

Krisztián Végh<sup>1</sup> 

# Issues of Countering Unmanned Aircraft Vehicles Concerning Deployed Forces

*The rapid proliferation and increasing accessibility of unmanned aerial vehicles (UAVs) have significantly transformed the threat environment of deployed military forces. Military camps, as predominantly static and spatially extensive installations, have become particularly vulnerable to UAV-based reconnaissance and attack capabilities. This paper argues that the drone threat affecting military camps cannot be considered homogeneous, as it is fundamentally shaped by the differing functions, military value, and vulnerability of internal functional zones. Building on the NATO Deployed Force Infrastructure concept, the study examines military camps as complex systems composed of service and accommodation zones. Different types of UAV threats are capable of exerting negative effects on areas designated for the accommodation and support of deployed forces in distinct ways; therefore, a zone-based theoretical framework for C-UAS2 detection and mitigation requirements is necessary.*

**Keywords:** military camp, drone threat, C-UAS, infrastructure

## Introduction

The technological advancement of UAVs and their widespread accessibility have fundamentally transformed the character of modern warfare. The employment of UAVs is no longer the exclusive privilege of state actors possessing high technological capabilities; owing to their low cost, ease of operation and rapid adaptability, they have also become accessible to nonstate actors. As a result, the threat posed by drones has emerged as one of the defining challenges of force protection, including in the case of deployed military forces.

A defining characteristic of military camps is that they are typically static or only limitedly relocatable installations, operating within the same geographical area for extended periods. This inherent static nature provides the adversary with opportunities for gradual reconnaissance, identification of operational patterns, and the preparation of targeted attacks.

---

<sup>1</sup> PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: [vegh.krisztian1@gmail.com](mailto:vegh.krisztian1@gmail.com)

<sup>2</sup> C-UAS: Counter-Unmanned Aerial Systems.

The employment of drones in this environment is particularly effective, as they are capable of conducting persistent surveillance, delivering precision strikes, and generating psychological as well as information effects.

A significant portion of NATO regulations or recommendations<sup>3</sup> on C-UAS currently available supports efforts to counter the drone threat in the context of FP<sup>4</sup> primarily through the formulation of general recommendations. However, military camps do not constitute homogeneous point targets. In accordance with relevant NATO doctrine, and consistent with technical and professional considerations, military camps comprise areas with different functions, which possess varying military value, differing levels of vulnerability and distinct threat profiles. The impact of an UAV attack against an energy generation or infocommunications facility fundamentally differs from an attack against a residential or recreational zone, in physical, operational and psychological terms.

This study is based on the assumption that effective counter-drone protection of military camps can only be achieved if both the threat and the defensive measures are interpreted in a functionally differentiated manner. To this end, drawing on the concept of Deployed Forces Infrastructure, the study examines military camps as complex systems that can be subdivided into service and accommodation zones. The objective of the study is to develop a theoretical framework that links the functional characteristics of these zones with the forms of threats posed by drones and, on this basis, defines zone-specific requirements for drone detection and counter-UAS measures. The essence of the study lies in its approach of not examining the drone threat in isolation, but rather interpreting it in alignment with the internal structure of the military camp, thereby supporting the planning of layered, priority-driven, and operationally relevant force protection solutions.

It should be emphasised that the drone threat is not merely a technical or tactical issue, but increasingly a system-level challenge affecting the resilience, sustainability and operational tempo of deployed forces. Consequently, counter-drone protection must be interpreted not only as an air defence task, but as an integral component of force protection and operational planning.

## Drones as sources of threat

The combat employment of drones has become one of the most dynamically evolving domains of warfare over recent decades. The pace of this development has been driven not primarily by state-sponsored development programmes, but rather by battlefield innovation, improvisation, and the rapid adaptation of commercially available technologies.<sup>5</sup> As highlighted by previous studies, drones have by now emerged in the operational environment not merely as auxiliary assets, but as independent military capabilities.

---

<sup>3</sup> NATO Standard ATP-117 Countering Class I Unmanned Aircraft Systems (UAS) Doctrine, Edition A.

<sup>4</sup> FP: Force (and asset) Protection.

<sup>5</sup> VÉGH 2024.

One of the most significant characteristics of drone development is the rapid expansion of functional diversity. Initially, the employment of drones was primarily limited to reconnaissance and surveillance tasks, in which the role of the “flying sensor” was dominant. The capability for real-time imagery transmission has fundamentally altered tactical-level situational awareness, complicating the covert concentration of forces, the achievement of surprise, and the concealment of movements.<sup>67</sup> This capability, due to its particularly low cost and ease of operation, has also rapidly become widespread among nonstate actors.

