ChatGPT

Notable Counter-UAS Programs and Standards

Across Europe and North America, a few law-enforcement/border programs have published concrete architectures or test frameworks for counter-unmanned aerial systems (C-UAS). For example, EU authorities and agencies have defined standardized C-UAS test scenarios and multi-layer concepts. INTERPOL's **Project "Courageous"** (2021–23) – funded by EU police/grants – developed uniform threat scenarios (prisons, airports, borders, smuggling) and a standardized test methodology for C-UAS detection/tracking/ID systems in real-world police contexts [1]. Similarly, the European Border Agency (Frontex) has run pilot contests for border-patrol C-UAS: in late 2025 it conducted a **Counter-Drone Prize** where multiple systems were scored on *detection accuracy*, *tracking*, and *neutralization* of illicit drones for border/coastguard use [2]. These EU initiatives emphasize practical performance metrics (e.g. false-alarm rate, sensor coverage) and inter-agency coordination. At the EU policy level, proposals like the **European Drone Defence Initiative** envision a *"multilayered system with interoperable counter-drone capabilities"* – a continent-wide mesh of sensors and countermeasures sharing situational awareness across member states [3]. While not a deployed "program" per se, this indicates a planned architecture of distributed detection/tracking links (e.g. radars, cameras, EW emitters) with a common network for threat data. In parallel, European standards efforts have emerged: e.g. CEN Workshop Agreement **CWA 18150:2024** lays out detailed test methods for C-UAS systems, and the new ISO project *25461* ("Counter UAS – DTI systems") explicitly defines a generic C-UAS DTI (Detect–Track–Identify) architecture and functional requirements [4].

Key Architecture Principles

Most programs converge on a common C-UAS architecture: **multi-sensor data fusion feeding a command interface**. For instance, a Eurocontrol/EuroCAE concept paper breaks down a law-enforcement C-UAS **DTI system** into modular functions:

- **Detection:** One or more sensors (radar, lidar, EO/IR cameras, acoustic arrays, RF receivers) scan for UAVs [5].
- **Tracking:** Sensor outputs are fused to maintain continuous "tracks" with position/velocity for each detected UAV [6].
- **Identification:** Tracks are correlated with known signatures or metadata to recognize friend vs. foe (e.g. registered drone vs. rogue) [7].
- **Classification:** Targets are categorized by type or behavior (e.g. quadcopter vs. large UAS, erratic vs. flight plan) [8].
- **Alerting:** The system flags threats (unauthorized or hazardous flights) according to site rules [9].
- **Control/Monitoring:** Operators set modes and check system status (health, sensor alignment) [10].
- **Recording/Visualization:** All data (raw and processed) are logged and displayed on a common user interface for real-time situational awareness [11].
- **Performance Analysis:** Built-in tools check system coverage/performance against mission requirements (e.g. detection range, track continuity) [12] [13].

In other words, a C-UAS network is treated as a **"system of systems"** with freedom to mix-and-match sensors and software, provided the output meets the mission performance requirements [13]. In practice, law-enforcement deployments often use a **multi-sensor fusion approach**. For example, a UK industry partnership (Cambridge Pixel + OpenWorks) has fielded a **portable C-UAS kit** combining radar processing with AI-driven EO/IR tracking [14]. Radar data are fused with optical detections to automate track/alert workflows: one vendor notes their system enables *“multi-sensor data fusion, target tracking and automated alerting”*, coupled with high-precision visual ID [15]. Such modular, containerized systems are designed for flexible use (fixed towers, mobile vehicles, or emergency response teams). This reflects the general standard being drafted: ISO AWI 25461’s abstract explicitly mentions an “example architecture” of detection/localization/identification systems and spells out high-level functional requirements for each [4].

National Programs (Police/Border)

- **Poland (Border Guard C-UAS system):** In response to recent drone incursions, Poland has started deploying a dedicated border anti-UAV network [16]. Initial elements include long-range radars mounted on high observation towers along the eastern frontier. These sensors form the first “cluster” of the system, feeding real-time data back to a central monitoring center (at a border electronics barrier in Białystok and to border guard HQ) [16]. The Phase-1 goal is simple: *detect and geolocate approaching drones*. Neutralization means (jamming, guns, etc.) will be added later. This illustrates a classic C-UAS chain: high-mounted radars (sensor), networking to ops centers (data links), and integration into existing border control rooms.

- **United States (Local Law Enforcement):** The U.S. has no single national C-UAS network for police, but agencies are building capabilities via grants and R&D. Notably, FEMA in 2025 announced a **$500M Counter-UAS Grant Program** for FY2026–27 [17]. This program encourages state/local police to set up drone defense units covering four capabilities: *Detection, Identification, Tracking/Monitoring,* and *Mitigation* [18]. Grant funds may buy commercial radars, RF sensors, cameras, or integration software for an emergency center [19]. In practice, this mirrors the standard architecture: jurisdictions must justify “where drones could threaten” critical sites and propose layered sensor architectures. (Separately, DHS S&T and law enforcement R&D groups have tested various mobile C-UAS kits, but FEMA’s guidance underscores the detection-to-mitigation chain [18].)

- **United Kingdom (Police Equipment):** UK forces have also adopted hybrid systems. A recent UK Police procurement involved the Cambridge Pixel/OpenWorks radar+camera stack above [14]. Other UK pilots (not publicly detailed) have tested RF direction-finders and drone-capture nets, but specific architectures are typically proprietary. Importantly, UK guidance (e.g. from NPSA/ProtectUK) emphasizes integrating any C-UAS tech into existing security plans with clear police coordination – echoing the need for system plans and rules of engagement [20] [21].

