ANALYTICAL REPORT 08

FROM LAB TO FIELD: STRUCTURAL BARRIERS TO THE DEPLOYMENT OF RF-BASED COUNTER-UAS SYSTEMS FOR CRITICAL INFRASTRUCTURE PROTECTION IN THE EU

An External Expert Report prepared for ENACT

Main Authors
Enrique de Nova

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

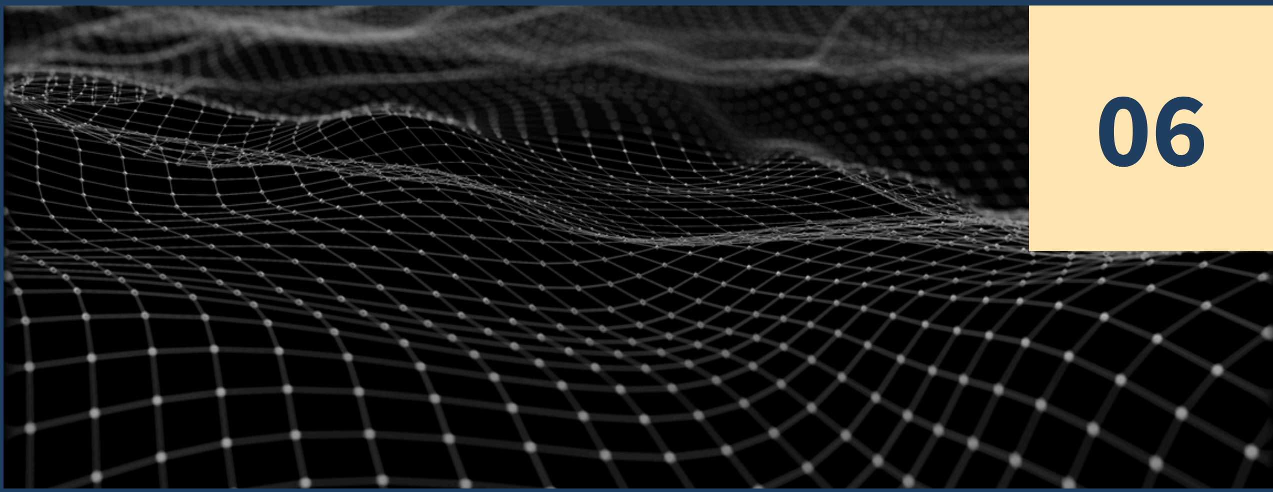
Generative AI tools were used in the preparation of this report as a drafting and editing aid, including structuring content, language editing, and formatting assistance. All analytical claims, regulatory interpretations, market assessments, and recommendations reflect the author's own expert judgement. The author has reviewed, verified, and takes full and exclusive responsibility for the quality, accuracy, originality, and integrity of all content presented in this report.

DECLARATION ON CONFLICT OF INTEREST

The author declares a potential conflict of interest arising from direct involvement as strategic advisor and fundraising manager for VASTIA and SCUUD, active technology ventures operating in the C-UAS domain covered by this report. This report has been developed as an independent analytical contribution based on publicly available evidence, regulatory analysis, and anonymised operational data. No commercially identifiable information about either venture has been included. The report does not promote, commercially reference, or seek to provide competitive advantage to any venture in which the author holds a position.

ACRONYMS

AI	Artificial Intelligence
C2	Command and Control
CAGR	Compound Annual Growth Rate
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CER	Critical Entities Resilience
C-UAS	Counter Unmanned Aircraft Syste,
EASA	European Union Aviation Safety Agency
EDIDP	European Defence Industrial Development Programme
EDIS	European Defence Industrial Strategy
EDA	European Defence Agency
EDF	European Defence Fund
EIB	European Investment Bank
EIC	European Innovation Council
EIF	European Investment Fund
ENISA	European Union Agency for Cybersecurity
EU	European Union
NATO	North Atlantic Treaty Organisation
NIS2	Network and Information Security Directive 2
PCP	Pre-commercial Procurement
PPI	Public Procurement of Innovative Solutions
RF	Radio Frequency
RF-DEN	RF-based Directed Energy Neutralisation
R&I	Research and Innovation
SMEs	Small and Medium-sized Enterprises
TRL	Technology Readiness Level
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle



06

EXECUTIVE SUMMARY

The European Union faces a growing and asymmetric threat from unmanned aerial vehicles (UAVs) targeting critical infrastructure, public spaces, and defence installations. Commercial drones available for as little as EUR 500 have been used for surveillance, smuggling, and armed attacks, with repeated incursions documented at NATO facilities and civilian airports across Member States. The CER Directive, NIS2, the EU AI Act, and the EASA U-space Regulation create clear obligations for infrastructure operators. The market has not produced commensurate operational solutions.

