International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXXII No 1 2026

MINI-DRONES, MAXIMUM THREAT: C-SUAS LESSONS FROM UKRAINE

Laviniu BOJOR, Alexandru VASILE, Alexandru PINTILI, Iulian MIHALACHE

"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
bojor.laviniu@armyacademy.ro, vasile.marius@armyacademy.ro, pintili.alexandru@armyacademy.ro, mihalache.iulian@armyacademy.ro

Abstract: *The conflict in Ukraine has established the mini-drone as the dominant tactical instrument of high-intensity ground combat, with FPV platforms and loitering munitions accounting for an estimated 60–70% of confirmed Russian battlefield losses by early 2025. Yet Counter-small UAS (C-sUAS) architectures remain, across every layer examined, structurally insufficient relative to the threat. This article provides a systematic analysis of C-sUAS effectiveness through a three-phase reconstruction of the Ukrainian aerial threat environment (2022–2025), a taxonomy of countermeasure layers — passive physical, electronic warfare, kinetic point-defence, drone-on-drone interception, directed energy, and AI-enabled sensor fusion — and a comparative effectiveness matrix. The central finding is structural: no single layer provides comprehensive protection. Four cross-cutting constraints — IFF ambiguity in a COTS ecosystem, cost asymmetry operationalised as deliberate strategy, doctrinal voids in engagement authority, and the human performance gap — simultaneously limit every countermeasure tier. The article concludes with an integrated five-line adaptation framework arguing that effective C-sUAS capability requires parallel progress across doctrinal reform, architectural integration, industrial reorientation toward a disposable arsenal model, passive-resilience institutionalisation, and Alliance-level IFF standardisation. The window for developing these capabilities before the next conflict, rather than within it, remains open — but is not unlimited.*

Keywords: counter-UAS, mini-drones, FPV drones, Ukraine conflict, electronic warfare

1. Introduction

The conflict in Ukraine has functioned as the most consequential empirical test of Counter-small Unmanned Aerial Systems (C-sUAS) in the history of modern warfare. By 2025, mini-drones account for an estimated 65–67% of confirmed Russian armoured vehicle losses [1], and the air littoral — the contested domain between ground level and the floor of conventional air defence — has become a permanently observable and targetable space for any force equipped with commercial off-the-shelf (COTS) technology. The defensive response to this threat, however, has received comparatively fragmented analytical treatment: individual C-sUAS technologies are well-described in the literature; their interaction, their structural failure modes, and the institutional adaptations required to operationalise them at the appropriate tactical echelons remain underexamined as an integrated problem.

This article addresses that gap. Drawing on academic literature, RUSI, RAND and CEPA analytical reporting, and primary field-level documentation from the Ukrainian theatre, it evaluates the full spectrum of C-sUAS countermeasures — passive physical, electronic warfare, kinetic point-defence, drone-on-drone interception, directed energy, and AI-enabled sensor fusion — against the operational conditions that three years of high-intensity conflict have empirically established. The central argument is structural: *no single C-sUAS*

DOI: 10.2478/kbo-2026-0015

layer provides comprehensive protection against the Phase III threat population. The question confronting NATO planners is therefore not which technology to adopt, but how to integrate all available layers within the constraints of cost, procurement lead time, and tactical echelon.

The article is organised as follows. Section 2 reconstructs the three-phase evolution of the aerial threat in Ukraine (2022–2025). Section 3 examines its tactical and strategic consequences: the collapse of rear-area sanctuary, the operationalisation of cost asymmetry, and the imperative to transition from linear kill chains to networked kill webs. Section 4 provides a systematic countermeasure taxonomy with a comparative effectiveness matrix. Section 5 identifies four cross-cutting structural constraints — Identify Friend or Foe (IFF) ambiguity, cost asymmetry, doctrinal voids, and the human factor — that limit every layer simultaneously. Section 6 translates the analysis into broader implications for NATO's Eastern Flank, focusing on interoperability, IFF standardization, and the urgent need for doctrinal convergence among Alliance frontline states. Section 7 synthesises the findings and outlines directions for further research.

