12th INTERNATIONAL SCIENTIFIC CONFERENCE ON DEFENSIVE TECHNOLOGIES
OTEH 2026
Serbia, Tara, 21 - 24 October 2026

A LAYERED COUNTER-UAS CONCEPT: FROM MULTI-SENSOR DETECTION AND CLASSIFICATION TO KILL-WEB INTEGRATION

ILIJA POPADIĆ, MILJAN VUČETIĆ, ZORAN BANJAC, BOŠKO BOŽILOVIĆ, IVAN VULIĆ
Vlatacom Institute of High Technologies, Belgrade, ivan.vulic@vlatacom.com

Abstract: *The proliferation of small unmanned aircraft systems (UAS), from commercial quadcopters to Shahed-class loitering munitions, has created a threat that legacy air defense was not designed to counter: low, slow, small, inexpensive, numerous and increasingly autonomous targets. This paper presents a layered counter-UAS (C-UAS) concept spanning the full engagement chain, grounded in engineering results and operational experience. We argue that no single sensing modality suffices: the sensor set must include a passive layer, with acoustic sensing — non-jammable and independent of line of sight — addressing the autonomous, fiber-guided and otherwise radio-silent platforms that defeat radio-frequency (RF) sensing. We then describe artificial-intelligence (AI) classification at the sensor edge, multi-sensor track fusion, and the integration of soft-kill and hard-kill effectors — operational directional jamming and, under development, the AURORA programmable airburst munition, a reusable kinetic micro-interceptor drone and a high-energy laser — into a kill web built on a C7ISTAR solution (command, control, communications, computers, cyber, combat systems and collaboration, with intelligence, surveillance, target acquisition and reconnaissance), whose ORAO (Observe, React, Analyze, Operate) command platform and ARES (Algorithmic Reconnaissance and Execution System) AI core have protected national critical infrastructure since 2024. The concept applies to counter-drone protection of fixed critical-infrastructure sites, vehicles, ships, and temporary sites, including operation in civilian environments.*

Keywords: *counter-UAS, layered defense, multi-sensor fusion, interceptor UAV, kill web.*

1. INTRODUCTION

Few threat classes have evolved as rapidly over the past decade as small unmanned aircraft systems (UAS). Platforms derived from commercial technology are cheap, numerous, simple to operate, and increasingly capable, and loitering munitions of the Shahed type extend the same logic to ranges once reserved for far more expensive weapons. Employed en masse, they impose an unfavorable cost exchange on the defender: over 14,700 one-way attack drones were launched against Ukraine between September 2022 and December 2024, at unit costs one to two orders of magnitude below those of the air-defense missiles initially expended against them [1]. On-board autonomy compounds the problem — a UAS navigating by waypoints or on-board perception offers no control link to detect or deny — and fiber-optically guided first-person-view (FPV) platforms are immune to jamming by construction [2]. It is now broadly recognized in the literature [3], [4], [5] and in strategy and doctrine [2], [6] that no single sensor and no single effector constitutes a counter-UAS (C-UAS) capability. Required is a layered system: complementary sensor modalities, machine-assisted classification, and a command-and-control (C2) layer connecting any sensor to the most appropriate effector — a kill web rather than a linear kill chain. Its measure, and the thread of this paper, is the path from sensor to shooter, which every layer must shorten without surrendering the operator's authority.

C-UAS is a demanding instance of the general command-support problem, whose vocabulary has grown from C2 through C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) to C7ISTAR — command, control, communications, computers, cyber, combat systems and collaboration, integrated with intelligence, surveillance, target acquisition and reconnaissance — which admits cyber defense, combat systems and collaboration as first-class capabilities [7]. The concept is grounded in an integrated anti-drone system — the ORAO (Observe, React, Analyze, Operate) C2 platform carrying the ARES (Algorithmic Reconnaissance and Execution System) artificial-intelligence (AI) core — that has protected a major critical-infrastructure facility in Serbia since 2024, and in research on electro-optical imaging [8], [9], target tracking [10], [11], radar [12], [13] and secure communications. Sections 2 to 6 treat detection, the sensor layer, classification and fusion, decision and effect, and deployment; Section 7 concludes.

