ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/ 10.47459/cndcgs.2026.24**

Protection against UAVs in the Environment of Hybrid Warfare

Jaroslav TUREČEK[1]*, Zbyšek KORECKI[1]

[1]*Department of Security management, AMBIS University, Lindnerova 575/1, 180 00 Prague, Czech Republic*

*Correspondence:*jaroslav.turecek@ambis.cz*

Abstract

The aim of this article is to propose a functional categorisation of counter-drone measures based on an analysis of selected technical and operational aspects of UAV (Unmanned Aerial Vehicles) protection for critical infrastructure and soft targets in hybrid conflicts. Traditional UAV protection approaches based primarily on legislative regulation and UAV cooperation are necessary but insufficient. Problematic are non-cooperative drones, especially autonomous systems. Emphasis is given to active protection and hard-kill solutions.

KEY WORDS: *Counter-UAS; hybrid warfare; critical infrastructure protection; cooperative and non-cooperative UAVs; hard-kill systems*

Citation: Tureček, J.; Korecki, Z. Protection against UAVs in the Environment of Hybrid Warfare. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, https://doi.org/ 10.47459/cndcgs.2026.24

1. Introduction

The Unmanned Aerial Vehicles (UAVs; drones), or more broadly Unmanned Aerial Systems (UAS have significantly altered the security environment, particularly in the context of hybrid warfare. UAVs are increasingly employed not only for reconnaissance but also for direct offensive operations against critical infrastructure and soft targets.

Traditional UAV protection approaches based primarily on legislative regulation and voluntary operator cooperation are necessary but insufficient [1]. Problematic are non-cooperative drones, especially autonomous systems used by both state and non-state actors.

The aim of this paper is to analyze selected technical and operational aspects of UAV protection in hybrid conflicts and, based on this analysis, to propose a functional categorization of protection measures suitable mainly for the defense of critical infrastructure and soft targets, with emphasis on active protection and hard-kill solutions.

2. Terminology and categorization issues in UAS protection

Scientific articles on drone protection in Europe, in the period before the open aggression of Russia against Ukraine, focused predominantly on the safety of UAS operations [1]. With the increasing importance of drones both in this conflict and in various forms of hybrid attacks, the focus of research has shifted to the field of C-UAS (Counter-Unmanned Aircraft Systems) [2]. Protection against drones is therefore currently the subject of extensive professional discussion. Individual publications often introduce their own terminology (nomenclature) in the field of drone protection, which is methodologically legitimate. The problem, however, is significant inconsistency: different terms are used to denote the same phenomena (concepts), while identical terms are used with different meanings across different sources.

At the same time, most publications do not deal with a comprehensive functional categorisation of UAS protection or formal protection models; rather, they tend to describe the operational sequence of C-UAS functions (e.g. detection, tracking, identification, mitigation/neutralisation), rather than a systematic classification of protection measures.

Given the scope limitations of this paper, it is not possible to perform a detailed analysis of a broader spectrum of publications. The authors therefore focus on current documents of relevant EU and UN organisations, whose terminology should represent a reference framework for further research.

The document United Nations – Guidelines on Counter Unmanned Aircraft Systems [3] attempts to define "UN-recognized terminology". It does not address the safety of UAS operations at all and focuses solely on protection against non-cooperative drones, which it refers to using the widely established term C-UAS. It presents a relatively clear functional structure of C-UAS, distinguishing four basic system functions: Detection, Tracking, Identification and Mitigation. According to the document, the last category includes two groups of measures: *Passive measures* (e.g. camouflage, concealment, deception, dispersion of forces, hardening or shelters) and *Active measures* (both soft-kill and hard-kill). The use and definition of the terms Active measures, with division into *soft-kill* and *hard-kill*, and especially the introduction of the term Passive measures, excellently reflect decades-established military terminology, known primarily from the protection of tanks and armoured vehicles in general. These terms are relatively clearly understood within the expert community. Among EU documents, only Hansen Pinto Faria [2] adopts a similar approach, using the terms Soft Mitigation and Hard Mitigation, which together form Neutralisation. Passive Measures are then referred to as Physical Protection. Apart from not addressing operational safety, the only question raised by the UN document is whether the term "mitigation" should have a broader meaning, as in the EU document by Hansen Pinto Faria [2], or a narrower one as in [4].