The next stage of development was marked by the emergence of strike capabilities, which are predominantly associated with the use of COTS<sup>7</sup> drones as improvised weapons. During the activities of the Islamic State, the employment of aerially delivered improvised explosive devices became widely known. These initially appeared in the form of simple dropped grenades and later evolved into increasingly sophisticated explosive charges.<sup>8</sup> The procedures developed through this learning process demonstrated that even small explosive charges are capable of producing significant tactical and psychological effects, particularly against concentrated personnel or unfortified infrastructure.

FPV<sup>9</sup>-based OWA<sup>10</sup> drones have emerged, representing an extremely challenging threat to defend against due to their high speed, excellent manoeuvrability and low detectability. These systems can essentially be interpreted as simplified, improvised variants of loitering munitions, combining certain characteristics of conventional weapon systems with the advantages of COTS technology.

During the Palestinian–Israeli conflict, the employment of drones already appeared as an obvious solution, although it did not, in essence, represent a new qualitative shift. Among the systems employed by Hamas and other Palestinian militias, drones equipped with anti-armour warheads also emerged, which – by exploiting top-attack profiles – were capable of circumventing traditional armoured protection measures.

Another important characteristic of this evolution is the system-level employment of drones. A drone is not merely a standalone asset, but rather a component of a broader system that includes the operator, the data link, the sensors, command, control and data-processing elements. This enables the use of drones not only for ISR<sup>11</sup> tasks and strike missions, but also for electronic warfare, deception, relay and target designation roles; furthermore, they may also serve as platforms for infantry or anti-armour weapons. These systems clearly illustrate that drones can be employed effectively not only against personnel, but also against high-value technical assets, while the required technological background has largely remained relatively accessible. During the Russo–Ukrainian War, the tactical role of drones rose to a new level. One of the most important lessons of the conflict is that the mass, routine and system-level employment of drones has become a defining feature of contemporary warfare.

<sup>6</sup> PETTYJOHN 2024.

<sup>7</sup> COTS: commercial-off-the-shelf.

<sup>8</sup> DARUKA–SZALKAI 2022.

<sup>9</sup> FPV: First Person View.

<sup>10</sup> OWA: One-Way-Attack.

<sup>11</sup> ISR: Intelligence, Surveillance, Reconnaissance.

As demonstrated by the tables, the initial capabilities of drones have undergone remarkable development. On the one hand, advancements are clearly observable in terms of range and operating altitude. On the other hand, their originally limited ISR and short-range mission sets have been expanded to include the capability to support artillery fires through target designation and target correction. Strike missions conducted by OWA drones now pose a threat to critical infrastructure<sup>12</sup> at strategic depth, while their employment has also been extended to include EW<sup>13</sup> mission sets.

Table 1: The most typical drones employed on the Russian side

| Type                 | Range (km)  | Maximum flight altitude (m) | Areas of employment                            | NATO category  |
|----------------------|-------------|-----------------------------|--|----------------|
| Orion (Inokhodets)   | 1,400 km    | 7,500                       | ISR, precise strike platform                   | Class-III MALE |
| Shahed-136 / Geran-1 | 1,500–2,000 | 4,000                       | OWA, deep strike                               | Class-II       |
| Forpost-R            | 400         | 6,000–7,000                 | ISR, deep strike                               | Class-II       |
| Korsar               | 250         | 2,000                       | EW, ISR, deep strike                           | Class-II       |
| Orlan-10             | 120         | 5,000                       | ISR, target designation, artillery support     | Class-I Small  |
| Orlan-30             | 300         | 6,000                       | ISR, target designation, artillery support     | Class-I Small  |
| Leer-3               | 120         | 5,000                       | EW, jamming comms                              | Class-I Small  |
| Eleron-10            | 50          | 3,500–4,000                 | ISR, target designation, artillery support     | Class-I Small  |
| Supercam S300/S350   | 50–100      | 1200                        | ISR, target designation, artillery support     | Class-I Small  |
| ZALA 421-16E5G       | 150         | 3,500–4,000                 | ISR, target designation, artillery support     | Class-I Small  |
| Takhion              | 40          | 4,000                       | ISR, target designation, artillery support, EW | Class-I Small  |
| Granat-4             | 55          | 2,000                       | ISR, target designation, artillery support, EW | Class-I Small  |
| Gerbera              | 300–600     | 3,000                       | ISR, OWA, Decoy                                | Class-I Small  |
| ZALA 421-16E         | 75–100      | 3,600                       | ISR, target designation, artillery support     | Class-I Mini   |

<sup>12</sup> Kovács 2024.