The EU C-UAS landscape has a growing number of technically validated counter-drone technologies at Technology Readiness Levels (TRL) 3 to 6. TRL is a scale from 1 to 9 used by the EU to measure the maturity of a technology: TRL 1-3 covers basic research and proof of concept; TRL 4-6 covers laboratory and pilot validation; TRL 7-9 covers operational demonstration and full deployment. Almost none of the EU-developed C-UAS systems have reached sustained operational deployment at scale. The barriers are structural.

The report closes with five groups of recommendations for EU policymakers, standardisation bodies, public procurement bodies, and the defence innovation ecosystem. Closing the C-UAS TRL-to-deployment gap requires more R&I funding, but also a different process for converting that innovation into operational capability.

KEY FINDINGS

The European counter-drone market is growing at a CAGR of 19-22% through 2034, yet most EU-developed C-UAS systems remain below TRL 7 and have not reached public procurement.

RF-based directed energy neutralisation (RF-DEN) — a technology that uses focused radio frequency energy to disable drone electronics without physical contact or explosive effect, making it deployable in civilian environments — has no harmonised legal framework in the EU for non-military actors. The EU Council documented in 2025 that an evaluation of the harmonisation of Member State laws and procedures is underway [1], implicitly acknowledging that harmonisation does not exist. The European Commission's 2026 Action Plan on Drone Security acknowledges that the military should not be the sole protector of critical infrastructure against low-cost UAVs, and calls for civil-military coordination (COM(2026)81) [2]. In practice, RF-DEN for private critical infrastructure operators is inaccessible in most Member States. This directly contradicts the resilience obligations of the CER Directive and NIS2, which fall precisely on those operators.

No EU-wide C-UAS certification standard exists. Its absence is the main reason infrastructure operators defer procurement.

EU SMEs face a funding gap between TRL 6 demonstrator and market-ready product that EDF, Horizon Europe, and national defence programmes do not adequately address.

Evidence from the Iberian ecosystem shows the path from validated proof-of-concept to first public procurement contract currently takes 4 to 7 years, with regulatory uncertainty as the dominant delay factor. For any SME developing C-UAS systems without institutional support, this period is a funding dead zone in the TRL 6-to-market transition.

KEY RECOMMENDATIONS

Establish a harmonised EU legal framework for civilian C-UAS deployment, with clear spectrum rights, liability rules, and proportionality criteria.

Create a European C-UAS Certification Pathway modelled on EASA aviation safety standards.

Mandate innovation procurement mechanisms (PCP, PPI) for C-UAS in CER-regulated sectors.

Establish a dedicated C-UAS Scale-Up Instrument within EDF/EDIDP.

Create an EU C-UAS Interoperability Standard as a condition of public procurement eligibility.

[1] Council of the European Union. (2025). Note on the use of counter-unmanned aircraft systems (C-UAS) by civilian authorities. ST-15128-2025. Council of the EU.
[2] European Commission. (2026). Action Plan on Drone and Counter-Drone Security (COM(2026)81). European Commission.

1 - INTRODUCTION

More than 2 million drone operators were registered in the EU by the end of 2024 [2]. The global drone market (all segments) reached USD 96.4 billion in 2026 [3]; the military segment alone is projected to reach USD 58.2 billion by 2033 [4]. Low cost, autonomous navigation, payload capacity, and ease of operation make drones useful for commercial operators and adversarial actors alike. Counter-UAS (C-UAS) systems are technologies designed to detect, identify, track, and neutralise unauthorised or threatening drones. They range from passive detection sensors to active neutralisation systems, and their deployment raises complex questions of regulation, certification, and procurement that this report examines.