2. Evolution of the Aerial Threat in Ukraine (2022–2025)

The conflict in Ukraine has functioned as a high-tempo evolutionary laboratory for unmanned aerial systems, where tactical innovation cycles rarely exceed a few months before being neutralised by a counter-measure [2]. Three distinct phases have progressively redefined C-sUAS requirements.

2.1 Phase I (Early 2022): The Shock of Tactical Transparency

The Bayraktar TB-2 and COTS quadcopters exposed a fundamental vulnerability in conventional Integrated Air Defence Systems: platforms designed for peer-level aviation proved ineffective against low, slow, small targets operating below the radar horizon. TB-2 strikes destroyed approximately half of Russia's forward-deployed surface-to-air missile systems within the opening weeks [3]. Battlefield transparency had become achievable through commercial, low-cost technology.

2.2 Phase II (Mid-2022–2023): Attrition and the Loitering Munition

The Geran-2 (Shahed-131/136) and Lancet-3 transitioned the threat from ISR dominance to mass precision strike, crystallising the cost asymmetry crisis. Ukraine achieved interception rates above 80% against Shaheds, but the sheer volume and low cost of these systems severely deplete expensive air defence stockpiles [4]. Low-tech kinetic responses, including reactivated Gepard systems, proved more economically viable than high-end interceptors against expendable airframes.

2.3 Phase III (2023–Present): FPV Proliferation and the EW Deadlock

First-Person View kamikaze drones became the dominant consumable munition of ground combat, accounting for 60–70% of Russian systems destroyed or damaged by early 2025 [5]. The Russian EW response — jamming densities of 15–17 installations per kilometre — inflicted losses of up to 10,000 Ukrainian drones per month, yet generated a strategic paradox: ubiquitous jamming accelerated adversarial counter-innovation [6]. Fibre-optic guided FPVs, immune to electromagnetic interference at ranges up to 41 km, and terminal AI guidance that renders jamming irrelevant in the final approach have both rendered soft-kill C-sUAS architectures increasingly obsolete [5]. Concurrently, drone-on-drone interception emerged as a tactically viable C-sUAS method, while mass deployment of inert decoy drones deliberately exhausted Ukrainian interceptor stocks.

This three-phase trajectory establishes the operational context within which contemporary C-sUAS solutions — analysed in Sections 4 and 5 — must be evaluated.

3. Tactical Impact: The Transparent Battlefield

Mini-drone proliferation has produced three mutually reinforcing pressures on conventional ground forces: the elimination of positional sanctuary, the structural unsustainability of high-cost point defence, and the inadequacy of linear engagement architectures. Each pressure, examined below, defines a design requirement that Section 4 addresses in turn.

3.1 End of Sanctuary: Battlefield Transparency and the Air Littoral

Small UAS operate in what Grieco and Bremer define as the *"air littoral"* — the low-altitude space that legacy radar architectures cannot reliably cover [7]. Russian ISR drone orbits averaged 1,000–1,500 daily sorties over the Donetsk axis by August 2024 [5], producing near-continuous *battlefield transparency*: no position, from forward trench to logistics node several kilometres to the rear, could be considered beyond observation or strike range. The operational response — armoured vehicles confined to covered hides at maximum 3 km from the line of contact, 500 km of road protected by anti-drone net tunnels [1] — illustrates how the aerial threat has migrated from a tactical nuisance into a foundational constraint on operational planning.

3.2 The Arithmetic of Defeat: Cost Asymmetry

FPV platforms attributed with approximately 50% of confirmed T-90M tank kills exemplify the core economic problem: a USD 500 drone destroying a USD 3,000,000 platform [1]. Scaled to campaign level, defending with assets costing orders of magnitude more than the attacking system is arithmetically unsustainable. Russia's Gerbera decoy programme operationalised this asymmetry deliberately — inert wooden-and-foam replicas, produced at one-tenth the cost of a Shahed-136, compel defenders to expend interceptors against targets carrying no payload [5]. Ukraine's above-80% Shahed interception rate failed to prevent progressive depletion of high-value interceptor stocks, confirming that kill-rate alone cannot resolve the cost dilemma [2].

