisation of unauthorised UAS threats such as illicit surveillance and smuggling.[17]

Testing and standardisation also have a strong interoperability dimension. For LEAs, C-UAS systems must often operate alongside existing C2 systems, emergency response platforms, airspace management tools and communication networks. Without common testing approaches, comparable performance metrics and shared operational requirements, there is a risk that Member States procure systems that are technically capable but difficult to integrate, scale or use in cross-border contexts.

[16] COURAGEOUS / COURAGEOUS² (ISF), *Building a common understanding of counter-UAS system performance and testing methodologies.* Available at: https://courageous-isf.eu/
[17] Frontex (2025), *C-UAS Prize Contest.* Available at: https://www.frontex.europa.eu/innovation/research-and-innovation/prize-contests/c-uas-prize-contest-sFXJdl

Cross-Border Cooperation and Information Sharing

In addition to technological and policy advancements, cross-border cooperation and information sharing play a fundamental role in strengthening C-UAS capabilities at the EU level. Drone-related threats may affect multiple jurisdictions, involve mobile or transnational actors, and combine criminal, terrorist or hybrid threat dimensions. This is particularly relevant for border areas, transport networks, ports, airports, critical infrastructure corridors and major international events.

Europol supports Member States through threat analysis, intelligence exchange and coordination activities related to emerging technologies, including unmanned systems. Its work highlights the growing relevance of drones in both legitimate and criminal contexts and underlines the need for LEAs to adapt to a future operating environment shaped by robotics, autonomy, data-driven systems and technological convergence.[4] **Europol**'s recent **Industry and Research Days** events further illustrate the growing relevance of counter-UAS and related unmanned-systems capabilities for law enforcement agencies. The 2025 edition included dedicated attention to robots, drones and other unmanned systems, as well as AI-enabled target detection, identification and tracking, highlighting how such technologies are increasingly linked to situational awareness, operational coordination and **Protection of Public Spaces**. The 2026 edition continued this trajectory, featuring mature, market-ready solutions in situational awareness and uncrewed systems for law enforcement operations, suggesting that C-UAS should be understood as part of a broader shift towards integrated, technology-enabled operational support for policing and security.[18]

At the international level, **INTERPOL** contributes to broader information-sharing frameworks and provides operational guidance for responding to drone incidents, including aspects related to first responders, digital forensics and evidence handling.[6] This is especially important in law enforcement contexts, where the drone, payload, controller, storage media and associated digital traces may constitute evidence for investigation and prosecution.

These cooperation mechanisms are essential for addressing the fragmentation of information and limited coordination that still characterise parts of the current C-UAS landscape. Strengthening cross-border collaboration, shared situational awareness, and common procedures will be necessary to ensure that counter-drone responses are not limited to local technical deployments but form part of a coherent European security ecosystem.

Taken together, these initiatives illustrate a progressive shift towards integrated and operationally validated C-UAS solutions, although challenges remain in ensuring interoperability, scalability and deployment readiness across Member States. To complement the narrative overview presented above, Table 1 provides a structured summary of key EU-funded projects and related initiatives, highlighting their main operational outcomes and the core capabilities they address across the C-UAS value chain.

[18] Alegria, A., & Rodrigues, F. (2026). *ENACT Flash Report 12 - Europol Industry and Research Days (1.0).* European Network against Crime and Terrorism (ENACT). https://doi.org/10.5281/zenodo.18626157

Project/Initiative	Principal operational tool/outcome	Core capability addressed
ALADDIN (H2020)	Integrated counter-UAS system combining multi-sensor detection, including radar, EO/IR and acoustic sensing, AI-based processing and neutralisation tools within a unified architecture.	End-to-end C-UAS capability: detection, identification, tracking and mitigation.
DAPS (H2020 SME)	Scalable drone alarm and protection system enabling detection and RF-based disruption of unauthorised drones in urban and security-relevant environments.	Detection and mitigation, including RF-based countermeasures.
RESPONDRONE (H2020)	Multi-UAS system-of-systems enabling coordinated operation of drone fleets, real-time data integration and decision support for first responders.	Situational awareness, data fusion and multi-drone coordination.
PRESERVE (Horizon Europe)	Integrated multi-layer C-UAS platform combining sensor fusion, intelligence analytics, response management and validation for the protection of public spaces against hostile drone threats.	Integrated C-UAS platform and response management, including complex and coordinated scenarios.
COURAGEOUS/ COURAGEOUS²(ISF)	Standardised testing methodologies and validation framework for assessing the performance of C-UAS solutions across operational scenarios.	Testing, validation, benchmarking and standardisation of C-UAS capabilities.
KNOX (H2020 SME)	Cost-efficient and scalable drone alarm and protection system integrating detection and jamming functions for security applications in urban contexts.	Detection and mitigation for scalable deployment solutions.
JRC experimentation and testing activities (European Commission)	Technical assessment, experimentation and testing support, through living labs, for evaluating C-UAS technologies under controlled and operationally relevant conditions.	Performance validation, benchmarking and evidence-based policy support.

