Sensor Fusion and the Common Operating Picture:

The Intelligence Architecture Required for Effective C-UAS Integration Across Echelons

ASSESSMENT SCOPE

This paper assesses the intelligence architecture required for effective C-UAS integration across echelons: the sensor modalities, data transport, fusion, track management, and common C2 frameworks that transform discrete detection events into actionable, cross-domain kill chains. It examines the structural failure mode of bespoke, siloed sensor networks; draws on Ukraine's GIS Arta and Kropyva software as a model of architecture-driven speed; evaluates the GAO-documented CJADC2 framework gaps that limit joint C-UAS data sharing; and analyzes JIATF 401's ongoing effort to build a common C2 network. The paper proposes a layered intelligence architecture spanning the tactical through strategic levels.

PRIMARY SOURCES

MWI West Point: Frontline Fusion (Jul 2025) | GAO-25-106454: Defense C&C, Further Progress Hinges on a Framework (Apr 2025) | CEPA: An Urgent Matter of Drones (Apr 2025) | JIATF 401 Establishment Memo (Aug 2025) | JIATF 401 NCRCC visit / data sharing emphasis (Dec 2025) | DefenseScoop: Pentagon Wants Common Network for Counter-Drone Systems (Dec 2025) | DIU / JIATF 401 Low-Cost Sensing Challenge (Dec 2025) | DefenseScoop: Pentagon C-UAS Authorities / Sensor Data Sharing (Jan 2026) | JIATF 401 Marketplace IOC (Feb 2026) | JIATF 401 Golden Dome Link (Dec 2025) | Army.mil: NGC2 / SDN (Jul 2025) | Army.mil: Adaptive C2 / C2 Fix (Jun 2025) | IFRI: Mapping the MilTech War (Feb 2026) | Military Embedded Systems: GPU Sensor Fusion at Tactical Edge (Sep 2025) | Systel: Turning Sensor Chaos into Decision Dominance (Jun 2025) | DoD OIG: Installation C-UAS Policy Gaps (Jan 2026) | CRS R48477 (Mar 2025) | Hegseth Dec 2025 Installation Defense Policy | CALL No. 25-1093 (Sep 2025) | DoD Ringleader Exercises / DAF Battle Network (Feb 2026) | GIS Arta / Kropyva / Delta analysis sources

DATE

April 2026 | UNCLASSIFIED

This paper draws exclusively on publicly available and officially released sources. No classified information is referenced.

Executive Summary

The C-UAS problem is not primarily a hardware problem. The United States military has invested hundreds of millions of dollars in handheld jammers, exquisite radars, kinetic interceptors, directed energy systems, and sensor towers. Each of these tools works. None of them, operating alone on a bespoke proprietary network, can deliver the detect-identify-track-defeat kill chain that the drone threat demands at the speed the threat operates. The structural failure mode of C-UAS is not missing hardware. It is a missing architecture.

The Modern War Institute's July 2025 analysis identifies the two tasks the Department of Defense must accomplish to solve its current C-UAS challenges: prescribing a common command-and-control system for all services, and implementing a network architecture to share sensor and effector data from the tactical to the strategic level. These two tasks define the intelligence architecture problem precisely. The first is a governance and policy problem. The second is a technical and acquisition problem. Both are harder than buying a better radar.

The operational evidence from Ukraine provides the model. Ukraine's GIS Arta and Kropyva software, developed with U.S. support and adopted at scale by the Armed Forces of Ukraine, compressed sensor-to-shooter timelines from 20 minutes using Soviet-era processes to as little as 30 to 45 seconds. These systems work not because they are technologically superior to U.S. C2 programs, but because they prioritize architecture over hardware: open interfaces, multi-source data fusion, user-accessible common operating pictures, and decentralized execution under shared situational awareness. A distributed, resilient, and scalable C4ISR architecture that fuses multiple ISR sources with C2 and fires platforms, as the CEPA analysis of Ukraine documents, is essential for preserving information dominance and expediting the kill chain.

The U.S. joint force is not without response. JIATF 401, established August 2025, is actively pursuing a common C2 framework for C-UAS systems across all service branches and interagency partners. The Department of the Air Force's Ringleader exercise series, announced February 2026, is integrating air, ground, and space-based sensors into a unified operational framework with a $1 billion Ground Moving Target Indicator allocation in FY2026. The JIATF 401 Low-Cost Sensing Challenge, concluded December 2025, selected MatrixSpace as the winner of a competition that drew 115 submissions across radar, RF, EO/IR, and acoustic sensor modalities. The JIATF 401 marketplace achieved initial operational capability in February 2026 as an online platform connecting validated C-UAS systems to authorized purchasers.

The gap that remains is structural. GAO-25-106454, published April 2025, found that the military services are pursuing CJADC2 projects largely in isolation and without clear goals, that overly restrictive data classification is a significant hindrance to sharing command and control data, and that no entity within DoD is working on solutions to several of these critical cross-organizational challenges. CJADC2 leadership told GAO that addressing these challenges was beyond their purview. The same data governance, classification, and interoperability failures that limit CJADC2 broadly are the precise failures that limit C-UAS sensor fusion and common operating picture delivery across echelons.

THE THREE FOUNDATIONAL FUNCTIONS OF C-UAS INTELLIGENCE ARCHITECTURE

Transport: Establishing robust network connectivity that links diverse sensors and effectors across echelons and domains without relying on bespoke proprietary enclaves. Without transport, sensor fusion and

cooperative engagement are not possible.