3.3 From Kill Chains to Kill Webs

The human performance gap reinforces the architectural conclusion. Soldiers at exposed positions achieve approximately 25% efficiency against attacking drones with small arms; experimental automated turret systems demonstrated reliable engagement at a fraction of the ammunition cost [5]. This 4:1 differential confirms that the human-in-the-loop becomes a bottleneck — not a safeguard — under high-density drone operations. The linear kill chain (Find–Fix–Track–Target–Engage–Assess) is correspondingly inadequate: a single jammed or fratricided node breaks the sequence. A *kill web* architecture — heterogeneous sensors and effectors interconnected via a resilient mesh, with automatic re-routing when individual nodes are degraded — is the structural response, as evidenced by the AI-driven Delta platform's processing of up to 12,000 identified objects per week on the Ukrainian front [8]. The taxonomy and evaluation of the specific layers composing such an architecture is the subject of Section 4.

4. The C-sUAS Spectrum: A Taxonomy of Countermeasure Layers and Operational Effectiveness

No single countermeasure resolves the threat posed by low-cost, commercially derived UAS. The evidence from Ukraine demonstrates that passive, electronic, kinetic, and autonomous measures each address a distinct subset of the threat envelope while exhibiting characteristic failure modes against the remainder. Effective C-sUAS architecture is therefore necessarily stratified: the operational question is not *which* layer to adopt, but how to integrate all layers against a rapidly adapting adversary.

4.1 Countermeasure Layer Overview

Table 1 maps each countermeasure layer against its operational mechanism, documented effectiveness in Ukraine, and primary structural limitation.

Table 1. C-sUAS layer taxonomy — Ukrainian theatre synthesis.

Layer	Mechanism	Effectiveness in Ukraine	Primary Limitation
Passive / Physical	Cope cages, anti-drone netting, covered hides, trench redesign	Reduces per-strike lethality; displaces attacks without attenuating sortie rate	Absorbs effects only; does not degrade adversary drone operations
Electronic Warfare (EW)	RF jamming, GPS spoofing, smart/reactive jamming architectures	High against standard 2.4/5.8 GHz links; ~10,000 FPV losses/month at peak density [6]	Structurally degraded by frequency-hopping, fibre-optic guidance, and terminal AI; omnidirectional jamming causes fratricide
Kinetic	Infantry shotguns, Gepard-type cannon, AI-driven automated turrets, Directed Energy Weapons (DEW — horizon capability)	Automated turrets close the human performance gap; Gepard effective against Shahed-class; DEW offers near-zero cost/shot against swarms	Human operators achieve ~25% engagement efficiency vs. FPV [5]; IFF ambiguity constrains automation; DEW not yet organic at platoon level
Drone-on-Drone (Hunter FPV)	Purpose-modified FPV interceptors physically ram or strike adversary UAVs	Operationally validated at altitudes exceeding 2,100 m against Zala/Orlan-10 ISR platforms; positive cost exchange ratio (~USD 500–1,000 vs. USD 35,000–50,000 target)	No IFF solution for COTS platforms; Rules of Engagement (RoE) framework absent at squad/platoon level; adversary counter-deploys FPV escorts
AI / Automation	Sensor fusion, threat classification, kill-web management; terminal AI guidance (offensive and defensive roles)	Ukrainian platforms identify up to 12,000 objects/week; AI-enabled systems prerequisite for swarm management [8]	Classification accuracy degrades against novel or modified signatures; terminal AI on offensive drones defeats EW entirely, accelerating kinetic demand

4.2 Three Operational Lessons from the Ukrainian Theatre

(a) The structural collapse of EW against fibre-optic and AI-guided platforms. Electronic warfare constituted the primary C-sUAS mechanism for both sides through 2023, with Russian jamming densities reaching 15–17 installations per kilometre. Its effectiveness is, however, contingent on the adversary's electromagnetic dependence. The transition to fibre-optic FPV guidance — operationally demonstrated at ranges up to 41 km [9] — eliminates the radio-frequency attack surface entirely, rendering the entire EW layer irrelevant at the terminal engagement phase [5]. Drones equipped with terminal AI vision lock onto their target after link severance and cannot be jammed, because there is nothing to jam. This structural limit, not tactical countermeasures, is the decisive constraint on EW's long-term contribution to layered C-sUAS architecture.