2. THE DETECTION PROBLEM

The difficulty begins with physics. Small UAS present radar cross-sections (RCS) orders of magnitude below those of manned aircraft and fly where the radar picture is dominated by clutter, birds and multipath; their speeds reach down to hover, inside the rejection region of classical moving-target processing; thermal signatures are modest, acoustic output attenuates quickly, and visual size defeats unaided observation beyond short range. An emitting UAS offers a radio-frequency (RF) signature buried in congested spectrum; a non-emitting one offers RF sensing nothing — decisive for Shahed-class and other autonomous threats.

Corresponding author: I. Vulić;
E-mail: ivan.vulic@vlatacom.com
DOI: 10.5937/OTEH26074P

Detection ranges are short, closing times shorter, and whatever the architecture achieves must be achieved at a manageable false-alarm rate, because a system that alerts on every bird will be switched off. Experience with a thermal panoramic sensor is instructive [9], [14]: a head covering the full circle in 2.3 s produces some fifty raw detections per second, dominated by clouds and birds; tracking, cloud rejection, bird filtering and AI classification of close targets reduce that flow to about one plausible drone detection per second. Detection is cheap and noisy; tracking, classification and fusion of complementary modalities produce a usable picture [3], [15].

3. THE MULTI-SENSOR DETECTION LAYER

Radar is the backbone of volumetric search: all-weather, day and night, with direct measurement of range and radial velocity; against small UAS, its discriminative asset is the micro-Doppler signature of rotating rotors [15], [16]. In the described system, a compact X-band pulse-Doppler radar is integrated as a third-party component, detecting targets with an RCS of about 0.01 m² at a few kilometers; earlier radar research [12], [13], [17] informs its integration and interpretation of small-target returns. The electro-optical layer compensates for its weak elevation scanning.

RF sensing is passive and continuous, and two of its functions must be distinguished. A wideband receiver performing real-time spectrum analysis over roughly 20 MHz to 6 GHz detects and classifies control, telemetry, and video links, but spectrum analysis alone yields no direction. A direction-finding (DF) antenna array measures bearing by comparing amplitudes across directional elements or using phase interferometry; bearings from two or more DF sensors are triangulated into an approximate position of the platform and, when its controller transmits, of the operator [4]. The limitation is categorical: RF sensing cannot detect non-emitting platforms, such as fiber-guided drones or autonomous ones in radio silence, and must work in dense civilian spectrum.

Electro-optical and infrared (EO/IR) sensing provides what no other modality can: an image — identification, payload assessment, and the visual confirmation that engagement decisions in most settings legally require. The VMSIS3 multi-sensor imaging turret fills this role with a cooled mid-wave (MWIR) or uncooled long-wave infrared (LWIR) channel, a high-definition day channel with optical zoom, a low-light channel and a laser rangefinder from which target coordinates are computed [8], [9]. On an extremely agile pan-tilt positioner, the ROBIN configuration slews to a cued target, and its on-board AI verifies a drone, aircraft, helicopter, or bird in under two seconds. EO/IR is narrow-field and visibility-dependent: most effective when cued rather than searching.

Acoustic sensing detects the propulsion signature of the target: fully passive, non-jammable, effective without line of sight and against precisely the radio-silent platforms — autonomous or fiber-guided — that defeat the RF layer, with 360° coverage at low unit cost and power; propagation modeling draws on earlier acoustic work [18]. Recent peer-reviewed results confirm the modality's maturation [19], and doctrine now recommends passive RF and acoustic layers alongside active sensors [2]. Its physics defines its role — short-to-medium-range passive cueing and gap-filling — and it earns its place exactly where the other modalities are weakest. Table 1 summarizes the complementarity of the four modalities.