Fusion: Correlating and integrating data streams from acoustic, radar, RF, EO/IR, and SIGINT sensors into unified, deduplicated track files with sufficient confidence for engagement authorization. Multi-modal fusion enables drone classification 70 percent faster than single-sensor systems.

Track Management: Assigning, deconflicting, and maintaining track identity across the enterprise as sensors and effectors transfer responsibility through the kill chain. Track identity management is not an afterthought; it is a core C2 function.

1. The Structural Failure Mode: Why Hardware Alone Cannot Solve C-UAS

1.1 The Bespoke Network Problem

The early response to the drone threat across the U.S. military has been to procure hardware: handheld jammers, tower-mounted radar, vehicle-mounted electronic warfare kits, kinetic interceptors. Each individual system performs its detection or defeat function with measurable effectiveness. The systemic failure occurs at the interface between systems. A DroneBuster handheld jammer at a forward operating base cannot pass its detection alert to a Sentinel radar operating on a different proprietary network at the installation perimeter. A LIDS crew that detects and classifies a Group 2 threat cannot automatically cue an adjacent installation's air defense battery if their battle management systems do not share a data protocol. A CUAS sensor tower at a headquarters provides point defense situational awareness; it provides no contribution to the division C-UAS common operating picture if there is no network to receive its output.

The Modern War Institute's July 2025 analysis of C-UAS network architecture is direct on this failure mode: hundreds of millions spent on handheld jammers, exquisite radars, and costly interceptors, each with limitations, and the bigger issue is that they operate independently on bespoke networks. These siloed tools offer little beyond point-defense solutions. They lack the ability to tap into the abundance of joint and strategic sensor data that could transform individual detection events into a coherent, predictive air picture. The architectural metaphor is precise: the good old days of implementing bespoke systems on hub-and-spoke networks are ending, as leaders become more aware of the archaic and siloed air defense architectures that C-UAS has inherited.

This analysis is confirmed by the DoD Inspector General's January 2026 report on installation C-UAS policy, which found that a large percentage of installations do not have the operational approval to use C-UAS capabilities, and that different officials within the same military branch described varying interpretations of approved drone defense policies. The fragmentation is not only technical; it is doctrinal and legal. An installation commander who cannot legally authorize a C-UAS engagement outside the installation perimeter, whose sensors cannot pass data to adjacent installations, and whose systems operate on a proprietary network inaccessible to interagency partners does not have a C-UAS architecture. The commander has a collection of C-UAS tools.

1.2 The Data Classification Barrier

GAO-25-106454, the April 2025 assessment of Defense Command and Control, identifies overly restrictive data classification as a significant hindrance to sharing command and control data. This finding applies with particular force to C-UAS intelligence: sensor fusion requires aggregating data from acoustic detection, passive RF analysis, radar track, EO/IR imagery, and SIGINT attribution across a single operational picture. Each of these data streams may carry different classification levels depending on the sensor, the platform, the intelligence derivation, and the applicable classification guide. When classification architecture requires that each data stream remain in its originating classification enclave, fusion is structurally prevented.

GAO also found that no entity within DoD is working on solutions to the data classification hindrance to CJADC2 data sharing, and that CJADC2 leadership told GAO that addressing this challenge was beyond their purview. For C-UAS, this means that the classification problem is unlikely to be resolved through the CJADC2 process alone. JIATF 401, as the DoD's operational C-UAS authority, must take explicit ownership of C-UAS data classification standards as a core governance function rather than treating them as a background interoperability issue.

The December 2025 Hegseth installation defense policy provides a partial remedy: it explicitly authorized UAS sensor data sharing between military installations and other federal agencies, creating the interagency data sharing authority that was previously absent. This policy action addresses the interagency dimension of the classification and authority barrier. It does not resolve the cross-service, cross-echelon classification fragmentation that prevents tactical C-UAS sensor data from contributing to the operational-level common operating picture.

1.3 The Proprietary Architecture Lock-In

GAO-25-106454 documents a second structural barrier: DOD entities have historically developed complex systems that often have difficulty sharing data because of military department-specific operational and acquisition requirements, stovepipe system development efforts, and proprietary contractor designs and architectures. In its January 2025 report on modular open systems architecture, GAO found that several acquisition programs did not take full advantage of open architecture, in part because DoD did not sufficiently incentivize programs to use and plan for open architecture.

In the C-UAS context, proprietary lock-in means that a sensor tower from vendor A and a battle management system from vendor B may physically co-locate on the same installation and still be unable to exchange track data without a custom-built gateway that introduces latency, requires manual operator action, and degrades the time advantage that sensor fusion is supposed to create. The MWI analysis identifies the SOSA (Sensor Open Systems Architecture) standard as the architectural framework that defense programs are increasingly adopting to prevent this outcome. SOSA-aligned embedded GPU-based plug-in cards provide the flexible, future-proof approach to real-time sensor fusion that proprietary architectures cannot deliver.

2. The Ukraine Model: Architecture-Driven Speed

2.1 GIS Arta and the Artillery Uber Model

Ukraine's GIS Arta, described by analysts as artillery Uber for its algorithmic matching of targets to available artillery units, is the most documented example of how architecture-driven design compresses kill chain timelines to operationally decisive levels. Standard Soviet-era artillery targeting required 20 minutes for preparation and fire mission execution. GIS Arta reduced this timeline to as little as 30 to 45 seconds from target acquisition to fire mission. The system fuses data from UAVs, forward observer reports via smartphones, counter-battery radars, and satellite-based imagery into a single geospatial interface that permits any qualified user to nominate a target and receive automatic assignment to the nearest available artillery unit.