(b) The performance superiority of automated kinetic systems over human operators. Soldiers engaging FPV drones with small arms achieve approximately 25% engagement efficiency — a 4:1 performance deficit against a fast-manoeuvring target that operates within human reaction-time limits [5]. Automated radar-guided turrets eliminate this bottleneck by operating within the sub-second engagement window that human gunners consistently miss. The doctrinal implication is unambiguous: as EW coverage shrinks against fibre-optic and AI-guided platforms, the terminal kinetic layer must compensate through increased automation. However, this creates an operational paradox: while automation is technically mandatory to match FPV reaction times, the lack of reliable IFF for COTS platforms creates a high risk of fratricide. Until cryptographic identification standards are integrated, autonomous kinetic systems must be restricted to designated *kill zones* where any UAS is engaged by default. Current doctrine attempts to resolve this through a human-confirmation veto, but this partially sacrifices the very reaction-time advantage that justifies automation in the first place.

(c) Hunter FPV interception as an emergent doctrinal category. The deliberate deployment of FPV interceptors to destroy adversary ISR drones — validated at altitudes above 2,100 metres against Zala and Orlan-10 platforms [10][11] — constitutes a qualitatively new C-sUAS modality with no precedent in prior doctrine [12]. Its tactical logic is compelling: it addresses a high-altitude target set that ground-based EW and kinetics cannot reliably reach, at a cost exchange ratio that inverts the asymmetry documented in Section 3. Its doctrinal integration, however, requires dedicated training pipelines, spectrum deconfliction with own-side ISR operations, and RoE frameworks that currently do not exist at the echelons where Hunter FPV is being employed. The absence of these enablers does not negate the operational case; it identifies the institutional work required to convert a proven battlefield improvisation into a sustainable C-sUAS layer.

5. Cross-Cutting Problems in C-sUAS: IFF, Cost Asymmetry, and Structural Gaps

The countermeasure layers catalogued in Section 4 share structural constraints that no single tier can resolve. This section examines the two most acute — IFF ambiguity and economic sustainability — before noting two additional challenges that condition any integrated C-sUAS architecture.

5.1 The IFF Problem: When Both Sides Fly the Same Drone

The proliferation of COTS platforms has produced a battlefield paradox: the same DJI quadcopter, the same FPV frame, and the same component set appear on both sides of the line of contact, making real-time identification of friend or foe structurally impossible with current technology. As Bendett, Roff, and Greenwood (2023) observe, Russian and Ukrainian commercial UAS are *"difficult to tell apart... there are also no electronic means to do so."* [13]. Field documentation from the Ukrainian war shows us a characteristic of the new operational environment full of drones: you cannot distinguish friendly drones from those of the adversary. [14].

The operational consequences cascade across every active C-sUAS layer. EW jamming is indiscriminate by nature: omnidirectional emitters suppress friendly ISR platforms on shared frequencies, and Watling and Reynolds (2025) document fratricide as an already-prevalent problem on both sides of the front. Automated kinetic turrets cannot distinguish a returning Ukrainian reconnaissance quadcopter from an incoming Russian FPV on a near-identical approach profile — the automation that efficiency demands is precisely what IFF ambiguity places at risk. The current resolution is procedural: time-spatial deconfliction, grounding friendly UAVs when C-sUAS systems are active. This is functionally adequate within a coherent formation but brittle at the moments that matter most — sector boundaries, communication breakdowns, and the opening chaos of an engagement. Until a cryptographic hardware-level authentication standard exists for sub-kilogram drones, automation of C-sUAS engagement cannot be implemented without a residual fratricidal risk that procedure alone cannot eliminate.