Table 1. Complementarity of sensor modalities in the C-UAS detection layer

Modality	Principal strengths	Principal limitations	Role in the layered system
Radar (X-band)	Volumetric all-weather search; range and radial velocity; micro-Doppler	Ground clutter; low-velocity regime; weak elevation scanning	Backbone of early warning and tracking
RF sensing	Passive; link classification; DF bearings and triangulation	Blind to non-emitting targets; congested spectrum	Wide-area passive tripwire and attribution
EO/IR (VMSIS3)	Identification and evidence; AI verification in < 2 s; laser ranging	Weather and visibility dependent; narrow field; requires cueing	Confirmation, identification and geo-location on cue
Acoustic	Passive, non-jammable, 360°; RF-silent UAS without line of sight	Short range; sensitive to wind and ambient noise	Persistent passive detection of azimuth, elevation and velocity

4. CLASSIFICATION AND TRACK FUSION

4.1. Separating targets from confusers

The first task of the intelligence layer is binary and unforgiving: is this track a UAS, or one of the innumerable confusers of the low-altitude environment — above all birds and clouds? In the described system, it is performed by ARES, the Algorithmic Reconnaissance and Execution System: the modular AI core of the C7ISTAR solution, which turns sensor data into a common operational picture and is organized in three tiers that follow the levels of command — ARES Edge (tactical) at the sensor, ARES Core (operational) for fusion across sites, and ARES Strategic (command) for language-model decision support. ARES Edge runs inference at the sensor itself, on a graphics processing unit (GPU) module delivering more than one hundred trillion operations per second, with deep-learning models distinguishing drone, bird, aircraft, and helicopter; only the track and its class label then traverse the network, which keeps the system usable on constrained links and limits data exposure, a concern formalized for distributed sensor networks in [20], [21]. With processing latency below 100 ms, it marks the target, assigns class and confidence, and drives automatic tracking; a Kalman filter with deep-learning re-identification holds the track through occlusion and maneuver, building on robust Kalman tracking in short-wave infrared (SWIR) imagery [10] and motion-triggered track activation [11]. Acoustic classification complements imagery when the target is beyond visual range or emits no visual signature.

4.2. Threat level, fusion and the model lifecycle

Beyond the binary decision, classification refines platform class, link type, payload indications, and signature type, and threat-level estimation combines what the object is with what it is doing — trajectory, altitude, speed, coordination — into a ranked picture. Fusion associates detections across modalities into single system tracks carrying classification, confidence, and full sensor provenance [22], [23]; gossip-type distributed estimation algorithms address consensus across heterogeneous, asynchronously communicating sensor networks [24]. The purpose is continuity — the acoustic layer holding a target behind cover, the radar holding one lost to glare — and credibility: a track confirmed by independent modalities justifies a response that a single-sensor track does not. Because the domain is adversarial and non-stationary, models are maintained assets — curated datasets, monitored in-service performance, controlled retraining [16] — and local training on the edge platform adapts them to the threat picture of a site without data leaving the security perimeter, a sovereignty requirement.

5. FROM SENSOR TO SHOOTER: DECISION, EFFECT AND KILL-WEB INTEGRATION

5.1. The ORAO command-and-control platform

ORAO (also the Serbian word for eagle) is the layer that turns sensing into effect: a C2 platform built on a scalable microservices architecture that underpins the C7ISTAR solution. It integrates sensors and effectors into a single operational picture, suppresses false alarms through fusion, and lets the operator act remotely; new sensors, effectors, or functions are added without altering the core, so that one architecture spans the configurations of Section 6. Figure 1 shows the platform fusing the bearing of the RF direction-finding sensor with electro-optical tracking of the same target, with jammer and sensor sectors on the map.