The document EUROCAE – ED-286 Operational Services and Environment Definition for Counter-UAS in Controlled Airspace [4] focuses on C-UAS in the context of controlled airspace. It understands protection against UAS primarily as part of integration into the air traffic management system, rather than as a separate field of object protection. The document does not contain a comprehensive protection model but works with an operational sequence of functions: Detection – Tracking – Identification – Mitigation/Neutralisation. This sequence represents a functional flow of operations, not a categorisation of protection measures. Unlike the UN document [3] or the JRC EU document [2], the document does not introduce terms such as active/passive measures or soft-kill/hard-kill. The term "mitigation" is used in a narrower, technical sense. From a terminological perspective, the main issue is the absence of a clear distinction between safety and security and the lack of a general protection model. The document thus provides an accurate description of C-UAS functions, but not their systematic categorisation.

The JRC EU document by Poppinga et al. [5] focuses primarily on the functional domain of DTI (Detection, Tracking and Identification) and does not represent a comprehensive model of UAS protection, but rather an operational flow of C-UAS system functions. This flow includes a sequence of steps from detection through localisation, tracking, classification and identification to decision-making and possible neutralisation, with individual functions occurring cyclically. Instead of the terms soft + hard kill, it uses the term neutralisation. The term mitigation is used in connection with passive protection, "to move target to safe area". Document [5] uses the term "C-UAS protection", which results in mixing concepts denoting an activity (C-UAS) and an outcome (protection). From a terminological standpoint, it is cleaner to understand C-UAS as a subset of measures within the broader concept of "UAS protection".

The JRC EU document by Hansen [2] distinguishes between a C-UAS system (an individual technical means) and a C-UAS solution (a comprehensive whole including systems, processes and actors). In terms of broader terminology, the document works with the pair of terms *safety and security*. For protection in an environment of cooperative UAS (i.e. with cooperation), it uses the designation "Safety of UAS traffic", which corresponds to operational safety. In contrast, for protection against non-cooperative UAS, it uses the designation C-UAS, which it defines as "securing a site against non-cooperative UAS", i.e. protection in the sense of security. Through this distinction, the document clearly separates the domain of operational safety from the domain of protection against threats and at the same time terminologically anchors the concept of C-UAS as a specific subset of UAS protection. The document uses the term "*monitoring*" to refer to DTI (Detection, Tracking and Identification).

The JRC EU document by Karlos [6] represents a practically oriented handbook focused on physical protection measures (physical hardening) for the protection of buildings, critical infrastructure and public spaces against threats associated with UAS, with its main contribution being the linkage with risk analysis. The Karlos document [6] complements the Hansen document [2] in parallel, and these documents refer to each other. For Soft Kills it uses the designation "non-kinetic interception systems", and for Hard Kill "kinetic-interception technologies" (incl. DEW + nets).

The differences in terminology in the above-mentioned documents are so numerous that they cannot be clearly described in a continuous text and are presented more clearly in Tables 1 and 2. In the left columns are the designations proposed by the authors, which resulted from the analysis and subsequent synthesis of the functional categorisation. In the other columns are the designations used in the above-mentioned documents. These designations are either explicitly defined in the respective documents or represent the designations that best follow from the given text. If it followed from the text that a given category (given designation) is a subset of a broader category, this is indicated in the tables.

As can be seen from the tables, the inconsistency of terminology is considerable. Since these are definitions, it is not, in principle, appropriate to describe them as incorrect. However, some definitions and the associated classification of certain categories are less suitable and can even be confusing for the reader. For example, the classification of Physical protection under Soft mitigation [2] is confusing, given the generally widespread and decades-established concepts of passive and active protection, as well as the already widely used term Soft Kill.

Not all documents also pay attention to the basic categorisation, well established in the field of object protection, into safety and security.

Table 1.