Table 1: Overview of EU-Funded Projects and Initiatives Supporting C-UAS Capabilities

Overall, these initiatives illustrate the progressive evolution of the European C-UAS ecosystem, combining technological innovation, operational validation, standardisation and cooperation mechanisms. Despite these efforts, several capability gaps remain, particularly in relation to interoperability, legal harmonisation, cross-border information sharing, procurement support and the translation of research outcomes into deployable LEA capabilities. Addressing these gaps will be essential to ensure that future European C-UAS solutions are not only technologically mature, but also usable, proportionate and legally deployable in real law enforcement and security contexts. This will be critical to enabling the European C-UAS ecosystem to effectively support operational needs across diverse law enforcement scenarios.

20

Key Capability Challenges and Limitations

Building on the previous analysis, the rapid evolution of C-UAS technologies and the growing number of EU-funded initiatives have not yet fully resolved the operational readiness challenges faced by LEAs. Their ability to counter malicious, coordinated or increasingly autonomous drone threats remains constrained by persistent capability gaps. These gaps are not only technological; they also relate to legal authority, proportionality, interoperability, training, procurement, cross-border coordination and the ability to operate C-UAS tools without disrupting legitimate drone activity. This highlights that the main challenge lies not only in technological performance but in the integration of these capabilities into coherent and operationally usable systems.

A central challenge for law enforcement is that C-UAS operations usually take place in complex civilian environments. Unlike many defence scenarios, LEAs must operate in populated areas, close to critical infrastructure, public events, transport systems and communication networks. They must also distinguish between hostile drones and legitimate UAS operated by police units, emergency services, infrastructure operators, media organisations or authorised commercial users. As a result, future C-UAS capability development must address not only performance against drone threats, but also safety, legal compliance, evidence preservation and operational deconfliction.[4,6]

Detection and Identification: Challenges in Early Warning, Discrimination and RF-Silent Threats

A first structural challenge concerns the ability to reliably detect and identify drones in heterogeneous and high-noise environments. The practical issue is not only detecting an airborne object, but generating actionable early warning and discriminating between authorised, careless, non-compliant and malicious activity in real time. This is particularly difficult around airports, prisons, public events, borders and critical infrastructure, where legitimate drone activity may coexist with hostile or unauthorised operations.

From a technological perspective, no single sensor can provide reliable detection and identification across all operational scenarios. RF monitoring can be effective when drones rely on wireless C2 links, but it may be less useful against autonomous, pre-programmed or RF-silent systems. Radar can provide wide-area detection, but may face limitations in urban environments or against very small, low-flying drones.

EO/IR sensors support visual confirmation and classification, but can be affected by line of sight, weather and lighting conditions. Acoustic sensors may add value in specific environments, but their performance can be limited by background noise.[7]

The emergence of fibre-optic FPV drones and other systems with reduced reliance on RF links reinforces this challenge. Such threats reduce the effectiveness of classical C-UAS approaches that depend primarily on RF detection or RF-based mitigation. This does not mean that RF capabilities lose relevance, but it highlights the need for layered architectures combining radar, EO/IR, acoustic, RF, AI-enabled classification and sensor fusion.[3,7]

A further limitation concerns identification and attribution. In law enforcement contexts, knowing that a drone is present is insufficient. Operators need to assess whether the drone is authorised, whether it carries a payload, whether it is approaching a protected asset and, where possible, where the operator is located. This requires the integration of sensor data with operational information, such as flight authorisations, event security plans, intelligence inputs, airspace restrictions and available identification mechanisms. Without this integration, LEAs may face either a delayed response or disproportionate intervention.

Tracking and Situational Awareness: Challenges in Integration, Interoperability and Deconfliction

A second set of challenges concerns the capacity to maintain tracking continuity and build a shared operational picture. C-UAS systems must support operators in understanding not only the drone's current position, but also its trajectory, intent, proximity to protected assets and possible relationship with other drones or ground actors. This becomes more difficult in scenarios involving multiple simultaneous drones, urban environments, cross-border areas or high-tempo incidents.

In practice, tracking and situational awareness capabilities often remain fragmented across systems, agencies and jurisdictions. Different sensors, C2 platforms, data formats and operating procedures may limit the ability to create a common operational air picture. This is particularly problematic for major public events, border operations and critical infrastructure corridors, where multiple organisations may need to coordinate their response in real time.[1,7]

Deconfliction is a particularly important LEA challenge. Law enforcement and emergency services increasingly use drones for surveillance, search and rescue, tactical support, disaster response and situational awareness. A C-UAS response that disrupts or misidentifies friendly drones may undermine the broader operation. Future systems, therefore, need to support whitelisting, operational coordination, remote ID integration where available, selective mitigation and clear procedures for distinguishing authorised from unauthorised UAS activity.