The threat classifications relevant to the EU Fighting Crime and Terrorism (FCT) domain cover at least four categories. Physical attacks using weaponised UAVs have moved from conflict zones into EU airspace, with incidents documented near NATO facilities in Germany, Poland, and the Baltic states. Surveillance and intelligence gathering using modified commercial drones has been confirmed at nuclear facilities, LNG terminals, and military logistics hubs. Drone smuggling operations are documented in prison systems across several Member States. A 2026 French court case exposed organised networks delivering drugs and encrypted phones into high-security facilities [5]; Ireland has recorded arrests for organised prison drone smuggling; and the scale in the UK, with 1,712 incidents in England and Wales between April 2024 and March 2025 [6], illustrates the magnitude of the risk across comparable European detention environments. Drone-based surveillance of protected individuals and privacy violations are a recognised concern in the EU regulatory framework, though quantified data at EU scale is not systematised.

The threat economics defeat traditional security responses. A EUR 500 consumer drone can cause operational disruption at a major airport costing tens of millions of euros per hour of closure. A swarm of 20 such drones, at a total cost of EUR 10,000, can overwhelm kinetic interception systems costing hundreds of millions to deploy.

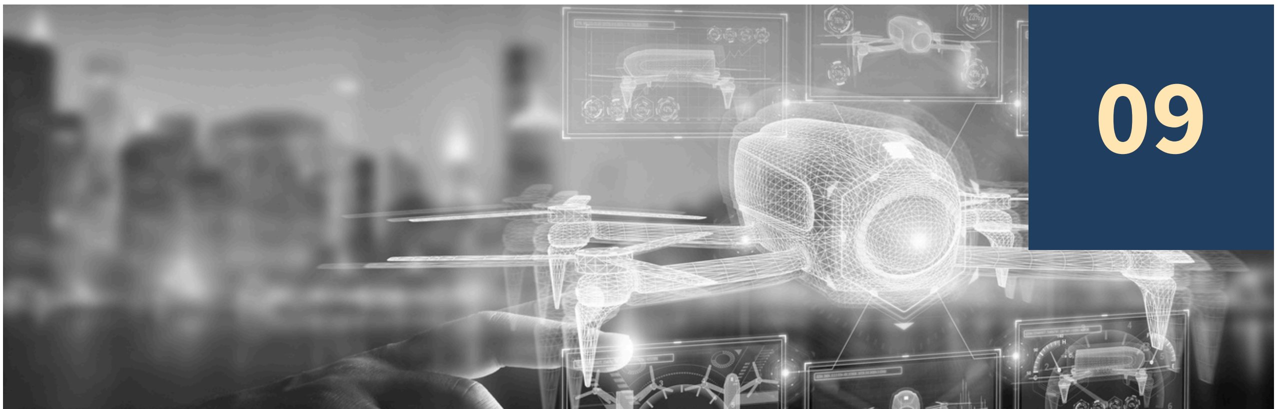
[3] Grand View Research. (2025). Anti-drone market size, share and trends analysis report 2025-2030. Grand View Research.
[4] Coherent Market Insights. (2026). Global Military Drone Market 2026-2033. Coherent Market Insights.
[5] Euro Weekly News. (2026). Drug deliveries by drone: French prison case exposes growing security gap across Europe. Euro Weekly News.
[6] D-Fend Solutions. (2025). C-UAS for Correctional Facilities: Preventing Drone Smuggling. D-Fend Solutions Blog.

This report examines why the EU, despite a clear legislative mandate under the CER Directive and NIS2 and a technically capable industrial base, has not produced C-UAS systems at operational scale. The gap between demonstrated technology readiness and deployment is structural.

The path from a validated counter-drone technology to its operational use in a real infrastructure environment involves several distinct stages: (1) technical development and TRL progression, (2) regulatory authorisation to deploy the technology in civilian contexts, (3) certification against recognised standards, (4) integration with existing security infrastructure, (5) public procurement or commercial sale, and (6) sustained operation with trained personnel. This report focuses on stages 2 through 5, where the evidence shows the most significant and systemic failures. Stage 1, technical development, is relatively well-funded in the EU. Stages 2 through 5 are not.

Report structure

The report reviews the EU regulatory framework (Section 3), analyses five structural barriers (Section 4), measures the impact on the FCT R&I landscape (Section 5), and closes with actionable recommendations (Section 6).



2 - METHODOLOGY

The report draws on three sources of evidence. The first is a structured review of the EU regulatory framework relevant to C-UAS deployment: the CER Directive (EU) 2022/2557 [7], the NIS2 Directive (EU) 2022/2555 [8], the EU AI Act (EU) 2024/1689 [9], the EASA U-space Regulation (EU) 2021/664 [10], and the Radio Equipment Directive 2014/53/EU [11].