The architectural principles that produce this performance are directly applicable to C-UAS: open interfaces that accept data from multiple heterogeneous sources without requiring format conversion by the operator; an algorithmic optimization engine that matches the threat to the optimal available effector based on range, munition type, and operational status; and a user interface simple enough for dismounted Soldiers with tablets to operate under fire. The system runs on Android tablets, connects via military radios, commercial smartphones, and Starlink satellite internet, and requires no custom hardware beyond what Ukrainian units already carry. The key insight is that GIS Arta did not require a new sensor network. It connected existing sensors through an open architecture that made their data actionable.

2.2 Kropyva and the Distributed Situational Awareness Model

The Kropyva system, developed with U.S. support beginning in 2014, provides a complementary model: a distributed situational awareness application that runs on Android devices and operates across armored units, air defense units, and infantry formations simultaneously. The Kropyva architecture addresses a different dimension of the C-UAS intelligence architecture problem: not how to compress the kill chain, but how to distribute situational awareness to every echelon that needs it without creating a centralized data repository that becomes a single point of failure.

The CEPA analysis of Ukraine's C4ISR architecture notes that Kropyva's data is not stored centrally on servers to be streamed to all devices. Each tablet has information only on the positions and weapons it needs. This federated data model, in which each node holds the minimum required data for its mission rather than requiring access to a central repository, is directly applicable to C-UAS at the tactical edge. A squad-level C-UAS operator does not need the full strategic air picture; the operator needs to know which threats are within engagement range, which friendly effectors are active in the sector, and what the applicable ROE permits. A federated, role-based architecture delivers this without requiring every squad tablet to be cleared for access to a classified central server.

The IFRI February 2026 analysis of Ukraine's military technology ecosystem frames the architectural lesson precisely: Ukraine demonstrates the value of open, adaptable architectures that tolerate partial failure, function under degraded connectivity, and integrate new tools rapidly. Rather than a single monolithic battle management system, the Ukrainian model is a modular, federated combat management ecosystem linking sensors, shooters, communications, and decision support across echelons. The decisive factor has not been visibility alone, but the ability to filter, prioritize, and act faster than the adversary under conditions of information saturation.

2.3 The Delta Ecosystem and Multi-Source Fusion

Ukraine's Delta system, initiated by the volunteer organization Aerorozvidka and later adopted by the Armed Forces of Ukraine, extends the GIS Arta and Kropyva model to the operational and strategic level. Delta is a web-based situational awareness system accessible to strategic headquarters and tactical units alike. It fuses information from UAS reconnaissance, smartphones, radars, satellite imagery, GPS trackers, and open-source intelligence into a comprehensive battlefield overview that serves as the connective tissue between echelons.

The Turkish drone-augmented battle network analyzed in the CEPA report provides a parallel model from a NATO partner perspective. Turkey's concept of operations for UAS in Syria and Libya employed a network-centric approach in which drones operate in conjunction with electronic warfare, long-range fires, and rapid C2 systems enabled by distributed sensor-fusion capabilities. This architecture, described by Turkish analyst Can Kasapoglu as drone-augmented battle networks, exploits UAS's force-multiplying role through integration rather than through any single platform's individual capability.

The common thread across GIS Arta, Kropyva, Delta, and Turkey's battle network is architecture preceding hardware. None of these systems required new sensors to produce their operational effects. All of them worked by connecting existing sensors through open interfaces, fusing their data into unified track files, and delivering actionable common operating pictures to operators at the echelon where engagement decisions must be made.

3. The U.S. Architecture: Current State, Recent Progress, and Persistent Gaps

3.1 JIATF 401 and the Common C2 Framework Effort

JIATF 401, established by Secretary Hegseth's August 2025 memorandum, is the most consequential organizational action in the C-UAS intelligence architecture space. The task force's establishment memo empowers the JIATF 401 Director with acquisition authority up to $50 million per effort, special hiring authority, and the power to determine whether new service-specific C-sUAS programs of record will be adopted. These authorities make JIATF 401 the first DoD organization with the combination of operational focus, cross-service mandate, and resource authority required to drive architecture-level change in C-UAS.

JIATF 401 Director Brig. Gen. Matt Ross stated publicly in December 2025 that all military installations running C-UAS systems in one region need to be able to share data, and that a new capability has to plug in immediately to a common C2 framework. Ross indicated that JIATF 401 planned to deliver this common C2 framework within 90 days of the December 2025 statement. The task force's December 2025 visit to the National Capital Region Coordination Center in Herndon, Virginia, where it met with DHS, TSA, Federal Air Marshal Service, and Air Force personnel, underscored how integrated data sharing, real-time information fusion, and interagency coordination are essential to safeguarding U.S. airspace.

JIATF 401's stated architecture vision aligns precisely with the MWI analysis: integrating sensors with kinetic and non-kinetic efforts and battle management systems into a responsive, interoperable network. The task force's three lines of effort, defending the homeland, supporting warfighter lethality, and joint force training,

all depend on the intelligence architecture being solved first. A warfighter cannot be supported with lethality if the sensor data that drives targeting is siloed behind proprietary interfaces.