5.2 The Cost Dilemma: Defending Against Arithmetic

The second structural constraint is economic. A defender who consistently expends assets worth orders of magnitude more than the attacking system is not pursuing a viable long-run strategy, regardless of tactical kill rates. Ukraine intercepted more than 80% of Shahed-136 drones [2] — and progressively drained its interceptor stocks in the process. The USD 500 FPV eliminated by a USD 100,000 interceptor represents a cost exchange that cannot be sustained at Phase III operational tempo.

Russia's Gerbera decoy programme operationalises this arithmetic as deliberate strategy. Of a typical nightly launch wave of 150 drones, only 20-30 carry explosive payloads; the remainder are inert wooden-and-foam replicas produced at one-tenth the cost of a Shahed-136, designed solely to exhaust Ukrainian interceptor stocks [15]. Defenders must engage every target because the cost of misidentifying a real threat exceeds that of expending an interceptor on foam. The economic logic of defence has been weaponised through acute cost asymmetries, as using conventional, million-dollar air defence missiles to intercept inexpensive drones is financially unsustainable over the long term. This dynamic imposes a severe financial burden on the defender, transforming cheap unmanned systems into strategic tools of economic exhaustion [16].

The structural implication is that cost-effectiveness must be a primary selection criterion for C-sUAS architecture. This demands reserving high-value interceptors for threats that lower-tier measures cannot address, treating expendable C-sUAS effectors as class-V munitions whose attrition is a design parameter, and investing in directed energy capability for static high-value sites where near-zero per-shot cost provides the only structurally viable answer to swarm saturation.

5.3 Additional Structural Challenges

Two further constraints condition any integrated C-sUAS response without admitting near-term resolution. The doctrinal gap—the lack of pre-authorized, echelon-specific Rules of Engagement delegating engagement authority to platoon and vehicle levels—means that even well-equipped units are unable to employ C-sUAS systems at their intended performance capacity without institutional reforms that precede, rather than follow, procurement decisions [3][17]. The human factor further compounds these challenges: the shift from direct gunner to systems supervisor inherent to automated C-sUAS architectures demands training pipelines, psychological resilience frameworks, and specialized operator profiles integrating RF literacy, software troubleshooting skills, and combat endurance—capabilities that legacy force development models have yet to systematically cultivate [5]. Both constraints are institutional rather than technological; both are enabling conditions for the layered architecture described in Section 4, and both are examined in the context of NATO Eastern Flank requirements in Section 6.

6. NATO Lessons and Implications for the Eastern Flank

Three outputs from the 2022–2025 period translate the analytical findings of Sections 4 and 5 into direct implications for Eastern Flank forces: the institutional context established by the NATO C-UAS Technical Interoperability Exercise 2024; the capability gaps that context illuminates; and the doctrinal consequence for ground forces.

6.1 What NATO C-UAS TIE 2024 Confirmed

The fourth edition of the NATO Counter-UAS Technical Interoperability Exercise (C-UAS TIE24), held 10–20 September 2024 in the Netherlands, brought together 450 participants from 19 Allied nations and three partner states to test over 60 systems — sensors, effectors, jammers, drone-on-drone platforms, and cyber interceptors — for their ability to operate seamlessly together against Class I UAS threats [18]. Critically, Ukraine participated for the first time — under the NATO–Ukraine Innovation Cooperation Roadmap endorsed at the Washington Summit — bringing direct operational experience from Phase III conditions to an Alliance that had until then engaged with small-drone warfare primarily through modelling and limited field trials. The publicly stated focus of TIE24 was precisely the set of challenges the present study has identified as structurally most acute: drone autonomy and interoperability across national systems [19]. The exercise's prior iterations had already identified C-UAS optimal architectures and data-sharing standards; TIE24 stress-tested these against live Class I UAS scenarios and fed findings directly into NATO's evolving C-UAS reference architectures. Against this confirmed institutional background, and drawing on the structural analysis of Sections 4 and 5, three challenges stand out as most pressing for Eastern Flank forces: sensor coverage below 300 metres remains fragmented across national architectures, producing detection gaps precisely at the altitude band where COTS mini-drones operate [20][7]; engagement authority protocols at lateral sector boundaries between adjacent national C-sUAS zones remain doctrinally unresolved, replicating at Alliance level the void identified at platoon level in Section 5.3 [17]; and the rapid innovation tempo documented from the Ukrainian front — where adversarial adaptation cycles operate in days rather than procurement quarters — is structurally incompatible with NATO's multi-year qualification timelines, establishing industrial responsiveness as a systemic gap in its own right [21].