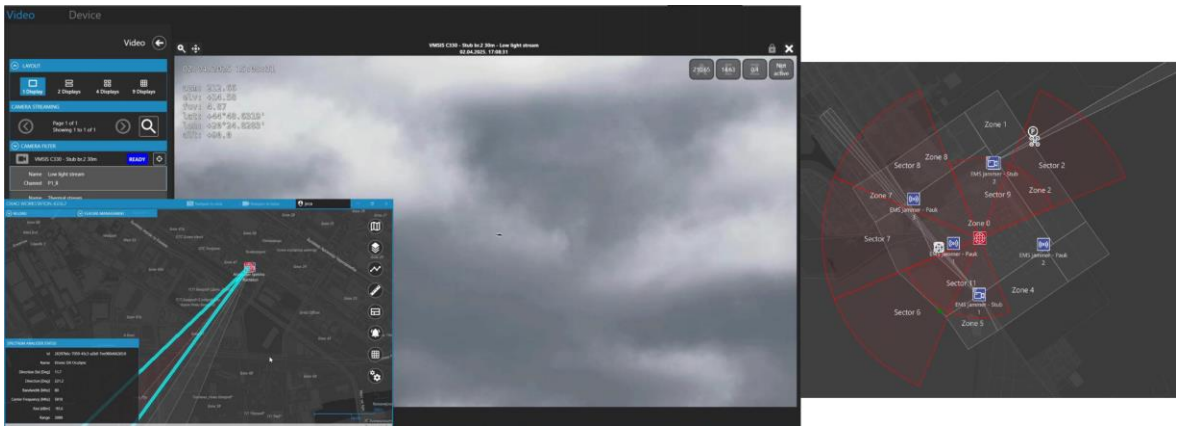


Figure 1. The ORAO console: live optical stream with telemetry, bearing lines of the RF direction-finding sensor with its status panel (classified link, bearing, standard deviation), and sensor and jammer sectors

5.2. The kill web

The integrating principle is the kill web (Figure 2): every sensor and every effector is a node on the common C2 fabric, and the system composes the engagement path best suited to each track — any sensor, best effector [25] — a principle the recent literature refines into federation scoped to concrete engagement chains rather than all-to-all interoperability [26]. The acoustic sensor may hold an RF-silent target the radar cannot separate from clutter; ORAO cues the VMSIS3 turret to that bearing, ARES Edge confirms the object in under two seconds and the rangefinder fixes its coordinates; ARES Core holds the fused track, while ARES Strategic couples the picture to language-model agents that give the operator situation reports and ranked courses of action; on the operator's decision, the appropriate effector is assigned. The fabric is resilient — redundant paths, graceful degradation — and efficient, using the cheapest adequate effector per engagement. It is also a security fabric: every node's identity must be established and its data protected, for which public key infrastructure (PKI) models for authenticating Internet-of-Military-Things devices [27], for interoperability across national and coalition PKI domains [28] and for time-stamped trust in device data [29] provide the design basis. ORAO is supervised-autonomous: AI and rule-based actions prepare and, where configured, execute responses, but authority over the use of force rests with the operator except where narrowly bounded, pre-authorized automatic responses have been deliberately enabled. Where a kill chain offers one path and fails when any link fails, the web offers many, selecting at each engagement the shortest path the rules of engagement allow.

5.3. Soft-kill and hard-kill effectors

Effectors divide into two families with complementary profiles. Soft kill — directional RF jamming of control, telemetry and satellite-navigation links in the standard drone bands — is low-cost per engagement, deep in magazine and comparatively benign; it is the proven method on which the operational system relies, driving the target to descend, return or land. It is ineffective against fiber-guided platforms and autonomous ones navigating without satellite signals, and its use of civilian spectrum is regulated. Hard kill is effective regardless of autonomy and is pursued along three complementary lines.