Interoperability also has a cross-border dimension. Drone-related threats may involve mobile or transnational actors, including organised crime groups, smugglers or hybrid threat actors. However, legal powers, operational procedures and technical capabilities still vary across Member States. This limits the scalability of C-UAS deployments and makes it harder to develop coherent European responses to incidents affecting borders, airports, ports, energy infrastructure or major international events.[4,17] These limitations can significantly affect the effectiveness of coordinated response in complex, multi-agency scenarios.

Mitigation and Neutralisation: Challenges in Lawful, Selective and Proportionate Response

The third challenge area concerns the ability to deliver effective, proportionate and legally compliant mitigation and neutralisation. In civilian security contexts, the key limitation is not only whether a system can disrupt or disable a drone, but whether it can do so safely, lawfully and without unacceptable collateral effects.

Soft-kill measures, including RF disruption, GNSS interference, spoofing or protocol-level intervention, may be effective against certain drones, but can interfere with nearby communications, navigation systems or friendly UAS. This is particularly relevant in urban environments, airports, public events and emergency response operations, where multiple radio systems may be operating simultaneously. Hard-kill measures, including physical interception, net capture or destruction, may avoid some spectrum-related effects, but introduce other risks such as falling debris, uncontrolled crashes or damage to people and infrastructure.[8]

In addition, the legal basis for mitigation measures may vary significantly across Member States. RF jamming, GNSS interference, spoofing, protocol-level takeover, kinetic interception, data collection and operator attribution may be subject to different authorisation procedures and operational constraints. For LEAs, this means that a technically available C-UAS measure may not always be legally deployable in the same way across jurisdictions, particularly in cross-border scenarios.

This creates a strong requirement for selective and controlled mitigation. For LEAs, the future challenge is not simply to jam or destroy a drone, but to choose the least risky effective intervention. In some cases, monitoring and attribution may be preferable to immediate neutralisation. In others, selective disruption, controlled landing, capture or physical interception may be justified. These decisions require clear rules of engagement, trained operators, legal authorisation and decision-support tools capable of assessing operational risk under time pressure.

The evolution of drone technologies further complicates mitigation. Autonomous flight, pre-programmed routes, swarming behaviour, GNSS-denied navigation and fibre-optic control links may reduce the effectiveness of traditional countermeasures that depend on disrupting command, navigation or communication links.

[17]Frontex (2025), *C-UAS Prize Contest.* Available at: https://www.frontex.europa.eu/innovation/research-and-innovation/prize-contests/c-uas-prize-contest-sFXJdl

This reinforces the need for multi-layered response options, including physical interception, drone-versus-drone concepts, AI-enabled tracking, robotic platforms and integration with broader intelligence and situational awareness systems.[3,7]

Finally, mitigation must be linked to post-incident recovery and investigation. In many LEA scenarios, the drone is not only a threat but also a source of valuable evidence. Its payload, controller, storage media, communication traces and digital logs may support attribution, prosecution and intelligence exploitation. C-UAS procedures therefore need to include safe recovery, evidence handling, documentation and chain of custody, ensuring that the operational response does not compromise subsequent investigative value.[6]

Overall, the main capability gap is not the absence of individual C-UAS technologies, but the difficulty of integrating them into a lawful, interoperable and mission-specific operational capability. Future development should therefore prioritise layered detection, shared situational awareness, selective mitigation, deconfliction with legitimate drone operations, realistic testing, trained operators and harmonised procedures across agencies and Member States.

Conclusions and Future Outlook

The analysis presented in this report shows that C-UAS capabilities in Europe are evolving rapidly, driven by the increased use of diverse drone types, the acceleration of defence innovation, EU policy initiatives and growing operational needs in law enforcement and internal security. Advances in multi-sensor detection, data fusion, C2, selective mitigation and testing methodologies demonstrate increasing maturity across the C-UAS capability chain.

At the same time, the report highlights that C-UAS should not be understood as a purely technological or military capability. For LEAs, counter-drone operations are shaped by legal authority, proportionality, public safety, privacy, spectrum management, evidence preservation and the need to deconflict responses with legitimate drone operations. This reinforces the importance of treating C-UAS as an operational ecosystem, combining technology, doctrine, training, procedures, testing, procurement and cross-agency coordination. However, a key remaining challenge is the operationalisation of these capabilities, ensuring their effective transition from research and validation into deployable, mission-ready tools for LEAs.