The second is a TRL-to-deployment gap analysis across the principal C-UAS technology families: RF detection, AI-based optical and infrared identification, radar, acoustic detection, RF directed-energy neutralisation, jamming, net capture, and laser neutralisation. TRLs are assessed against publicly documented EU-funded projects (2019-2025) and against direct evidence from active development projects in which the author is involved.

The author is strategic advisor and fundraising manager for two active C-UAS development projects: an RF-based neutralisation platform validated in a NATO-linked project context, and a multi-sensor AI drone detection system in active development. Evidence from these projects is presented in anonymised form to preserve commercial confidentiality. A conflict of interest arising from these roles is declared; the report does not promote or commercially reference either project.

The third is a market analysis combining published data [12][3][13][14] with evidence from direct engagement with infrastructure operators, defence sector stakeholders, and public procurement bodies in the Iberian ecosystem.

[7] European Commission. (2022). Directive (EU) 2022/2557 on the resilience of critical entities. Official Journal of the European Union.
[8] European Commission. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). Official Journal of the European Union.
[9] European Commission. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (EU AI Act). Official Journal of the European Union.
[10] European Union Aviation Safety Agency. (2021). Regulation (EU) 2021/664 on a regulatory framework for the U-space. Official Journal of the European Union.
[11] European Commission. (2014). Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (RED). Official Journal of the European Union.
[12] Mordor Intelligence. (2025). Anti-drone market: growth, trends, forecasts 2025-2030. Mordor Intelligence.
[13] Market Data Forecast. (2025). Europe anti-drone market size, share and growth report 2025-2034. Market Data Forecast.
[14] Fortune Business Insights. (2025). Counter-UAS market global forecast 2025-2034. Fortune Business Insights.

Limitations. The primary source of direct operational evidence in this report is the Iberian ecosystem, specifically Spain and Portugal. While the structural barriers identified, regulatory fragmentation, absent certification, interoperability deficits, procurement deadlock, and SME funding constraints, are corroborated by EU-level regulatory documents, CORDIS project data, and market analysis, their specific manifestation in other Member States may differ in degree and configuration. Member States with more developed national C-UAS programmes, such as France or Germany, face a different barrier profile than those without any civilian framework. Findings from the Iberian context are used as illustrative evidence of a broader EU-wide pattern, not as a representative sample of all Member States. Where this report makes EU-wide claims, these are grounded in publicly available EU institutional sources rather than in the operational evidence from the Iberian ecosystem alone.

3 - CURRENT SITUATION, TECHNOLOGY LANDSCAPE, AND REGULATORY CONTEXT

3.1 - REGULATORY DRIVERS AND THE OBLIGATIONS GAP

The CER Directive, adopted in December 2022, establishes a harmonised framework for the resilience of critical entities across eleven sectors, including energy, transport, water, and digital infrastructure. It requires Member States to identify critical entities and ensure they adopt resilience measures. The NIS2 Directive complements CER by extending cybersecurity obligations to a broader range of essential entities and setting 24-hour incident reporting requirements.

These directives create clear legal obligations to address the drone threat as part of physical resilience planning. They do not specify which countermeasures are legally permissible, technically certifiable, or operationally deployable. The EU AI Act, in force since August 2024, adds complexity by classifying AI-based threat identification systems, including those in C-UAS platforms, as high-risk AI systems requiring conformity assessment and human oversight.

The EASA U-space Regulation manages legitimate drone operations; it does not provide a framework for countermeasures against adversarial UAVs. Its interaction with C-UAS deployment, particularly near airports or in urban areas, generates significant legal uncertainty for operators of neutralisation systems.

Table 1. EU regulatory framework relevant to C-UAS deployment: obligations and gaps.