3.2 The Low-Cost Sensing Challenge and Sensor Diversity

The JIATF 401 / DIU Low-Cost Sensing Challenge, concluded December 2025, represents the most operationally relevant sensor architecture effort to date. The challenge, launched in May 2025 in collaboration with USNORTHCOM, drew 115 submissions across the full spectrum of sensing modalities, evaluated finalists at the Falcon Peak 25.2 exercise at Eglin Air Force Base in September 2025, and selected MatrixSpace as the overall winner. Three additional companies, Guardian RF, Hidden Level, and Teledyne FLIR Defense, received awards for their performance.

The challenge's design criteria are architecturally significant: the winning systems were evaluated not only on detection, classification, and localization performance, but on scalability, cost, and integration readiness. Integration readiness, the ability for a sensor to plug into the common C2 framework JIATF 401 is building, was an explicit evaluation criterion. This represents a departure from the hardware-first procurement approach that the MWI analysis criticizes, and signals that JIATF 401 is using its acquisition authority to enforce architecture-compatibility requirements in C-UAS sensor procurement.

The multi-modal nature of the winning sensor pool is also architecturally instructive. MatrixSpace operates a radar-based sensing system. Guardian RF focuses on passive radio frequency detection. Hidden Level provides wide-area RF sensing. Teledyne FLIR Defense brings electro-optical and infrared capability. The four systems represent four distinct sensing modalities, none of which alone provides sufficient classification confidence for engagement authorization in a congested airspace. All four together, integrated through a common fusion engine, provide the multi-modal track correlation that enables 70 percent faster drone classification than single-sensor approaches, as Systel's analysis of tactical edge fusion documents.

3.3 The Ringleader Exercises and the DAF Battle Network

The Department of the Air Force announced the Ringleader exercise series at the Warfare Symposium in February 2026, describing a comprehensive initiative to integrate air, ground, and space-based military sensors into a unified operational framework. Secretary of the Air Force Troy Meink stated that the focus has shifted from developing advanced weapon system sensors to closing the kill chain by fusing diverse data streams and executing operations effectively. The exercises leverage the evolving DAF Battle Network, which forms a critical part of the broader CJADC2 effort.

The $1 billion FY2026 budget allocation for Ground Moving Target Indicator applications, disclosed in the Ringleader announcement, represents the financial signal that sensor fusion and data integration have moved from conceptual investment to programmatic investment. Space Force General Michael Guetlein's statement that establishing a robust C2 network is a priority and Chief of Space Operations General Chance Saltzman's emphasis that Ringleader aims to collect and analyze data on a global scale and translate it rapidly into actionable battle management decisions describe the strategic level of the C-UAS intelligence architecture.

3.4 CJADC2 Gaps That Directly Constrain C-UAS Architecture

GAO-25-106454 identifies three specific failures in the CJADC2 program that directly constrain C-UAS sensor fusion and common operating picture development. First, the military services are pursuing CJADC2 activities largely in isolation, without a common framework to guide investments or measure progress. The ICD finalized in October 2024 defines 12 functional requirements across four categories, but military departments and

combatant commands continue to develop capabilities to meet their specific needs without steering toward the CJADC2 vision. For C-UAS, this means that the Army's C-UAS data architecture, the Air Force's Base Defense Operations Center networks, and the Navy's Installation protection systems are each developing independently, with no common data standard, interface requirement, or track format enforcing interoperability.

Second, GAO found limited awareness of experimentation lessons learned across CJADC2 efforts, leading to duplicative investments and slower progress. The Global Information Dominance Experiment series has conducted 11 GIDE events through mid-2024 without a mechanism for systematically incorporating lessons across services. For C-UAS, this means that sensor fusion solutions validated at one GIDE event are not necessarily available to the C-UAS program manager at the next acquisition milestone.

Third, the original CJADC2 vision of connecting every sensor to every shooter has been abandoned by senior Air Force officials as unrealistic and unhelpful, without being replaced by a clearly articulated alternative framework. The CDAO's OPEN DAGIR initiative, announced May 2024, explicitly states that there will not be a single data repository or integration layer of any kind across DoD. For C-UAS, this means that the common C2 framework JIATF 401 is building must be designed for a federated, not centralized, data architecture, exactly the model that Ukraine's Kropyva and Delta ecosystems demonstrate.

Exhibit 1 | C-UAS Intelligence Architecture: Current State Assessment

Architecture Layer	Current Capability	Primary Gap	Key Program / Authority
Sensor Layer (Detection)	Diverse sensor modalities fielded: radar, RF, EO/IR, acoustic. JIATF 401 LCS Challenge completed Dec 2025	Sensors operate on bespoke proprietary networks; integration readiness inconsistent across programs	JIATF 401 LCS Challenge; SOSA/MOSA open architecture standards; MatrixSpace, Guardian RF, Hidden Level, Teledyne FLIR
Transport Layer (Network)	ATAK/CoT at tactical edge; ITN/PACE plans for echelons above brigade; Starlink forward; NGC2 SDN in development	No common C-UAS transport standard; classification barriers fragment data flows across echelons; proprietary gateways introduce latency	Army C2 Fix / NGC2; ADSI C2 gateway (cATO); JIATF 401 common C2 framework (90-day plan, Dec 2025)
Fusion Layer (Track Correlation)	GPU-based edge AI fusion fielded by some programs (SOSA-aligned); multi-modal fusion 70% faster classification documented	No joint C-UAS fusion standard; different programs use incompatible track formats; no enterprise deduplication across echelons	DEVCOM C5ISR SDN experimentation; GPU edge fusion (Systel, HENSOLDT); JIATF 401 authoritative data set requirement
Track Management (Identity / C2)	FAAD C2 for ADA units; ATAK for dismounted; LIDS battle management software; Mastodon Beast+ EW C2	No common C-UAS track number standard; track identity lost at echelon transitions; no joint C-UAS common operating picture	JIATF 401 common C2 framework; MWI transport-fusion-track management framework; CJADC2 ICD Oct 2024
Common	National Capital	No theater or operational-	JIATF 401 / NCRCC model; Hegseth