The Shift Towards AI-Enabled, Autonomous and RF-Silent Threat Scenarios

A key trend is the progressive shift towards more complex drone threat scenarios. AI-enabled navigation, pre-programmed flight routes, coordinated drone operations, GNSS-denied navigation and reduced reliance on conventional RF links may challenge traditional C-UAS assumptions. The recent use of fibre-optic FPV drones in defence contexts is particularly relevant, as it illustrates how hostile systems can maintain command and video links while reducing their vulnerability to RF detection and jamming.

This creates a continuous cycle of adaptation between drone threats and counter-drone capabilities. Future C-UAS systems will need to combine layered sensing, AI-enabled classification, multi-sensor fusion, common operational picture tools and adaptable mitigation options. However, for LEAs, these capabilities must remain legally deployable, proportionate and operationally safe in civilian environments. This reinforces the need for adaptable and resilient C-UAS architectures capable of addressing evolving and non-traditional threat scenarios.

Recommendations for LEAs

In light of the identified challenges, several priorities can be highlighted for LEAs and other security practitioners:

- **Develop mission-specific concepts of operation**: C-UAS deployment should be tailored to use cases such as prisons, public events, borders, airports, critical infrastructure, and counter-terrorism operations.
- **Strengthen dual-use knowledge exchange between security and defence**: LEAs should benefit from defence lessons learned on emerging drone threats, including FPV drones, electronic warfare, GNSS disruption, swarming concepts and RF-silent systems. At the same time, these lessons must be adapted to civilian security environments, where proportionality, legal authorisation, public safety, evidence preservation and deconfliction with legitimate drone users are essential.
- **Strengthen layered detection and identification**: Future systems should avoid over-reliance on a single sensor type and combine RF, radar, EO/IR, acoustic and data-fusion capabilities where appropriate.
- **Prioritise deconfliction and selective mitigation**: C-UAS responses should distinguish between hostile, careless, non-compliant and authorised drones, while preserving the ability of police and emergency services to operate their own UAS.
- **Improve testing, validation and procurement support**: Standardised testing initiatives and operational trials should continue to support evidence-based procurement and realistic performance assessment.
- **Clarify legal and operational frameworks**: LEAs require clear rules of engagement, authorisation procedures, evidence-handling processes and cross-agency coordination mechanisms.
- **Strengthen EU-level cooperation**: Cross-border information sharing, common procedures and interoperability are essential for responding to transnational drone-related threats, including organised crime, terrorism, and hybrid activities.

These priorities should be addressed in a coordinated manner to ensure coherence across technological, operational and regulatory dimensions.

Future Directions

Looking ahead, the evolution of C-UAS in Europe will depend on the ability to align technological innovation with operational readiness and legal deployability. The EU policy direction confirms that drones and counter-drone capabilities are becoming a strategic priority across both internal security and defence domains. For LEAs, this creates an opportunity to frame C-UAS as a key capability area for countering crime and terrorism in technologically complex environments. Future work should focus on translating research outcomes into operationally usable capabilities, supporting LEA-oriented concepts of operation, identifying priority use cases, promoting training and exercises, and ensuring that counter-drone systems can be deployed safely, proportionately and effectively in real Security contexts.

Overall, the main challenge is no longer only the availability of C-UAS technologies, but their integration into coherent, interoperable and legally accountable operational capabilities. Addressing this challenge will be essential to strengthen Europe's preparedness and resilience against malicious drone use, while preserving the legitimate and beneficial use of drones by public authorities, emergency services and society. This ultimately requires a system-level approach centred on interoperability, operational usability and the effective integration of C-UAS capabilities within the broader European security ecosystem.

Annex 1: C-UAS Project Information

Frame-work	Grant Agreement	Acronym	Name	Funding Call	CORDIS Link	Start	End
H2020	740859	ALADDIN	Advanced hoListic Adverse Drone Detection, Identification Neutralization	H2020-SU-SEC-2016-2017	ALADDIN	2017	2020
H2020	719382	DAPS	Drone Alarm and Protection System	H2020-SMEINST-1-2015	DAPS	2016	2016
H2020	833717	RESPONDRONE	Novel integrated solution for operating a fleet of drones with multiple synchronized missions	H2020-SU-SEC-2018	RESPONDRONE	2019	2022
Horizon Europe	101168392	PRESERVE	Protecting European public spaces against emergent hostile drone threats	HORIZON-CL3-2023-FCT	PRESERVE	2024	2027
ISF	101034655 101190646	COURAGEOUS / * COURAGEOUS^2	Building a common understanding of counter-UAS system performance and testing methodologies	ISF-Police	COURAGEOUS	2021	2028
H2020	211671	KNOX	Cost advantageous and scalable drone alarm and protection system	H2020-SMEINST-2-2016-2017	KNOX	2017	2019

*COURAGEOUS^2 represents the continuation of the original COURAGEOUS project under the Internal Security Fund (ISF), extending its activities on standardisation and testing methodologies.

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.