Regulation	Relevant Obligation	Gap for C-UAS deployment
CER Directive 2022/2557	Physical resilience of critical entities; risk assessments; incident response	No specification of permissible countermeasures; no EU C-UAS standard referenced
NIS2 Directive 2022/2555	Cybersecurity of essential entities; 24-hour incident reporting	C-UAS platforms with connected components subject to NIS2 but guidance absent
EU AI Act 2024/1689	High-risk AI systems: conformity assessment, human oversight	AI-based threat ID in C-UAS = high-risk AI; most SME developers not yet compliant
EASA U-space Reg. 2021/664	Integration of drones into civil airspace; geofencing; remote ID	C-UAS neutralisation in shared U-space airspace legally unresolved
Radio Equipment Directive 2014/53/EU	Market access for RF-emitting devices; type approval	C-UAS jammers and RF neutralisers not clearly addressed; national rules vary

3.2 - WHY CURRENT COUNTERMEASURES ARE NOT SCALING

Kinetic interception is effective in controlled environments but generates unacceptable collateral damage risk in populated areas and cannot address swarm threats. Traditional RF jamming disrupts friendly communications alongside adversarial signals and lacks precision in electromagnetically dense environments such as airports or power substations.

High-energy laser systems require capital investment of several million euros per installation and energy infrastructure incompatible with most critical infrastructure deployment contexts. Missile-based interception has a cost-per-engagement far exceeding that of the drones it intercepts, making it economically unviable for the frequency of commercial drone incursions documented at civilian sites.

The result is a market failure induced by the absence of a regulatory/certification framework. The threat is real, growing, and legally mandated to be addressed. No affordable, legally deployable, and technically scalable solution has reached the mass market.

3.3 - TECHNOLOGY FAMILIES AND READINESS LEVELS

RF detection, based on passive listening for drone communication signatures, is mature and widely deployed. Vision-based detection using optical and infrared cameras with AI classification is approaching TRL 7-8 for certain drone categories in controlled environments. Radar offers all-weather capability but generates false positives from birds and requires significant investment. Acoustic detection identifies motor signatures but has limited range. Multi-sensor fusion systems combine multiple detection modalities with AI classification and are the technically most complete configuration available.

High-power directed RF targets drone electronics directly rather than jamming the command link. It is the only non-kinetic technology with effective neutralisation capability in civilian environments at operational ranges, but most EU developers are at TRL 3-5. Laser neutralisation is mature in military contexts; for civilian use it is prohibited or cost-prohibitive.

Table 2. C-UAS technology family comparison, EU market context, 2026

Technology	TRL range (EU)	Civilian legal	Swarm capable	Key constraint
RF detection	7 - 9	Partial	Partial	Passive only
AI vision / IR detection	6 - 8	Yes	Yes	Weather and lighting limits
Radar detection	7 - 9	Yes	Yes	Cost; false positives
RF jamming	7 - 9	Partial	Partial	Spectrum interference
High-power directed RF	3 - 5	Yes	Yes	Regulatory and TRL gap
Net capture	6 - 8	No	No	Range and speed limits
Laser Neutralisation	7 - 9 (military)	Partial	Partial	Cost; civilian prohibition

Analysis of EU-funded C-UAS projects in CORDIS between 2019 and 2025, including ALADDIN (H2020, GA 740859) [15], DAPS (GA 719382) [16], KNOX (GA 768242) [17], ASPRID (GA 892036) [18], and PRESERVE (Horizon Europe, GA 101168392) [19], shows a consistent pattern: projects reach validated detection and identification capabilities in laboratory or pilot environments but do not reach sustained operational deployment. ENACT's own June 2026 report on EU-funded C-UAS [20] projects concludes that the ecosystem shows a clear evolution from isolated detection or mitigation components toward more integrated capabilities, but no project has reached mass adoption by critical infrastructure operators or security forces. Detection-only systems have achieved commercial deployment at several EU airports, notably Dedrone in Germany and DroneShield in the UK, while neutralisation-capable systems remain predominantly in R&D or pilot phases.

[15] ALADDIN - Advanced hoListic Adverse Drone Detection, Identification Neutralization - https://cordis.europa.eu/project/id/740859/
[16] DAPS - Drone Alarm and Protection System - https://cordis.europa.eu/project/id/719382
[17] KNOX - Cost advantageous and scalable drone alarm and protection system for urban contexts - https://cordis.europa.eu/project/id/768242
[18] ASPRID - Airport System Protection from Intruding Drones - https://cordis.europa.eu/project/id/892036
[19] PRESERVE - Protecting euRopean public spaces against Emergent hoStile drone thrEats thRough an adVanced multidimensional shield and cross-border intelligEnce - https://cordis.europa.eu/project/id/101168392
[20] De Tommaso, M., Rodrigues, F., & Alegria, A. (2026). ENACT Flash Report 23 - Counter-UAS capabilities in the EU: technologies, projects and operational challenges (Version 1.0). *European Network against Crime and Terrorism (ENACT).* https://doi.org/10.5281/zenodo.20978143