Architecture Layer	Current Capability	Primary Gap	Key Program / Authority
Operating Picture (COP)	Region Coordination Center (interagency COP); installation-level COPs (proprietary); NORAD/NORTHCOM strategic COP	level C-UAS COP spanning tactical to strategic; interagency data sharing authority expanded Dec 2025 but not fully implemented	Dec 2025 policy (interagency sensor data sharing authorized); Golden Dome data sharing link (Group 3)
Interagency Integration	NCRCC model (DHS, TSA, FAMS, AF co-located); JIATF 401 interagency summit (Nov 2025); Task Force for American Airspace Sovereignty	No standardized interagency data sharing protocol below national-level; legal authorities for C-UAS data sharing inconsistently applied	Hegseth Dec 2025 policy (interagency data sharing authorized); JIATF 401 / DHS / DOJ coordination; FY2025 NDAA Section 1090

4. The Required Architecture: A Layered C-UAS Intelligence Framework

The required C-UAS intelligence architecture is not a single system, a single program of record, or a single acquisition program. It is a layered framework of standards, interfaces, data governance decisions, and organizational authorities that connect existing and future sensors, networks, fusion engines, and command systems into a coherent whole. The Ukrainian model and the MWI analysis both converge on this framing: architecture-driven integration on a common C2 platform, not hardware-first procurement on proprietary networks.

4.1 Layer One: The Sensor Mesh (Tactical Edge)

The foundational layer of the C-UAS intelligence architecture is the tactical sensor mesh: the ensemble of acoustic, passive RF, active radar, and EO/IR sensors that provides the raw detection and classification input to the kill chain. The tactical sensor mesh must meet two requirements that current C-UAS procurement has not consistently enforced: multi-modal redundancy and open interface standards.

Multi-modal redundancy means that no single sensor failure, jamming event, or environmental condition can defeat the detection layer. Active radar is degraded by electronic attack and weather. Passive RF sensors are defeated by frequency-hopping or fiber-optic drone guidance. EO/IR sensors are limited by darkness, obscurants, and clutter. Acoustic sensors are defeated by ambient noise and wind. The combination of all four modalities, with algorithmic cross-correlation, provides the classification confidence that no single modality can deliver. The Systel analysis documents the specific operational gain: correlating acoustic, radar, and optical cues enables C-UAS classification 70 percent faster than single-sensor approaches, and passive RF combined with EO/IR fusion preserves target custody in GPS-denied environments.

Open interface standards mean that every sensor added to the tactical mesh must be able to pass its track data, in a common format, to the transport layer without requiring a custom integration gateway. The SOSA standard provides this framework. JIATF 401's integration readiness evaluation criterion in the LCS Challenge is the enforcement mechanism. All future C-UAS sensor acquisitions under JIATF 401 authority should require SOSA compliance as a threshold requirement, not a desirable characteristic.

4.2 Layer Two: The Transport Network (Tactical to Operational)

The transport layer connects sensors at the tactical edge to fusion engines at the operational level. The MWI analysis is precise: without reliable data transport modes, sensor fusion and cooperative engagement are not possible. The critical hurdle lies in the network plumbing, the infrastructure that allows combat formations to see the same thing in real time. Sensors and effectors at the operational and strategic level must live on actual live networks, not a joint data network, integrated fires network, or some other bespoke enclave that is closed off from the C-UAS data flow.

The Army's C2 Fix initiative and Next Generation Command and Control program address the Army's contribution to this transport layer. C2 Fix, launched 2022 and fielded beginning with the 1st Armored Division in early 2024, modernizes C2 capabilities for divisions and brigades, with MMC-S and ATAK as tactical common operating picture solutions. NGC2, in early development with prototypes tested at Capstone events in 2024 and 2025, addresses the long-term transport architecture through software-defined networking that provides configurable C2 for Army data needs. Army.mil reporting from July 2025 identifies that historically, C2 systems have been designed for discrete functions with underlying architectures that stovepipe data based on warfighting functions and network configurations, leaving limited options to get data to the point of need in degraded connectivity conditions.

The Operation Lethal Eagle exercise in 2024 revealed challenges in achieving a standardized common operating picture due to software version discrepancies and limited real-time data sharing, exactly the transport layer failure that C-UAS data requires to be solved. C2 Fix aims to address these issues at the division level and below, but the C-UAS intelligence architecture requires this problem to be solved across all echelons and all services simultaneously, not sequentially within each service's modernization timeline.

4.3 Layer Three: The Fusion Engine (Operational Level)

The fusion layer is where discrete sensor detections become correlated track files with sufficient identity confidence for engagement authorization. The fusion engine performs three distinct functions: sensor data correlation, track deduplication, and confidence scoring. Sensor data correlation matches detections from multiple modalities against a common target: the radar track, the passive RF detection, and the acoustic signature that all correspond to the same FPV drone approaching from the north. Track deduplication eliminates redundant tracks that arise when multiple sensors detect the same object independently and register it as separate targets. Confidence scoring assigns a classification probability to each track that informs the operator's engagement authorization decision.