Review of UAS protection terms

Proposed designation		[10] UN	[30] EUROCAE	[12] Poppinga Anderson Amendola
UAS protection	designation	-	-	C-UAS protection
UAS protection with UAS cooperation (UAS safety)	designation	-	„safe integration of UAS into the airspace system“	physical hardening
	subset of	-	-	prevention
UAS protection without UAS cooperation (C-UAS; UAS security)	designation	C-UAS	C-UAS	C-UAS (C-UAS protection)
	subset of	-	-	-
Passive protection/ passive C-UAS	designation	Passive measures[1]	-	a) physical hardening b) mitigation (to move target to safe area)
	subset of	Mitigation	-	a) prevention b) netralisation/mitigation
Active protection/ active C-UAS	designation	Active measures	C-UAS	neutralisation
	subset of	Mitigation		-
Detection (DTI)	designation	detection, tracking and identification	Global Detection	DTI
	subset of	-	-	-
Detection	designation	Detection	Initial Detection	Detection
Traking	designation	Tracking	Tracking	Tracking (localisation over time)
Identification	designation	Identification	Identification	a) Identification b) Classification or Identification
Soft + Hard Kill	designation	soft kill and hard kill options	Mitigation/Neutralisation	Neutralisation
	subset of	Mitigation	-	-
Soft kill	designation	soft kill options	-	-
	subset of	-	-	-
Hard kill	designation	hard kill options	-	-
	subset of	-	-	-
functional model of UAS protection		C-UAS Framework: detect, track, identify, and mitigate	Operational sequence of C-UAS functions, not a protection model, kill chain	C-UAS protection model: Cyclic process

Table 2.

Review of UAS protection terms

Proposed designation		[2] Hansen Pinto Faria	[11] Karlos Larcher
UAS protection	designation	Mitigation (of UAS threat); Protection against UAS	Physical hardening + C-UAS
UAS protection with UAS cooperation (UAS safety)	designation	Safety of UAS traffic	Physical hardening + C-UAS
	subset of	Mitigation of UAS threat	
UAS protection without UAS cooperation (C-UAS; UAS security)	designation	C-UAS (securing a site against non-cooperative UAS)	
	subset of	Mitigation of UAS threat	Physical hardening + C-UAS
Passive protection/ passive C-UAS	designation	Physical protection	Physical hardening
	subset of	C-UAS / Soft mitigation	Physical hardening
Active protection/ active C-UAS	designation	neutralisation	C-UAS
	subset of	C-UAS	C-UAS
Detection (DTI) (monitoring)	designation	Monitoring (monitoring/ prevention)	detection, tracking and identification
	subset of	C-UAS (< mitigation)	C-UAS
Detection	designation	Detection	Detection
	subset of	monitoring	-
Traking	designation	Tracking	Tracking
	subset of	monitoring	-
Identification	designation	Identification	Identification
	subset of	monitoring	-
Soft + Hard Kill	designation	Neutralisation	-
	subset of	C-UAS (< mitigation)	-
Soft kill	designation	Soft mitigation	non-kinetic interception systems
	subset of	neutralisation	-
Hard kill	designation	Hard mitigation	kinetic-interception technologies *(incl. DEW+nets)*
	subset of	neutralisation	-
functional model of UAS protection		-	-

3. Investigation results - Functional categorisation of UAS protection

Based on the *analysis* of selected operational and technical aspects of UAS protection in hybrid conflicts, a *functional categorisation* of protection measures suitable mainly for the defence of critical infrastructure and soft targets, with emphasis on active protection and hard-kill solutions, has been proposed. This categorisation was subsequently slightly modified with regard to the above-mentioned documents. The resulting functional categorisation is shown in the following figure:

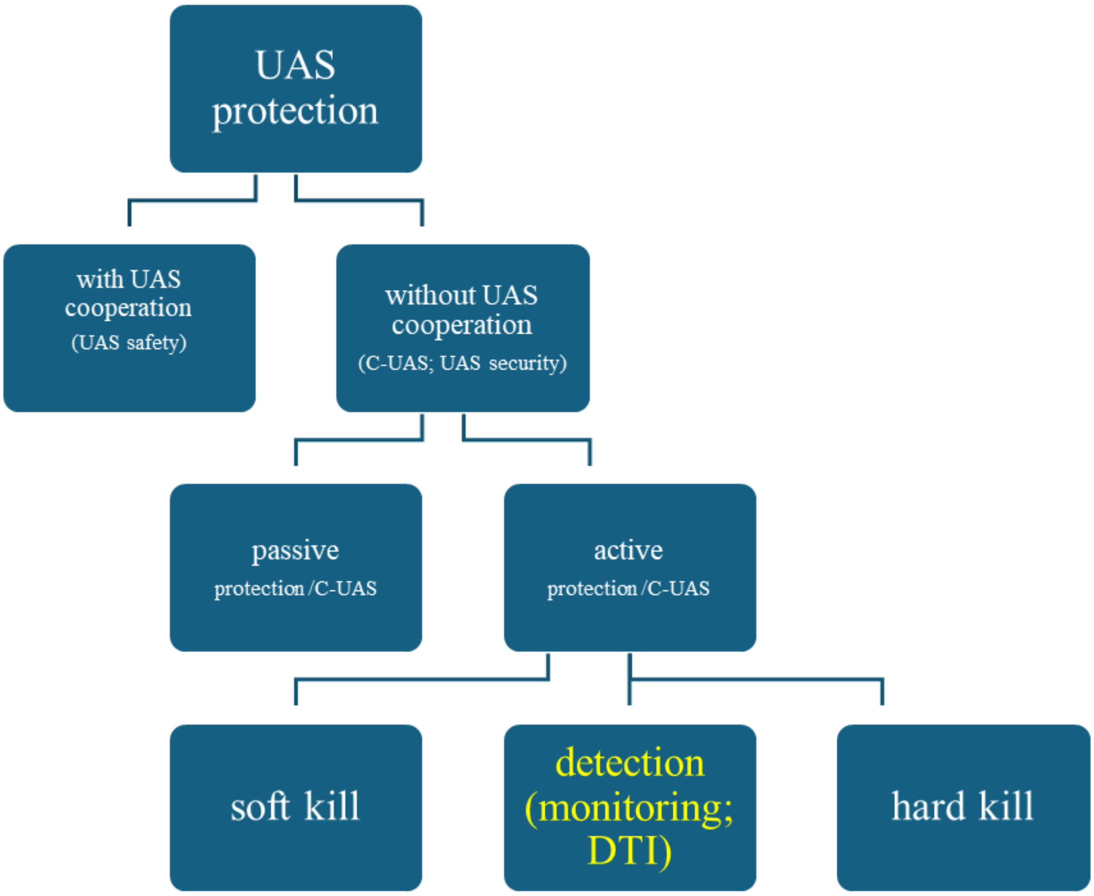

Fig. 1. Functional categorization of UAV protection.

3.1 Protection systems with cooperation with drones (UAS safety; UTM)

In the EU, the emerging UAS Traffic Management (UTM) systems essentially represent administrative protection of selected objects against cooperative drones. These systems assume cooperation of the entire or at least part of the chain manufacturer – distributor – operator – pilot with regulatory authorities:

a) Remote identification system – a system for remote identification, an identification e-system of an unmanned aircraft ("e-identification")

b) Geo-awareness system ("geo-fencing") – warns the remote pilot (or autopilot) about possible violation of a prohibited geographical zone for a given drone

It can be assumed that in higher implementation phases of U-space, UTM will not rely only on position data of individual drones transmitted by the drones themselves, but that U-space will be monitored by high-resolution radars, possibly cameras and other optical devices. These detection means will then be able to detect non-cooperative drones and provide data to active drone elimination systems.

3.2 Protection systems without cooperation with drones (C-UAS; UAS security)

Regulatory frameworks, traffic management and technologies cooperating with drones are a necessary foundation for the protection of important objects against drones, but they are absolutely insufficient for protection against non-cooperative drones. In such cases, it is necessary either to defend passively or, preferably, to actively eliminate the drones. Extensive knowledge can be drawn from the defence of Ukraine against Russian aggression. This is despite the fact that standard C-UAS scenarios for the protection of critical infrastructure and soft targets [7] differ in some aspects.