4 - ANALYSIS

The five barriers below do not act in isolation. They combine to produce a systemic deadlock that none could create alone

4.1 - REGULATORY FRAGMENTATION: THE RF INHIBITION PROBLEM

The first barrier to C-UAS deployment in civilian contexts is the fragmented legal framework governing RF use for counter-drone countermeasures. RF-based C-UAS systems depend on frequency bands regulated under national telecommunications law and the Radio Equipment Directive, and the situation varies enormously across Member States.

Germany and France have moved toward RF inhibition authorisation frameworks for public authorities. In January 2025, the German federal cabinet approved an amendment to the Aviation Security Act extending neutralisation capability, and in 2024 France updated its Internal Security Code to allow police use of directional RF inhibitors at large public events [13][21]. Neither country has extended these frameworks to private critical infrastructure operators. Spain and Portugal have no civilian authorisation framework for RF-based C-UAS neutralisation outside military contexts, with responsibility distributed across telecommunications regulators, aviation authorities, and interior ministries in ways that produce bureaucratic deadlocks. Poland and the Baltic states have accelerated some regulatory adaptation due to their proximity to active conflict, but the resulting frameworks are not harmonised with the rest of the EU.

A developer that validates a system in one Member State cannot deploy it commercially in another without repeating the authorisation process from scratch. For SMEs with limited legal resources, this cost is prohibitive.

[21] Sentrycs. (2026). Navigating the European Skies: The Push for a Unified Counter-Drone Regulatory Framework. Sentrycs Blog.

4.2 - THE ABSENT CERTIFICATION PATHWAY

In adjacent domains, EU certification frameworks give market confidence, insurance coverage, and procurement eligibility: CE marking for radio equipment, EASA certification for aviation systems, EN standards for security equipment. For C-UAS, no equivalent exists.

The usual outcome is procurement deferred indefinitely, or awarded to large international suppliers offering political assurances in place of technical certification. Infrastructure operators have a CER obligation to implement resilience measures, but their insurers will not cover deployments without recognised certification.

No EU body has been formally tasked with developing a civilian C-UAS certification standard, despite the clear market need created by the CER Directive.

4.3 - INTEROPERABILITY DEFICITS

Critical infrastructure operators, airports, energy grid managers, rail network operators, have invested significantly in command-and-control (C2) platforms, security operations centres, and incident management systems. Any C-UAS deployment must interface with these existing systems to be operationally useful. Current EU C-UAS offerings are almost universally proprietary in their C2 integration: they use vendor-specific APIs, communication protocols, and data formats that are incompatible with each other and with legacy security infrastructure.

The result is vendor lock-in, inability to share threat data across systems, and multi-vendor deployments requiring costly custom engineering.

NATO has C2 integration standards for military C-UAS, developed primarily by the Counter-UAS Working Group [22]. They are classified and inaccessible to the civilian security market. No civilian equivalent exists.

[22] NATO Allied Command Transformation. (2023). Counter-unmanned aircraft systems (C-UAS): Alliance approach. NATO.

4.4 - THE PROCUREMENT DEADLOCK

EU public procurement law permits selection criteria based on prior demonstrated performance. In security-sensitive contexts, contracting authorities frequently require prior deployment evidence as a minimum selection criterion. This is a reasonable risk-management approach for the buyer. For innovators with validated but not-yet-deployed systems, it is a structural market entry barrier.

Risk aversion among post-NIS2 operators sharpens the deadlock. Operators now legally accountable for security incidents perceive greater risk in deploying a countermeasure that fails than in suffering a drone incursion, even though the latter is now a compliance failure.

C-UAS deployment at civilian critical infrastructure advances only under extreme operational pressure: airports after serious incidents, military installations in high-alert zones, or high-profile events with explicit government mandate. Without that pressure, regulatory risk, absent certification, and diffuse legal liability produce inaction. Pilot public procurement or normative requirements with defined deadlines are the only mechanisms that can break this cycle.