GPU-based edge AI provides the computational platform for real-time fusion without requiring connectivity to a remote cloud. Military Embedded Systems September 2025 reporting on GPU sensor fusion documents that in C-UAS and active protection systems, GPUs are essential for fusing high-speed sensor data and running AI models at the edge. Their ability to process visual, radar, and RF inputs simultaneously enables faster decision-making and reduces false alarms in complex, often cluttered environments. As defense programs adopt MOSA standards, including SOSA, embedded GPU-based plug-in cards provide a flexible, future-proof approach to real-time sensor fusion that is compatible with the open architecture requirements that JIATF 401's LCS Challenge is enforcing.

The fusion engine must be positioned at the operational level, not only at fixed installation operations centers. Armored formations moving through contested terrain cannot tolerate fusion latency introduced by routing track data to a rear-area server and waiting for a fused picture to return. The edge AI fusion model places the

fusion engine on vehicle-mounted computing platforms that move with the formation, delivering fused track files to the common operating picture within the latency budget that the kill chain requires.

4.4 Layer Four: The Common C-UAS Operating Picture (All Echelons)

The common C-UAS operating picture is the output of the sensor mesh, transport network, and fusion engine combined: a real-time, multi-echelon display of all detected, classified, and tracked UAS threats within the area of interest, with engagement status, effector assignment, and ROE authorization state visible to every operator with a legitimate need. The NCRCC model that JIATF 401 visited in December 2025 provides the interagency template: military, law enforcement, and homeland security professionals working side by side around the clock from a unified, 24/7 hub with integrated sensor feeds, intelligence inputs, aviation data, and threat reports fused into a single watch floor picture.

The common operating picture must be role-differentiated, not monolithic. A squad-level C-UAS operator needs threat azimuth, range, classification, and applicable ROE for the immediate sector. A battalion S2 needs threat patterns across the brigade area over the past six hours to support predictive analysis. A JIATF 401 analyst needs national-level sensor coverage for homeland airspace sovereignty assessment. The Kropyva federated model, in which each node holds the information required for its mission rather than accessing a common central repository, provides the architecture for delivering role-differentiated COP access without requiring every user to be cleared for the full integrated picture.

4.5 Layer Five: The Interagency and Allied Integration Tier

The fifth layer of the C-UAS intelligence architecture extends beyond the military enterprise to the interagency community and coalition partners. JIATF 401's December 2025 policy authority explicitly permits UAS sensor data sharing between DoD installations and other federal agencies. The JIATF 401 Golden Dome data sharing link, announced December 2025, will focus data sharing on Group 3 drones between JIATF 401 and the Golden Dome missile defense project. The task force's support to World Cup 2026 security planning, involving DHS and local law enforcement in a unified drone threat picture, provides the operational model for large-scale event protection.

NATO interoperability is the allied dimension. The CEPA analysis documents that Turkey's drone-augmented battle networks are the most mature NATO-partner C-UAS architecture, and that NATO collectively has too few drones for a high-intensity fight against a peer adversary and would be severely challenged to effectively integrate those it has in a contested environment. CJADC2's Combined JADC2 initiative extends the JADC2 framework to include coalition and partner collaboration. The ADSI C2 gateway, which demonstrated CJADC2 interoperability at the NATO Coalition Warrior Interoperability Exercise in Bydgoszcz in mid-2024, provides the cross-domain gateway model for passing C-UAS track data between U.S. and allied systems via Cursor on Target, Link 16, and JREAP-C protocols.

5. Five Priority Actions for the C-UAS Intelligence Architecture

Action 1: Mandate SOSA-Compliant Open Interfaces for All JIATF 401-Funded C-UAS Sensors

JIATF 401 should immediately establish integration readiness as a threshold requirement in all C-UAS sensor acquisition programs under its authority, using the SOSA standard as the mandatory interface framework. Sensors that cannot pass track data in a common, non-proprietary format to the JIATF 401 common C2 framework should not receive JIATF 401 acquisition support regardless of their individual detection performance. This action does not require new legislation; it requires JIATF 401 to use the acquisition authority it already has.

Action 2: Establish a C-UAS Data Classification Standard

JIATF 401, working with the CDAO and the classification authorities for each sensor modality, must develop and publish a C-UAS Data Classification Standard that defines the minimum classification level required for each type of C-UAS sensor data and the conditions under which data aggregation elevates classification. Without this standard, the data classification barrier documented by GAO will continue to prevent cross-echelon fusion. The standard should define the baseline as unclassified for passive acoustic, commercial RF detection, and EO/IR track data on Group 1 and 2 threats, enabling tactical operators to share this data without classification caveats.

Action 3: Deploy Edge AI Fusion at the Formation Level

JIATF 401 should fund the development and rapid fielding of vehicle-mounted and dismounted GPU-based edge AI fusion platforms that can integrate multi-modal sensor data at the tactical level without requiring connectivity to a rear-area fusion server. The SOSA-compliant GPU plug-in card architecture provides the hardware standard. JIATF 401's $50 million per effort acquisition authority provides the funding vehicle. Priority fielding should begin with Transforming in Contact 2.0 ABCT formations and JCU-trained C-UAS operators as the primary operational test community.

Action 4: Establish a C-UAS Common Track Standard and Deconfliction Protocol

The MWI analysis identifies track identity management as a core C-UAS C2 function, not an afterthought. JIATF 401 should develop and publish a C-UAS Common Track Standard that defines the data fields, unique identifier format, update rate, and confidence scoring methodology for C-UAS track files across all services and interagency partners. The standard should require every C-UAS sensor and battle management system to assign and maintain unique track numbers, to pass track handoffs with identity continuity, and to report deconfliction conflicts to the C-UAS COP when multiple sensors track the same object with different identifiers.