6.2 Three Acute Capability Gaps for the Eastern Flank

The most acute gaps identified for Eastern Flank forces are three. The first is organic low-altitude detection at the battalion level and below: the absence of persistent acoustic, RF, and short-range radar coverage below conventional air defence sensor floors means that a Phase III FPV swarm can approach a forward position undetected until it is within terminal attack range, at which point no engagement architecture has sufficient reaction time. The second is the cost-exchange structural imbalance — the "Arithmetic of Defeat" in which interceptors consistently cost orders of magnitude more than the drones they destroy. Eastern Flank nations face this imbalance compounded by the Gerbera-type saturation-decoy tactic: waves of inert decoy drones, produced at one-tenth the cost of an armed platform, force the defender to expend high-value interceptors against non-threatening targets [15]. The third gap is Emission Control (EMCON) discipline at the individual soldier level. The RF direction-finding tactic described by Chávez [22] and Osburg et al. [23]—which exploits unsecured commercial datalinks to geolocate operators and subsequently target them with rapid artillery strikes—effectively transforms every electronic device into a potential liability on the battlefield. Yet, despite this lethal reality, electromagnetic signature management (EMCON) largely remains a specialist skill rather than a universal infantry competency, exposing critical vulnerabilities across Eastern Flank ground forces whose field skills were eroded during decades of counter-insurgency operations.

6.3 C-sUAS as an All-Arms Requirement: The Doctrinal Consequence

The direct implication for Eastern Flank ground forces is the one Watling and Reynolds (2025) identify as the central Ukrainian lesson: C-sUAS is no longer a specialist air defence task assignable to designated units but an all-arms requirement that every formation must possess organically. Kallenborn and Vornik anticipated this in 2022 — noting that *"Counter-UAS systems will become a critical component for heavy armour, such as tanks and howitzers, and will form a part of the soldier portable kits"* [3][24] — and three years of operational data from the Ukrainian theatre have confirmed this assessment without qualification. The practical minimum this implies at each echelon is fixed: individual vehicles require passive physical hardening (cope cage, pre-fitted C-sUAS mounting point, signal-reduction kit); platoons require portable EW jamming and pre-authorised engagement RoE against aerial objects meeting defined criteria without real-time higher-headquarters confirmation; companies require at least one Hunter-FPV team with expendable reserve stock treated as class-V munitions rather than accountable equipment. None of these measures requires high-end procurement. All of them require doctrinal reform — the pre-authorised engagement authority, the class-V reclassification, and the institutionalisation of EMCON discipline at the basic training level — that the Alliance has not yet systematically produced. As Kelly et al. [21] document, this gap is not a technology deficit: it is a doctrine, training, and institutional culture gap that procurement alone cannot close.

7. Conclusions

Ukraine has established, at operational scale and without ambiguity, that ***C-sUAS is no longer a specialist capability — it is an all-arms requirement***. Every tactical echelon, from the infantry platoon to the logistics convoy, must possess organic detection and neutralisation capability; the alternative is not a gap in the order of battle but an existential vulnerability in the operating environment that the conflict has normalised. This conclusion is not extrapolated from edge cases: it is the direct implication of a theatre in which 60–70% of confirmed armoured vehicle losses were attributed to drones, in which rear-area sanctuary has ceased to exist below 1,500-metre ISR orbit ceilings, and in which a USD 500 FPV has become the dominant consumable munition of ground combat. The Ukrainian experience did not create a new class of military problem; it revealed the gap between the C-sUAS capability NATO ground forces currently possess and that which the Phase III threat environment structurally requires.