4.5 - SME-SPECIFIC BARRIERS IN THE EU INNOVATION ECOSYSTEM

The European Defence Fund, with EUR 8 billion for 2021-2027, requires at least 10% of the consortium budget to flow to SMEs. In practice, consortia are led by large prime contractors that control research agendas and IP arrangements. The NATO Innovation Fund is more accessible to SMEs, but its 10-year investment horizon and governance restrictions create barriers for companies that have historically depended on non-NATO-aligned growth capital.

Horizon Europe predominantly supports lower- and mid-TRL research in the security domain. The EIC Accelerator, the instrument most relevant to bridging the TRL 6-to-market gap, has funded C-UAS-adjacent projects but does not specifically address the regulatory and certification barriers that are the primary constraint on commercialisation.

5 - IMPACT ON FCT R&I LANDSCAPE

The barriers in Section 4 produce four measurable consequences for the EU FCT landscape.

Private investment in C-UAS is concentrated outside Europe. Over the past 24 months, C-UAS startup capital has gone to US companies: Epirus, Alpine Eagle, and Allen Control Systems raised USD 291 million, 42% of all disclosed capital in the period [23]. Israeli startups such as Skapion, founded in 2025, raised USD 36 million at seed stage alone. Pure-play European C-UAS SMEs do not appear in venture capital funding data for this period. The most likely reason is what Section 3 documents: without a certification pathway or accessible public procurement, there is no credible investment case for a private investor in a European market that cannot generate regulated revenue.

The global C-UAS market is dominated by US and Israeli suppliers. North America holds 31% of global market share [24], and the principal supply contracts to European NATO countries in 2024-2025 were awarded to companies including Elbit Systems, RAFAEL, and Fortem Technologies. Among European actors with significant presence, only Thales, Leonardo, Rheinmetall, and Saab have C-UAS lines, all integrated into broader defence systems, with no relevant presence in the civilian critical infrastructure segment. This concentration of supply outside the EU creates supply chain dependency, data sovereignty risk, and an inability to audit the systems protecting European critical infrastructure, directly contradicting the EDIS objective [25] of reducing defence import dependency from 78% to 50% by 2030.

The European anti-drone market is growing at a CAGR of 22.6% through 2033 [13], with projections placing the European market at USD 11.6 billion by 2032 [23]. The three principal demand segments are defence and military applications, airports and civil aviation, and critical infrastructure protection, with the latter two directly driven by the CER Directive and NIS2 obligations analysed in Section 3. The interdiction segment, dominated by RF technology, represents more than 53% of global market value in 2026 [15]. The European industrial base captures a marginal share of this growth while the market continues to be served primarily by non-European suppliers.

[23] New Market Pitch. (2026). Counter-UAS startup funding analysis 2024-2026. New Market Pitch.
[24] Mobility Foresights. (2026). Europe Anti-Drone Market Size and Forecasts 2031. Mobility Foresights.
[25] European Commission. (2024). European Defence Industrial Strategy (EDIS). European Commission.

6 - RECOMMENDATIONS

The recommendations below are addressed to four groups: the European Commission and policymakers; standardisation bodies; public procurement authorities in CER-regulated sectors; and the innovation ecosystem, including EDF, EIC, and the NATO Innovation Fund. Each recommendation directly addresses one or more of the five structural barriers identified in Section 4. Recommendations 6.1 addresses barrier 4.1 (regulatory fragmentation). Recommendation 6.2 addresses barrier 4.2 (absent certification). Recommendation 6.3 addresses barrier 4.4 (procurement deadlock). Recommendation 6.4 addresses barrier 4.5 (SME funding gap). Recommendation 6.5 addresses barrier 4.3 (interoperability deficits).

6.1 - HARMONISE THE LEGAL FRAMEWORK FOR CIVILIAN C-UAS DEPLOYMENT

The Commission should adopt a delegated act or implementing regulation under the CER Directive establishing: a positive list of C-UAS technologies permissible for critical infrastructure operators without case-by-case ministerial authorisation; a standardised RF spectrum authorisation process with a maximum processing time of 60 days; clear liability allocation between C-UAS operators and infrastructure owners; and proportionality criteria for sensitive environments. The framework should be developed with national telecommunications regulators (via BEREC) and EASA, and integrated with the NIS2 incident reporting system.