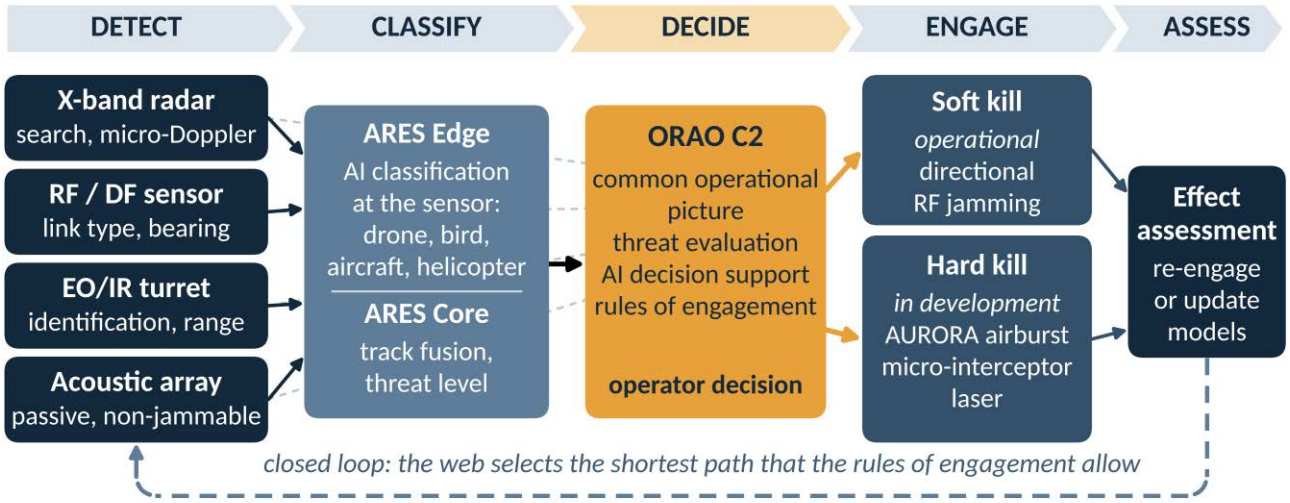


Figure 2. The C-UAS kill web along the engagement sequence: sensors, ARES classification and fusion, ORAO C2 under the rules of engagement, soft kill (operational), hard kill (in development), and effect assessment



Figure 3. Concept rendering of micro-interceptors of the 7-inch class at readiness in a five-position dock-and-launch module; launch is authorized through ORAO over a secure C7ISTAR link

The first line is gun-based: AURORA, a dual-caliber programmable airburst munition for 30 mm and 23 mm autocannons, at technology readiness level 2 with a roadmap to level 7. Instead of requiring a direct hit on a small, agile target, the round carries an electronic fuze built around a high-g-resistant field-programmable gate array (FPGA) timer, set inductively at the muzzle from the muzzle velocity measured for each round; it detonates at the computed intercept point, ejecting a forward cone of pre-formed tungsten fragments that saturates the flight path and defeats the target from a near miss. Timing accuracy is of the order of 2 ms, and the design objective is a kill probability above 85% against agile UAS at a cost per engagement that conventional high-explosive fire cannot approach. As a retrofit — a bolt-on muzzle programming unit and a fire-control interface — it upgrades existing guns without replacement. The program is phased: AURORA-30 (30 × 165 mm, 2A72-class guns, 150–200 tungsten sub-projectiles per round) proves the timer logic and power-source survival under launch loads before the design is scaled down to AURORA-23 (23 × 152 mm, ZU-23-2-class guns, 50–70 sub-projectiles).

The second line is a kinetic micro-interceptor unmanned aerial vehicle (UAV), another effector node of the kill web (Figure 3): a compact tail-sitting quadrotor of the 7-inch class (177.8 mm airframe height) with four electric propulsion units, vertical launch, and a forward-looking electro-optical camera for the terminal phase. Its effect is purely kinetic, by direct impact, with no explosive warhead — a property that matters in the populated settings of Section 5.4. Vehicles wait at readiness in five-position dock-and-launch modules with charging, health monitoring, and safety interlocks; two modules hold ten ready vehicles. The engagement follows the same accountable sequence as every other effector: ORAO holds the fused track, a designated operator authorizes the launch under the rules of engagement, the mission travels over the authenticated C7ISTAR data link, and the vehicle is guided into the intercept basket and completes the engagement with on-board terminal sensing; on a miss or abort, a commanded parachute-assisted recovery returns it for inspection, recharge, and readiness. A reusable interceptor thus extends the cost-exchange logic of AURORA beyond the gun envelope, engaging the fiber-guided and autonomous platforms that jamming cannot defeat, at a per-engagement cost that scales to mass attack — the reason interceptor drones have become the fastest-growing hard-kill layer internationally, up to the autonomous drone-on-drone interception now reported in the literature [2], [30]. Terminal-guidance performance and the recovery cycle are qualification objectives of the current phase.

The third line is a high-energy laser, past functional-model testing and progressing toward a prototype. Neutralization requires holding a small, agile target in a spot of the order of 10 mm for seconds — a collimator, a rangefinder and a pan-tilt and tracking chain of exceptional precision, all inherited from the VMSIS3 line, whose gyro-stabilization is studied in [31]. All three lines consume what the web already produces — fused track, range and authenticated tasking — and the layered system selects per engagement: soft kill first wherever the threat depends on its radio links, hard kill where soft kill cannot reach.