Three practical implications follow with equal force. **First**, no single C-sUAS layer suffices: passive physical hardening, smart reactive EW, organic Hunter FPV capability, and automated terminal kinetics are not alternatives but *complements*, each addressing the failure modes the others cannot cover. An architecture that deploys only one layer — however technically mature — will be defeated by the adversary's adaptation cycle within weeks. **Second**, effective intercept rate is not a valid proxy for effective defence when the cost ratio is adverse: *successful interception is not the same as successful defence* if the defender is expending assets one to two orders of magnitude more expensive than the targets. Restructuring the engagement cost profile — reclassifying attritable effectors as class-V munitions, investing in directed energy for static high-value sites, inverting the exchange ratio through Hunter FPV at the ISR altitude layer — is an industrial and doctrinal imperative, not a procurement preference. **Third**, equipment investment without doctrinal reform delivers hardware without warfighting output. Pre-authorised engagement RoE at the platoon level, air littoral jurisdiction clarity, and the institutional recognition of C-sUAS as a collective training standard are the enabling conditions for every system fielded; they are not adjuncts to procurement — they *are* the procurement's operational value.

The most structurally consequential unresolved problem remains IFF. Because no reliable mechanism currently exists to distinguish a friendly COTS drone from a hostile one in real time, this gap limits the automation of C-sUAS engagements and exacerbates fratricidal risks. Ultimately, this inability to automatically discern targets establishes the normative boundary for deploying Lethal Autonomous Weapon Systems (LAWS), reinforcing the necessity of human oversight in lethal engagements.

Resolving it requires a NATO-level cryptographic authentication standard for mini-drones — a collective-action problem that no national programme can solve unilaterally, and one that must begin *before* technology selection rather than after it. The most urgent direction for further research is accordingly not technical but institutional: a systematic assessment of the degree to which Alliance member states have moved from acknowledging the Ukrainian lessons to embedding them in doctrine, training evaluations, and procurement planning — because the window to build this capability before the next conflict is open, and, as Ukraine has demonstrated at cost, it is not unlimited. ***Ukraine has already paid for these lessons; the only question is whether NATO will learn them on paper or in the field.***

Acknowledgements

The authors declare no external funding or assistance in the preparation of this manuscript.

References

[1] Bojor L, Mandache AR. The $500 Drone That Kills a $3M Tank: Cost-Efficient Lethality and the Rise of FPV Warfare. International conference KNOWLEDGE-BASED ORGANIZATION. 2025;31(1):46–54.

[2] Kunertova D. Learning from the Ukrainian Battlefield: Tomorrow’s Drone Warfare, Today’s Innovation Challenge [Internet]. Wenger A, editor. Center for Security Studies (CSS), ETH Zürich; 2024 [cited 2026 Apr 18]. Available from: http://hdl.handle.net/20.500.11850/690448.

[3] Kallenborn Z. Seven (Initial) Drone Warfare Lessons from Ukraine - Modern War Institute [Internet]. 2022 [cited 2026 May 8]. Available from: https://mwi.westpoint.edu/seven-initial-drone-warfare-lessons-from-ukraine/.

[4] Kunertova D. Drones have boots: Learning from Russia’s war in Ukraine. Contemporary Security Policy. 2023;44(4):576–591.

[5] Watling J, Reynolds N. Tactical developments during the third year of the russo–ukrainian war [Video] [Internet]. Royal United Services Institute; 2025 [cited 2025 Mar 17]. p. 24. Available from: https://static.rusi.org/tactical-developments-third-year-russo-ukrainian-war-february-2205.pdf.