6.2 - CREATE A EUROPEAN C-UAS CERTIFICATION PATHWAY

CEN and CENELEC, with ETSI and EASA, should develop a European C-UAS certification standard covering: detection and neutralisation performance requirements; AI system requirements consistent with the EU AI Act; interoperability; and data protection consistent with GDPR. The standard should include a pre-commercial certification pathway, similar to EASA's Design Organisation Approval process, allowing TRL 5-6 systems to obtain provisional certification for defined, controlled operational pilots. Target timeline: Technical Specification within 24 months, full EN standard within 48.

6.3 - ADOPT INNOVATION PROCUREMENT MECHANISMS

PCP contracts in the EUR 500,000-2M range for pilot deployments at critical infrastructure sites generate operational track record for SME developers and empirical data for the certification standard. A coordinated PPI initiative across airport operators, energy network managers, and rail operators, organised at EU level under the CER Directive, can create a demand signal large enough to justify the certification investment required from developers.

6.4 - CREATE A C-UAS SCALE-UP INSTRUMENT

The European Investment Bank Group's Security and Defence Office, operational since May 2024, is already eligible to finance C-UAS-relevant technologies under its current mandate, including advanced sensors, AI systems, UAVs, and radar systems. In 2025, EIB Group financing in security and defence reached EUR 4 billion, up from EUR 1.2 billion in 2024 [23]. Concrete examples in adjacent domains include EUR 70 million to Quantum Systems for unmanned technologies and EUR 140 million to Exosens for detection and imaging technologies for defence and surveillance [25]. The recommendation for a dedicated C-UAS Scale-Up Instrument should therefore be structured as a targeted facility within the existing EIB Security and Defence framework, combined with EIF equity investment through the Defence Equity Facility under InvestEU, rather than as a standalone new instrument.

Of the five structural barriers identified in this report, the funding gap in this recommendation is the one generating the least friction in the short term. Public financing instruments, including the EIB Group's Security and Defence framework and the NATO Innovation Fund, are already active and eligible. Private venture capital, while still concentrated in US and Israeli companies, is growing in Europe as the geopolitical context sharpens the investment case.

The four remaining barriers, regulatory fragmentation, absent certification, interoperability deficits, and the procurement deadlock, have no equivalent pipeline of active instruments. They require political decisions and institutional mandates that do not yet exist. This asymmetry means sequencing matters: funding instruments can be deployed quickly once regulatory and certification barriers are removed, but funding alone will not move the market while those barriers remain in place.

6.5 - ADOPT INTEROPERABILITY-BY-DESIGN

The Commission, with EDA and ENISA, should publish a minimum interoperability specification for C-UAS systems covering: API standards for security operations centre integration; data format standards consistent with ENISA's common incident reporting format; geospatial data standards; and communication protocol standards for multi-system deployments. This requirement should be phased: advisory in 2027, a condition of EDF/EIC funding eligibility in 2028, and a condition of CER-regulated procurement eligibility in 2029.

[25] European Investment Bank. (2026). Security and Defence: Strengthening Europe's security and defence industry. EIB Group. https://www.eib.org/en/projects/topics/security-defence/index

7 - CONCLUSION

The EU C-UAS landscape shows a gap between innovation policy and operational outcome: a clear and growing security threat, a legislative mandate to address it, a technically capable industrial ecosystem, and a systematic failure of European solutions to reach deployment at scale. The five barriers identified in this report, regulatory fragmentation, absent certification, interoperability deficits, procurement deadlock, and SME constraints, reinforce each other and collectively produce this outcome.

Each year EU-developed C-UAS technologies fail to reach deployment is a year in which European critical infrastructure depends on non-EU systems or inadequate countermeasures, European SME innovators lose competitive position to US and Israeli rivals operating in more enabling regulatory environments, and the investment case for European C-UAS innovation deteriorates further.

The recommendations in this report do not require new R&I investment or new institutional architectures. They require regulatory harmonisation, standards development, and procurement process adaptation, all within the existing mandate of EU institutions. The EU should treat the C-UAS TRL-to-deployment gap as a policy problem with a policy solution, not as a market phenomenon that will resolve itself.

The geopolitical context of 2026, with active conflict on the European continent and documented drone incidents at NATO installations and critical infrastructure sites, makes the urgency of this problem self-evident. The question is whether the EU will create the conditions for its own industrial ecosystem to deliver the sovereign counter-drone capability it has already mandated under the CER Directive.

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.