5.4. Operation in civilian environments

C-UAS operates over and around civilian life, making constraints design inputs rather than afterthoughts:

jamming interacts with regulated spectrum and legitimate users; kinetic and directed-energy effects over populated areas carry collateral risk; and interception of aircraft, however small, engages aviation law and requires a documented decision trail. The operational system therefore provides selective control of jammer power and coverage zones, safeguards against unauthorized triggering unless a fully automatic mode is explicitly enabled, geographic and functional zoning of permitted effects, and evidentiary logging of imagery, tracks and decisions in time-stamped, cryptographically verifiable records [29]. Among hard-kill options, a warhead-free kinetic interceptor with controlled recovery best fits these constraints, introducing neither blast nor fragmentation over the protected area.

6. DEPLOYMENT AND USE CASES

The clearest evidence that the architecture is more than conceptual is that it is deployed. Since 2024 the integrated anti-drone system has protected a major critical-infrastructure facility in an urban environment in Serbia, stopping small commercial and FPV drones before they come within 500 m of the perimeter: sensor towers with panoramic cameras, RF detection and direction-finding sensors and agile VMSIS optics cover roughly one square kilometer, and a countermeasure tower provides RF jamming with selective radiation and coverage control so that the surrounding area is unaffected, all operated through ORAO; because the site is urban, radar was omitted and the passive and optical layers carry detection. The site maps onto concentric functions — early warning at distance, confirmation in the middle zone, countermeasures in the inner zone — under continuous unmanned watch that alerts a small response element.

The same architecture has been engineered for mobility: a configuration on a 4×4 mine-resistant ambush-protected (MRAP) vehicle packages ORAO, the sensor suite, the edge-AI optoelectronic turret, and RF countermeasures onto a protected cross-country platform, rapidly movable to a threatened location and remotely commanded.

The maritime profile extends the architecture to vessels and offshore infrastructure, where operational experience has made the cost-exchange argument unanswerable: in the Red Sea, warships expended roughly 220 air-defense missiles — on the order of a billion dollars — against UAS and missile attacks in a single year [32]. In the configuration engineered for a very large crude carrier (VLCC), two radar heads with overlapping coverage, six acoustic nodes along the hull and four marinized Skua EO/IR turrets feed a shipboard ORAO instance, with two five-position micro-interceptor dock modules on the aft weather deck as the effector layer; the installation is a segregated security enclave with no control path into ship systems and no default external dependency. Maritime sensing experience — surface-wave radar for wide-area sea surveillance [12], [17] and fusion of automatic identification system (AIS) data with over-the-horizon radar tracks [23] — carries directly into this profile, and the low-altitude picture of the vessel federates into the same recognized picture as the shore-side sites.

Temporary sites and public events form a fourth profile: rapidly deployable, soft-kill-preferred and bound by the tightest civilian constraints. Across all profiles the same components scale from a self-contained site to federated regional coverage within the recognized air picture; the passive acoustic node is most valuable in mobile and temporary profiles, where emission control is itself protective.

7. CONCLUSION

There is no single-sensor, single-effector answer to the small-UAS threat: the threat is defined precisely by the properties — small, slow, low, cheap, numerous, increasingly autonomous — that defeat point solutions. The answer is architectural: a distributed multi-modal sensor layer including a passive component effective against non-emitting targets; a classification and fusion stage producing a credible, ranked threat picture at a manageable false-alarm rate; and a kill-web C2 layer connecting any sensor to the best available effector under explicit rules of engagement — the shortest defensible path from sensor to shooter, under human authority and recorded at every step.

The presented results substantiate each element: ARES discriminates drones from birds, aircraft, and helicopters at the sensor edge and fuses tracks into one picture; the agile optoelectronic turret confirms a cued target in under two seconds; the passive acoustic sensor addresses the radio-silent platforms that defeat the RF layer; and ORAO binds these sensors with the operational jammer and with the airburst gun, micro-interceptor, and laser under development into one kill web, whose operational core has protected national critical infrastructure since 2024. Future work covers integrating the acoustic layer into the wider air picture, maturing AURORA, qualifying the micro-interceptor and its recovery cycle, advancing the high-energy laser, and improving the adversarial robustness of classification; defense against coordinated multi-axis swarms remains the next open problem [3], [5]. Sensors, AI and effectors are becoming one sovereign loop, in which the decisive quantity is the time — and the trust — with which an observation becomes an effect.