3.3 Passive protection against drones (passive C-UAS)

Passive protection against drones does not attack the drone, does not interfere with the drone's operation, and certainly does not affect the drone itself; instead, it aims to conceal the protected object from the drone and primarily seeks to withstand a potential drone strike and thereby protect the object or at least mitigate the consequences.

3.4 Active protection against drones (active C-UAS)

Active protection against drones is divided into "soft kill" and "hard kill" protection. Both types of protection, soft kill mostly and hard kill always, require detection means (including identification and tracking).

3.5 Detection of drones (UAS monitoring; DTI)

As mentioned above, active protection against drones requires detection means in the broader sense, i.e. drone monitoring systems. This monitoring consists of detection (in the narrower sense), tracking and identification of drones, collectively referred to as DTI (Detection, Tracking and Identification) [2, 8]. It is therefore appropriate to distinguish between the broader and narrower meanings of the term "drone detection". In the narrower sense, detection represents the mere recognition of the presence of an object. In the broader sense, however, it also includes subsequent processes of determining position over time (tracking) and at least basic classification or identification of the object. In practice, most detection means provide information about the position of an object with a certain accuracy and at the same time allow at least basic differentiation of the target type (e.g. bird, debris, drone, possibly type of drone). More advanced means, especially in the field of electronic identification, may also allow unambiguous identification of a specific drone. From this it follows that detection in the broader sense effectively includes elements of tracking and identification.

3.6 Active drone monitoring

Active drone detection systems emit various forms of energy into the surrounding space and receive reflections of this radiation from objects in the environment.

a) Radiolocation: RADAR (RAdio Detection And Ranging) transmits radio waves into space and receives a portion of these waves reflected back from objects, subsequently processing the received signals. It can determine the direction, distance, speed of the object, as well as various characteristics of the target.

b) Lidar-based (2D LIDAR; 3D LIDAR): LIDAR (Light Detection and Ranging) is a remote sensing technology that uses pulses of laser light to measure distances and create precise 3D (3D LIDAR) maps of the environment.

3.7 Passive drone monitoring

Passive drone detection systems do not emit energy into the surrounding space in any form but only receive various forms of energy emitted by UAS.

a) Optical and thermal (EO/IR – Electro-Optical / InfraRed): Electro-optical cameras (without imaging thermal radiation of objects) capture light from natural illumination of the scene reflected from objects, primarily in the visible spectrum and possibly also in the near-infrared range. Thermal cameras (thermal imaging; thermal IR) display radiation in the range of 2–15 μm, i.e. in the regions of maximum thermal emission of persons, running engines, etc.

b) Detection of RF communication of drones (RF-DF; passive radars): Detects RF communication of drones. It usually also determines direction and is then referred to as RF-DF (Radio Frequency – Direction Finding). If this direction is determined from multiple positions using several receivers, it constitutes a so-called passive radar.

c) Acoustic: Detects acoustic signatures of flying drones, in the case of battery-powered drones primarily the sound of rotating propellers. Area acoustic detection has found significant application in detecting the operation of combustion engines of drones such as the Shahed type [9], but is also used for detecting small drones such as FPV types, etc.

3.8 Active protection systems of the soft-kill type

Soft-kill means do not involve direct physical (material) damage to the drone or its control system, but disrupt the drone's information processing, specifically its observation, detection, navigation, communication, computational, decision-making and control processes. Soft-kill means include:

a) RF communication jamming of drones: A jammer (jammer, “RF inhibitor” or “RF effector”) disrupts communication channels between the drone and the ground pilot, either direct or via a relay. From the drone to the pilot, this mainly includes video transmission as well as data on position, battery status, etc. From the pilot to the drone, these are mainly flight control commands. Jammers can be omnidirectional or directional. Another classification distinguishes stationary, mobile, portable (e.g. omnidirectional jammer in backpack form) and handheld devices (typically anti-drone guns).

b) RF cyber takeover (RF Cyber takeover, Cyber takedown, “RF cyber technology” or “Electronic attack”): These means hack control over the drone and take over its operation. They are mainly effective against commercial, unmodified drones.

c) Navigation signal jamming (GPS jamming): These means disrupt navigation signals (GPS, Galileo, GLONASS)

d) Navigation signal spoofing (GPS spoofing): These means provide the drone with false position data.