[6] Molloy O. Drones in Modern Warfare: Lessons from the war in Ukraine [Internet]. Australian Army Research Centre; 2024 [cited 2025 Jan 17]. Report No.: Australian Army Occasional Paper No. 29. Available from: https://doi.org/10.61451/267513.
[7] Bremer MK, Grieco KA. The Air Littoral: Another Look. The US Army War College Quarterly: Parameters. 2021;51(4):67–80.
[8] Kirichenko D. The Heart of War: Ukraine's Key Battlefield System [Internet]. CEPA. 2026 [cited 2026 Apr 26]. Available from: https://cepa.org/article/the-heart-of-war-ukraines-key-battlefield-system/.
[9] Fiber optic drones are going to become the new standard. [Internet]. 2025 [cited 2025 Mar 18]. Available from: https://www.youtube.com/shorts/ffJ7IcKl0jU.
[10] DefenseSphere. The Most Brutal FPV Combat Drones Used in the Ukraine War [Internet]. 2024 [cited 2026 May 8]. Available from: https://www.youtube.com/watch?v=TmreZrd6z8Q.
[11] Sabbagh D. "It is impossible to outrun them": How drones transformed war in Ukraine. The Guardian [Internet]. 2025 Jan 4 [cited 2025 Jan 22]; Available from: https://www.theguardian.com/world/2025/jan/04/it-is-impossible-to-outrun-them-how-drones-transformed-war-in-ukraine.
[12] Toroi I. Integration of first person view (FPV) unmanned aerial systems in Romanian ground forces operations. 2024. Available from: https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2024/4%202024/TOROI_1.pdf.
[13] CNA. Drones Over Ukraine: Commercial Technologies in Combat [Internet]. 2022 [cited 2026 May 8]. Available from: https://www.youtube.com/watch?v=QvmTvOV9sUU.
[14] They thought drone was friendly... big mistake! [Internet]. YouTube; 2025 [cited 2025 Mar 28]. Available from: https://www.youtube.com/shorts/V0bKdfOMEpg.
[15] Sebastian C, Vasco C, Goodwin A. Russia is intensifying its air war in Ukraine. A secretive factory is ramping up drone production to fuel the offensive | CNN [Internet]. [cited 2026 May 8]. Available from: https://edition.cnn.com/2024/12/27/europe/russia-ukraine-war-drones-alabuga-factory-intl-invs.
[16] Black J, Paillé P, Kleberg C, et al. Russia's War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine [Internet]. 2024 [cited 2026 May 8]. Available from: https://www.rand.org/pubs/research_reports/RRA3400-1.html.
[17] Mustofa A, Al E. The Use of Drones: From the Perspective of Regulation and National Defense and Security. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021;12(10):670–677.
[18] NATO. NATO tests counter drone technology during interoperability exercise [Internet]. www.ncia.nato.int. [cited 2026 May 9]. Available from: https://www.ncia.nato.int/about-us/newsroom/nato-tests-counter-drone-technology-during-interoperability-exercise.aspx.
[19] Inside Unmanned Systems. NATO Brings Industry to Brussels for C-UAS Week, Ramps Up Counter-Drone Efforts [Internet]. Inside Unmanned Systems. 2026 [cited 2026 May 9]. Available from: https://insideunmannedsystems.com/nato-brings-industry-to-brussels-for-c-uas-week-ramps-up-counter-drone-efforts/.
[20] Calcara A, Gilli A, Gilli M, et al. Why Drones Have Not Revolutionized War: The Enduring Hider-Finder Competition in Air Warfare. International Security. 2022;46(4):130–171.

[21] Kelly TK, Putney A, Parker T, et al. Small Uncrewed Aircraft Systems in Divisional Brigades: Requirements and Findings [Internet]. 2025 [cited 2026 Apr 18]. Available from: https://www.rand.org/pubs/research_reports/RRA2642-1.html.
[22] Chávez K. Learning on the fly: Drones in the Russian-Ukrainian war. 2023;
[23] Osburg J, Parker T, Stoll H, et al. Small Uncrewed Aircraft Systems (SUAS) in Divisional Brigades: Electronic Warfare and Spectrum Management Considerations [Internet]. 2025 [cited 2026 May 8]. Available from: https://www.rand.org/pubs/research_reports/RRA2642-4.html.
[24] Vornik O. Lessons from use of drones in the Ukraine war [Internet]. 2022 [cited 2026 May 8]. Available from: https://www.defenceconnect.com.au/key-enablers/10094-.