Acknowledgment

The Vlatacom Institute of High Technologies funded this work through its projects VMSIS3_Advanced and AI-DECIDE. Passive acoustic sensing was developed jointly with the School of Electrical Engineering, University of Belgrade.

References

[1] HOLLENBECK,N., ALTAF,M.H., AVILA,F., RAMIREZ,J., SHARMA,A., JENSEN,B.: *Calculating the Cost-Effectiveness of Russia's Drone Strikes*, Center for Strategic and International Studies, Washington, DC, 2025.

[2] WATLING,J., BRONK,J.: *Protecting the Force from Uncrewed Aerial Systems*, RUSI Occasional Paper, Royal United Services Institute, London, 2024.

[3] PARK,S., KIM,H.T., LEE,S., JOO,H., KIM,H.: *Survey on Anti-Drone Systems: Components, Designs, and Challenges*,

IEEE Access, 9 (2021) 42635–42659.

[4] GUVENC,I., KOOHIFAR,F., SINGH,S., SICHITIU,M.L., MATOLAK,D.: *Detection, Tracking, and Interdiction for Amateur Drones*, IEEE Communications Magazine, 56(4) (2018) 75–81.

[5] XU,L., LUO,Z.: *Anti-UAV Detection and Identification Technology: Fundamentals, Methods and Challenges*, Physical Communication, 71 (2025) 102676.

[6] U.S. DEPARTMENT OF DEFENSE: *Strategy for Countering Unmanned Systems*, Washington, DC, 2024.

[7] VULIC,I.: *Introduction to Command-Information Systems*, in: Command-Information Systems, University of Defence, Belgrade, 2026 (in Serbian).

[8] VUJIC,S., PERIC,D., LIVADA,B., RADISAVLJEVIC,M., DOMAZET,D.: *Optical Protective Window Design and Material Selection Issues in the Multi-Sensor Electro-Optical Surveillance Systems*, Sensors, 23 (2023) 7211.

[9] PERIC,D., LIVADA,B., PERIC,M., VUJIC,S.: *Thermal Imager Range: Predictions, Expectations, and Reality*, Sensors, 19 (2019) 3313.

[10] PAVLOVIC,M., BANJAC,Z., KOVACEVIC,B.: *Object Tracking in SWIR Imaging Based on Both Correlation and Robust Kalman Filters*, IEEE Access, 11 (2023).

[11] CIZELJ,D., PAVLOVIC,M., UNKASEVIC,T., BANJAC,Z.: *Automated Target Tracking Activation Based on Motion Detection*, Proc. 10th Int. Conf. on Electrical, Electronic and Computing Engineering (IcETRAN), East Sarajevo, 2023.

[12] NIKOLIC,D., STOJKOVIC,N., PUZOVIC,S., POPOVIC,Z., STOJILJKOVIC,N., GRBIC,N., ORLIC,V.: *Increasing Maritime Safety and Security in the Off-Shore Activities with HFSWRs as Primary Sensors for Risk Assessment*, Journal of Marine Science and Engineering, 11 (2023).

[13] PETROVIC,P., GRBIC,N., LEKIC,N., PERIC,M., SAVIC,S.: *Aircraft Detection Range for HF Radar*, Proc. 31st Telecommunications Forum (TELFOR), Belgrade, 2023.

[14] POPADIC,I., PERIC,M., TOMIC,B., SIMIC,A., MILANOVIC,P.: *High-End Video Processing Platform for Electro-Optical Systems*, Proc. 9th International Scientific Conference on Defensive Technologies (OTEH), Belgrade, 2020.

[15] FARLIK,J., KRATKY,M., CASAR,J., STARY,V.: *Multispectral Detection of Commercial Unmanned Aerial Vehicles*, Sensors, 19(7) (2019) 1517.

[16] TAHA,B., SHOUFAN,A.: *Machine Learning-Based Drone Detection and Classification: State-of-the-Art in Research*, IEEE Access, 7 (2019) 138669–138682.