Soft-kill measures, including communication and navigation jamming and cyber takeover, currently remain dominant in internal security applications [2, 22]. However, due to fibre-optic guidance and AI-based autonomous navigation, the importance of hard-kill protection is increasing.

3.9 Active protection systems of the hard-kill type

Hard-kill means physically attack the drone, destroy it or at least damage it and thereby limit its ability to harm the protected target. These include:

a) Machine guns and rapid-fire cannons against drones: Machine guns and rapid-fire cannons belong to classical short-range air defence systems (SHORAD – SHOrt Range Air Defense). For effectiveness against drones, their placement on automated weapon stations is essential. In the case of cannons, the use of airburst munitions (ABM) is also necessary.

b) Surface-to-air guided missiles: Ground-based air defence guided missiles (SAM systems) also belong to classical air defence systems. They typically use rocket propulsion and guidance systems such as infrared, laser or radar (active or semi-active).

c) Lasers: Combat lasers (“Light Amplification by Stimulated Emission of Radiation”) irradiate the drone for a short period with a high-power laser beam.

d) Microwave weapons: Microwave hard-kill means (HPM – High Power Microwave) emit strong electromagnetic pulses (EMP) in the microwave spectrum, capable of disrupting electronic devices of drones. EMP disrupts or even destroys electronic circuits inside drones through damaging voltages and currents induced in the electronics.

Lasers and microwave weapons fall into the category of Directed Energy Weapons (DEW). DEW destroy drones using various forms of energy, practically exclusively electromagnetic, directed at the drone(s). Directed Energy Weapons remain constrained by availability and collateral damage concerns and are unlikely to be widely deployable in the near term [10, 11].

e) Net weapons: Nets neutralise a drone by immobilising rotor blades. There are three main delivery methods: ground-based net guns (also “net cannons”; handheld; shoulder-fired; mounted), net guns mounted on interceptor drones, and suspended nets carried by interceptor drones. In all three methods, the net may be equipped with a parachute for partially controlled descent. In the case of suspended nets, the parachute is particularly useful when the captured drone is too heavy. Net systems appear particularly suitable for protecting critical infrastructure in internal security contexts.

f) Interceptor drones: Interceptor drones are typically powered by electric propellers, occasionally by more expensive turbines. Against slower drones such as FPV types, FPV drones are also used as interceptors. Against faster fixed-wing drones, interceptor designs combining multirotor take-off with fixed-wing flight are more effective. These drones take off (and possibly land) as quadcopters, but after gaining speed they utilise fixed wings, allowing propulsion power to be concentrated on forward thrust. They may also use auxiliary rocket motors for rapid ascent to altitudes of several kilometres.

Historically, the first and still probably the most common method of neutralising an enemy drone is simple ramming by an interceptor drone. Interceptor drones may also destroy the target by firing recoilless weapons, using specialised guided missiles, capture nets or similar capture mechanisms, including microwave-based methods. In such cases, it appears more appropriate to describe the means of destruction primarily as the interceptor drone itself, e.g. “neutralisation by interceptor drone”, and only subsequently specify the method (e.g. “neutralisation by interceptor drone using guided missiles”).

4. Conclusions

The proposed functional categorisation of UAS protection of critical infrastructure and soft targets in hybrid conflicts is based on a systematic analysis of selected operational and technical aspects of UAS protection. Given the existing terminological inconsistency in the field of UAS protection, the proposed terminology is not intended to be normatively binding. Rather, it is conceived as a functionally oriented and open framework that allows, where justified, the parallel use of one to three equivalent terms for the same meaning, in order to maintain compatibility with different professional and institutional approaches.