Action 5: Scale the NCRCC Model to Theater and Operational-Level C-UAS COPs

The NCRCC interagency co-location model provides a proven operational architecture for interagency C-UAS common operating picture delivery. JIATF 401 should work with NORTHCOM, INDOPACOM, and EUCOM to establish theater-level C-UAS common operating picture cells modeled on the NCRCC, connecting JIATF 401's national sensor data, service tactical-level C-UAS feeds, and interagency intelligence inputs into a theater-wide air picture that spans Group 1 through Group 3 threats. The JIATF 401 marketplace's initial operational capability in February 2026 provides the procurement vehicle for validated sensors; the theater COPs provide the operational framework for integrating their data.

Exhibit 2 | C-UAS Intelligence Architecture Implementation Roadmap

Action	Timeline	Lead	Authority / Resource
Mandate SOSA-compliant open interfaces as threshold requirement for all JIATF 401 C-UAS sensor acquisitions; publish integration readiness standard	Immediate (0-90 days)	JIATF 401 Director	JIATF 401 acquisition authority ($50M/effort); FY2026 NDAA alignment
Develop and publish C-UAS Data Classification Standard; define minimum classification level for Group 1-2 sensor data; establish aggregation elevation thresholds	0 to 6 months	JIATF 401 / CDAO / OSD Intelligence	JIATF 401 implementing directive; CDAO classification reform authority
Deliver JIATF 401 common C2 framework; connect all military installation C-UAS systems in at least one region to shared sensor data platform	0 to 90 days (Ross commitment, Dec 2025)	JIATF 401 Director / Brig. Gen. Ross	JIATF 401 acquisition authority; existing JIATF 401 marketplace contract vehicle
Fund and field SOSA-compliant GPU-based edge AI fusion platforms for TiC 2.0 ABCT formations and JCU-trained C-UAS units; establish performance standard	6 to 18 months	JIATF 401 / PM C-UAS / DEVCOM C5ISR	JIATF 401 rapid acquisition authority; DEVCOM S&T program
Develop and publish C-UAS Common Track Standard; define unique track identifier, data fields, update rate, confidence scoring, and deconfliction protocol	6 to 12 months	JIATF 401 / Joint Staff J6 / CJADC2 CFT	JIATF 401 implementing directive; coordination with CJADC2 ICD framework
Establish theater-level C-UAS COP cells at NORTHCOM, INDOPACOM, and EUCOM modeled on NCRCC; connect JIATF 401 national data to theater sensors	12 to 24 months	JIATF 401 / NORTHCOM / INDOPACOM / EUCOM	Combatant command exercise authority; JIATF 401 coordination support
Extend interagency sensor data sharing authorization from homeland installations to tactical formations overseas under Status of Forces Agreements and applicable bilateral agreements	12 to 24 months	JIATF 401 / OSD Policy / Joint Staff J3	FY2025 NDAA Section 1090; Hegseth Dec 2025 policy extension precedent
Establish NATO C-UAS track data exchange protocol using ADSI / Cursor on Target / JREAP-C gateway; exercise with Five Eyes partners in at least one Ringleader event	18 to 36 months	DAF / Joint Staff J6 / JIATF 401	NATO standardization agreements; Ringleader exercise series; CJADC2 CJADC2 framework

Action	Timeline	Lead	Authority / Resource
Implement federated, role-differentiated C-UAS COP access control modeled on Kropyva federated data model; deliver squad-level, battalion-level, and JIATF 401-level interface tiers	18 to 30 months	JIATF 401 / PM DCGS-A / DEVCOM C5ISR	JIATF 401 program authority; Army NGC2 program alignment
Evaluate and publish lessons learned from Ringleader exercise series on sensor fusion effectiveness; incorporate into JIATF 401 sensor acquisition requirements	36 months (recurring)	DAF / JIATF 401 / CJADC2 CFT	Ringleader exercise series lessons integration; GAO-25-106454 recommendation on lessons sharing mechanism

6. Conclusion

The C-UAS problem has been framed for a decade as a technology problem. It is not. Ukraine's $45 billion in military aid has produced some of the most advanced conventional weapons the world has seen, and yet a $500 FPV drone operated by a skilled operator remains one of the most effective weapons on the battlefield. Ukraine's response was not more hardware. It was GIS Arta. It was Kropyva. It was Delta. It was an architecture that connected existing sensors through open interfaces, fused their data into actionable track files, and delivered role-differentiated common operating pictures to operators at every echelon from squad to strategic headquarters.

The U.S. military is beginning to make the same architectural turn. JIATF 401's common C2 framework commitment, the Ringleader exercise series, the JIATF 401 marketplace, and the LCS Challenge's emphasis on integration readiness all signal an institutional recognition that architecture-driven integration is the decisive variable. GAO-25-106454's findings that the military services are pursuing CJADC2 in isolation without a common framework, that data classification is a significant barrier to data sharing, and that no entity is working on several of the critical challenges represent the gap that must be closed.

JIATF 401 has the authority. The SOSA standard provides the interface framework. The federated data model from Ukraine's software ecosystem provides the architectural template. The five priority actions in this paper provide the implementation sequence. What the C-UAS intelligence architecture requires now is execution: the discipline to enforce SOSA compliance in acquisition, to publish a data classification standard that enables fusion, to deliver the common C2 framework that Brig. Gen. Ross committed to in December 2025, and to build the theater-level common operating pictures that allow the joint force to see the drone threat across echelons before it is too late to act.