[17] GOLUBOVIC,D., ERIC,M., VUKMIROVIC,N., ORLIC,V.: *High-Resolution Sea Surface Target Detection Using Bi-Frequency High-Frequency Surface Wave Radar*, Remote Sensing, 16 (2024).

[18] KASCA,L., PAVLOVIC,D.S., BJELIC,M., NESKOVIC,DJ., MARKOVIC,M.: *Underwater Model for Acoustic Waves Propagation*, Proc. 23rd International Symposium INFOTEH-JAHORINA, IEEE, 2024.

[19] GHENESCU,M.T., GHENESCU,V., CARATA,S.V.: *Acoustic Source Drone Detection System Using Tetrahedral Microphone Array and Deep Neural Networks*, Sensors, 26(6) (2026) 1778.

[20] PRODANOVIC,R., RANCIC,D., VULIC,I., ZORIC,N., BOGICEVIC,D., OSTOJIC,G., SARANG,S., STANKOVSKI,S.: *Wireless Sensor Network in Agriculture: Model of Cyber Security*, Sensors, 20(23) (2020) 6747.

[21] PRODANOVIC,R., SARANG,S., RANCIC,D., VULIC,I., STOJANOVIC,G.M., STANKOVSKI,S., OSTOJIC,G., BARANOVSKI,I., MAKSOVIC,D.: *Trustworthy Wireless Sensor Networks for Monitoring Humidity and Moisture Environments*, Sensors, 21(11) (2021) 3636.

[22] HALL,D.L., LLINAS,J.: *An Introduction to Multisensor Data Fusion*, Proceedings of the IEEE, 85(1) (1997) 6–23.

[23] MOSTAFA,M.A.R.M., VUCETIC,M., STOJKOVIC,N., LEKIC,N., MAKAROV,A.: *Fuzzy Functional Dependencies as a Method of Choice for Fusion of AIS and OTHR Data*, in: Smart Sensors and Devices in Artificial Intelligence, Springer, Basel, 2022.

[24] ILIC,N., VUCETIC,M., MAKAROV,A., PETROVIC,R., PUNT,M.: *Adaptive Asynchronous Gossip Algorithms for Consensus in Heterogeneous Sensor Networks*, IEEE Internet of Things Journal, 12 (2025).

[25] CLARK,B., PATT,D., SCHRAMM,H.: *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations*, Center for Strategic and Budgetary Assessments, Washington, DC, 2020.

[26] CLARK,B., PATT,D., SERAPHIN,A., MILES,W.: *Integrated by Mission — Federated for Execution*, Hudson Institute, Washington, DC, 2024.

[27] VULIC,I., PRODANOVIC,R., TOT,I., BOGICEVIC,D.: *Model for Authenticating the Internet of Military Things and Internet of Battlefield*, Proc. 10th Int. Conf. on Information Society and Technology (ICIST), Kopaonik, 2020, 206–210.

[28] PRODANOVIC,R.I., VULIC,I.B.: *Model for PKI Interoperability in Serbia*, Vojnotehnicki glasnik / Military Technical Courier, 65(2) (2017) 530–549.

[29] VULIC,I., PRODANOVIC,R., VUKCEVIC,G., SRETENOVIC,S.: *Trust Establishing Model in IoT Using PKI and Timestamp*, Proc. 8th Int. Conf. on Information Society and Technology (ICIST), Kopaonik, 2018, 333–338.

[30] ROTHE,J., KESSLER,N., HENRIQUEZ WEHR,M., HOHBACH,A., STROHMEIER,M., MONTENEGRO,S.: *Autonomous Drone-on-Drone Interception Using an Integrated LiDAR–Vision Detection System for High-Precision Capture*, Drones, 10(6) (2026) 420.

[31] MILANOVIC,P., POPADIC,I., KOVACEVIC,B.: *Gyroscope-Based Video Stabilization for Electro-Optical Long-Range Surveillance Systems*, Sensors, 21 (2021) 6219.

[32] PYLE,F.: *Operations in the Red Sea: Lessons for Surface Warfare*, Center for Strategic and International Studies, Washington, DC, 2024.