- **Other Countries:** Some border forces are experimenting too. For example, Hungarian border police report using drones and thermal cameras in their patrols [22] (though this is surveillance use, not explicitly countering other drones). Hungary’s military has tested physical “anti-drone corridors” of net barriers in exercises [23], but that is a specialized concept. In summary, **few public “program standards” exist** beyond what Europe/U.S. are codifying. Most nations are buying C-UAS kits or running pilots rather than issuing formal nationwide specs.

Implementation Takeaways

From these examples we can infer some common principles and architectural choices:

- **Multi-modal Sensing:** Combining radars (for range), RF/DF sensors (for link detection), cameras (for ID) and even acoustics is typical. For instance, Eurocontrol notes acoustic/optical sensors have much shorter range than radar, so they only cover urban zones [24], whereas long-range radars can scan the sky [5]. Programs therefore layer sensors to cover low-flying craft.

- **Data Fusion and C2:** All systems route sensor outputs into a common picture. The Frontex drone-surveillance pilot (2015) is an example of such fusion: it integrated drone video, IR imagery, and other camera feeds into a shared GIS display for command staff [25]. The Project Courageous trials likewise assume a networked SOC that ingests multiple sensor feeds to "compare different C-UAS tools" on a level playing field [1].

- **Lawful Engagement:** Especially in civilian contexts, systems are built to comply with regulations. The FEMA program stresses coordination with aviation authorities and avoiding collateral effects [26]. Likewise, European contests require systems that *"detect, track and stop drones… in full compliance with EU law"* [2]. In practice, this means most programs initially focus on *soft* countermeasures (signal alerting, jamming, capture nets) rather than lethal measures – though layered kinetic options (guns, missiles) are sometimes envisioned in layered defense (e.g. Poland's planned "drone wall" includes guns and jammers [27]).

- **Test & Performance Metrics:** As noted, programs employ standardized metrics. Eurocontrol's approach and CWA 18150 both aim to define *what* to measure (e.g. probability of detection vs. false-alarm, track continuity, ID accuracy) under varied conditions. FEMA's four capability areas also imply metrics (e.g. X drones tracked within Y seconds). In short, successful C-UAS programs marry technical architecture (sensors+fusion+UI) with explicit performance requirements.

Sources: Open sources from recent EU and US initiatives were used above. For example, Eurocontrol/EuroCAE defined C-UAS functions [28] [13], FEMA published its grant guidance [18], Frontex released contest results [2], Poland announced its border radar project [16], and ISO has documented the basic C-UAS architecture [4]. All citations are provided for verification.

---

[1] Project Courageous
https://www.interpol.int/en/How-we-work/Innovation/Projects/Project-Courageous

[2] Frontex concludes final tests in C-UAS prize contest – Unmanned airspace
https://www.unmannedairspace.info/counter-uas-systems-and-policies/frontex-concludes-final-tests-in-c-uas-prize-contest/

[3] Europe proposes C-UAS funding and joint air defence initiatives – Unmanned airspace
https://www.unmannedairspace.info/counter-uas-systems-and-policies/europe-proposes-c-uas-funding-and-joint-air-defence-initiatives/

[4] ISO/AWI 25461 - Uncrewed aircraft systems — Counter UAS — Functional requirements for detection, localization, and identification
https://www.iso.org/standard/90482.html

[5] [6] [7] [8] [9] [10] [11] [12] [13] [28] PowerPoint Presentation
https://www.eurocontrol.int/sites/default/files/2025-06/20250603-best-practices-cuas-lupton-eurocae.pdf

[14] [15] European police forces to receive advanced C-UAS capabilities - cuashub.com
https://cuashub.com/en/content/european-police-forces-to-receive-advanced-c-uas-capabilities/

[16] Poland has deployed the first elements of a counter-drone system on the border with Belarus
https://babel.ua/en/news/123905-poland-has-deployed-the-first-elements-of-a-counter-drone-system-on-the-border-with-belarus

[17] [18] [19] [26] FEMA Announces New Counter-UAS Grant Program to Empower Cities, Towns and Villages - National League of Cities
https://www.nlc.org/article/2025/12/09/femas-announces-new-counter-uas-grant-program-to-empower-cities-towns-and-villages/

[20] [21] Countering threats from Uncrewed Aerial Systems (C-UAS) | ProtectUK
https://www.protectuk.police.uk/countering-threats-uncrewed-aerial-systems-c-uas

[22] Hungarian President Praises Border Protection Efforts - Hungarian Conservative
https://www.hungarianconservative.com/articles/current/tamas-sulyok-border-visit-protection-praise/

[23] Hungary Tests Anti-Drone 'Corridors' in Largest Modern Military Drills
https://thedefensepost.com/2025/10/06/hungary-anti-drone-corridors/

[24] cencenelec.eu
https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa-18150.pdf

[25] Frontex and Bulgaria conclude drone pilot project, paving way for smarter EU border surveillance
https://www.frontex.europa.eu/media-centre/news/news-release/frontex-and-bulgaria-conclude-drone-pilot-project-paving-way-for-smarter-eu-border-surveillance-WnJYVT

[27] Poland preparing €2bn anti-drone fortifications along its eastern border amid Russian threat | Poland | The Guardian
https://www.theguardian.com/world/2025/dec/27/poland-anti-drone-fortifications-eastern-borders-cezary-tomczyk