The drone threat operates in seconds. The architecture that defeats it must operate in seconds. Bespoke networks that require manual data transfer between sensor systems operate in minutes. The difference between seconds and minutes, on a battlefield where 42 percent of vehicle losses in Ukraine came from drone strikes, is measured in lives and mission outcomes. The architecture is the capability. Building it is the mission.

Principal Sources

- Modern War Institute at West Point: Frontline Fusion: The Network Architecture Needed to Counter Drones (transport, fusion, track management; bespoke network failure mode), July 23, 2025
- GAO-25-106454: Defense Command and Control: Further Progress Hinges on Establishing a Comprehensive Framework (services in isolation; data classification barrier; no entity addressing critical challenges), April 8, 2025
- CEPA: An Urgent Matter of Drones: Lessons for NATO from Ukraine (GIS Arta / Kropyva sensor-to-shooter timeline compression; distributed C4ISR architecture; Turkey drone-augmented battle networks), April 2025
- JIATF 401 Establishment Memorandum, Secretary of War Pete Hegseth, August 28, 2025 ($50M/effort acquisition authority; sunset review; JCO disestablishment)
- Army.mil: JIATF-401 Visits NCRCC, Emphasizes Data Sharing, Interagency Unity to Protect US Airspace (Brig. Gen. Ross; community of action; sensor/intelligence/aviation data fusion), December 8, 2025
- DefenseScoop: The Pentagon Wants a Common Network for Its Counter-Drone Systems (Brig. Gen. Ross; 90-day common C2 framework commitment; installation data sharing; World Cup preparation), December 19, 2025
- DIU / JIATF 401 / USNORTHCOM: Winners Announced for C-UAS Low-Cost Sensing Challenge (MatrixSpace, Guardian RF, Hidden Level, Teledyne FLIR; 115 submissions; Falcon Peak 25.2), December 12, 2025
- DefenseScoop: Pentagon Broadens Counter-Drone Authorities (Hegseth Dec 2025 installation defense policy; interagency data sharing authorized; expanded defensive area), January 2026
- ExecutiveGov: JIATF 401 Counter-UAS Marketplace Reaches IOC (JIATF 401 online marketplace; common hardware systems electronic catalog; IDIQ contract vehicle), February 25, 2026
- DefenseNews / JIATF 401: Pentagon Counter-Drone Task Force Plans Golden Dome Link (Group 3 data sharing; multilayered defense; sensor-effector-C2 interoperable network), December 22, 2025
- Army.mil: Software-Defined Networking Provides Configurable C2 for Army's Next Generation Data Needs (NGC2; SDN; stovepipe data architecture failure), July 28, 2025
- Army.mil: Adaptive C2: Modernizing Army Command and Control (C2 Fix; NGC2; Operation Lethal Eagle COP challenges; MMC-S / ATAK; software version discrepancies), June 10, 2025
- IFRI: Mapping the MilTech War: Eight Lessons from Ukraine's Battlefield (Kropyva, Delta, GIS Arta; federated modular combat management ecosystem; open adaptable architecture), February 12, 2026
- Military Embedded Systems: Sensor Fusion at the Tactical Edge: Why GPUs Are Essential for Modern C5ISR Systems (GPU-based edge AI; SOSA standard; visual/radar/RF real-time fusion), September 5, 2025
- Systel Rugged Computing: Turning Sensor Chaos into Decision Dominance (passive RF + EO fusion; 70% faster classification; GPS-denied target custody; JADC2 Project Convergence limits), June 1, 2025
- Next Move Strategy Consulting: Sensor Fusion Powers Next-Gen Defense Integration 2026 (Ringleader exercises; DAF Battle Network; $1B GMTI FY2026; Gen. Saltzman / Gen. Guetlein statements), 2026
- New America / Future Frontlines: How Ukraine's Uber for Artillery Is Leading the Software War Against Russia (GIS Arta; 30-45 second kill chain; open-source sensor fusion; Starlink/Android), 2023
- ACIG Journal: Military Situation Awareness: Ukrainian Experience (Kropyva; 90-95% artilleryman adoption; 5x faster battery deployment; federated data model), 2024
- Wavell Room: AI on the Battlefield: Lessons from Ukraine (Kropyva sensor-effector integration; targeting cycle acceleration; software as integration layer), 2023
- Congressional Research Service R48477: Department of Defense Counter-UAS: Background and Issues for Congress, March 2025
- Center for Army Lessons Learned CALL No. 25-1093: Counter-Unmanned Aerial Systems Training and Implementation at the National Training Center, September 2, 2025
- DoD OIG: Installation C-UAS Policy Report (large percentage of installations without operational approval; varying policy interpretations), January 2026
- AUSA / Army: Achieving Decision Dominance Through Convergence: The U.S. Army and JADC2 (Project Convergence; joint kill web; JSIL; LEO transport layer)
- Breaking Defense: DoD Authorizes First C2 Gateway to Modernize for CJADC2 (ADSI cATO; CoT/JREAP-C/Link 16; CWIX 2024 coalition interoperability), 2024

- Booz Allen Hamilton: Solving the Hidden Challenges of JADC2 (data stewardship vs. data ownership; proprietary OEM lock-in; JADC2 enterprise-level management requirement)