For the protection of critical infrastructure within internal security, a rapidly evolving range of active counter-drone neutralisation systems is available, primarily originating from the military domain. The foundation of internal security remains regulation and protection based on voluntary–mandatory cooperation of drones. However, the possibility of attacks by purely hostile drones must not be overlooked, and legislation must enable active protection. Due to the possibility of fibre-optic control of drones and especially the rise of autonomous drones, the importance of soft-kill measures is decreasing, while the emphasis shifts toward hard-kill solutions. A major challenge for the deployment of active hard-kill protection in internal security will be ensuring that third parties are not endangered during intervention. These conditions are best met by interceptor drones equipped with capture nets. Future research should focus on integrating individual protection elements into layered C-UAS systems [12,13] and on addressing legal and safety issues related to their deployment in civilian environments.

Acknowledgements. The paper was prepared on behalf of AMBIS University, and the authors would like to thank the institution for its support.

References

1. **Konert A., Dunin T.** A Harmonized European Drone Market? – New EU Rules on Unmanned Aircraft Systems. In: Advances in Science, Technology and Engineering Systems Journal, Volume 5, Issue 3, Page No 93-99, 2020 DOI: 10.25046/aj050312.
2. **Hansen P., Pinto Faria R.** Protection against Unmanned Aircraft Systems, Anderson, D., Meersman, B., Karlos, V. and Larcher, M. editor(s), Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/18569, JRC132714.
3. **United Nations** Guidelines on Counter Unmanned Aircraft Systems. United Nations Department of Operational Support; Department of Peace Operations, 2025. Ref. 2025.16.
4. **European Organization for Civil Aviation Equipment** EUROCAE ED-286: Operational Services and Environment Definition for Counter-UAS in Controlled Airspace, ed. 21, p. 54, 2021
5. **Poppinga G., Anderson D., Amendola D.** Technical developments in counter-drone technology: C-UAS detection, tracking and identification technology - Annual report, Publications Office of the European Union, Luxembourg, 2025, 10.2760/1517220
6. **Karlos V., Larcher M.** Protection against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/969680, JRC132967
7. **Petsioti P., Życzkowski M., Brewczyński K., Cichulski K., Kamiński K., Razvan R., Mohamoud A., Church C., Koniaris A., De Cubber G., Doroftei D.** Methodological Approach for the Development of Standard C-UAS Scenarios. Open Research Europe, 2024, 4. 240. doi: 10.12688/openreseurope.18339.1.
8. **Brewczyński K., Życzkowski M., Cichulski K., Kamiński K., Petsioti P., De Cubber G.** Methods for Assessing the Effectiveness of Modern Counter Unmanned Aircraft Systems. Remote Sensing, 2024, 16. 3714. 10.3390/rs16193714
9. **Заріцький O., Ponomarenko O.** Intelligent Analysis of Sound Patterns of Unmanned Aerial Vehicle Engines in the Tasks of C-UAS Systems Development. International Journal of Computing, 2025, p. 387-396. 10.47839/ijc.24.2.4023
10. **Horváth G.** No Drone's Sky: Full Spectrum Drone Surveillance and Neutralisation Concept for Enhanced Counter-UAS Framework, (Part 2, Neutralisation). Military Engineer, 2024, 19 (2), p. 107–121. 10.32567/hm.2024.2.9
11. **Wang J., Liu Y., Song H.** Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends. IEEE Aerospace and Electronic Systems Magazine, 2021, 36. p. 4-29. 10.1109/MAES.2020.3015537.
12. **Grigoraş C., Octavian Ș. M.** "Integrating Artificial Intelligence Into C-UAS Systems to Match the Modern Warfare Advancements" Land Forces Academy Review, 2025, vol. 30, no. 2, Nicolae Balcescu Land Forces Academy, p. 269-276. 10.2478/raft-2025-0026
13. **Son I., Park S.** Designing Hyper-Connected Interoperable Functions for Integrated C-UAS System of National Critical Facilities. International Journal of Advanced Culture Technology, 2024, 12(4), p. 302–309. 10.17703/IJACT.2024.12.4.302