<sup>13</sup> EW: electronic warfare.

| Type            | Range (km) | Maximum flight altitude (m) | Areas of employment                    | NATO category |
|-----------------|------------|-----------------------------|--|---------------|
| ZALA 421-16E2   | 30         | 3,600                       | Close ISR                              | Class-I Mini  |
| ZALA 421-22     | 5-10       | 1,000                       | Close ISR                              | Class-I Mini  |
| Privet-82       | 30         | N.d.                        | LM <sup>14</sup> – smaller targets     | Class-I Mini  |
| KUB-BLA (KYB)   | 50         | 3,000                       | LM – smaller targets                   | Class-I Mini  |
| ZALA Lancet-1/3 | 40-50      | 1,000-1,500                 | LM – smaller targets, radar, artillery | Class-I Mini  |

Source: compiled by the author based on online sources and manufacturer data derived from open-source information

The capabilities of the drones employed by Ukraine – particularly from the perspective of their operational use – are largely similar to those of the opposing side. In their case as well, the pace of development is clearly perceptible. In addition to the aspects discussed above, particular attention should be paid to the LM systems of various ranges present on both sides, as well as to drones optimised for deep strike missions. Depending on the type, these systems possess autonomous target acquisition, identification and (limited) decision-making capabilities.<sup>15</sup> It is notable that the development of all these capabilities required no more than two decades.

Table 2: The most typical drones employed on the Ukrainian side

| Type               | Range (km) | Maximum flight altitude (m) | Areas of employment           | NATO category  |
|--------------------|------------|-----------------------------|-------------------------------|----------------|
| Bayraktar TB2      | 4,000      | 7,000                       | ISR, precise strike platform  | Class-III MALE |
| PD-1               | 700        | 3,000                       | ISR, target tracking          | Class-I Small  |
| R18 (Aerorozvidka) | 4-8        | 300-500                     | Strike                        | Class-I Small  |
| Mugin-5            | 800        | 3,000-4,000                 | OWA, deep strike              | Class-I Small  |
| Shark              | 80-180     | 3,000                       | EW, ISR                       | Class-I Small  |
| RAM II             | 30         | 3,000                       | LM – antitank, fortifications | Class-I Small  |

<sup>14</sup> LM: Loitering Munition.

<sup>15</sup> VÉGH-DARUKA 2025.

| Type            | Range (km) | Maximum flight altitude (m) | Areas of employment                        | NATO category |
|-----------------|------------|-----------------------------|--|---------------|
| UJ-22           | 800        | 6,000                       | ISR, OWA, deep strike                      | Class-I Small |
| Bober           | 1,000      | 5,000                       | OWA, deep strike                           | Class-I Small |
| Morok           | 800        | 4,000–5,000                 | OWA, deep strike                           | Class-I Small |
| Leleka-100      | 50–100     | 1,500                       | ISR, target designation, artillery support | Class-I Mini  |
| Furia           | 50–100     | 2,500                       | ISR, target designation, artillery support | Class-I Mini  |
| Spectator-M1    | 150        | 3,600                       | ISR, target designation, artillery support | Class-I Mini  |
| Punisher        | 45         | 400                         | ISR, target designation, artillery support | Class-I Mini  |
| Warmate         | 30         | 3,000                       | LM– anti personnel, antitank               | Class-I Mini  |
| Switchblade 600 | 40         | 4,500                       | LM– antitank                               | Class-I Mini  |
| Flyeye          | 30         | 3,000                       | Close ISR                                  | Class-I Mini  |
| Mini shark      | 45         | 7,000                       | Close ISR                                  | Class I Mini  |
| Switchblade 300 | 30         | 4,500                       | LM– anti personnel, antitank               | Class-I Micro |

*Source: compiled by the author based on online sources and manufacturer data derived from open-source information*

I believe that the development of drones is not linear, but adaptive and highly responsive to battlefield experience. Both the Palestinian–Israeli conflict and the Russo–Ukrainian War demonstrate that, due to their low cost and mass employment, drones can become a particularly dangerous threat from the perspective of deployed forces and military camps. This clearly justifies the application of zone-specific, functionally differentiated counter-drone protection approaches.

From the perspective of force protection, UAV threats can be grouped into reconnaissance-oriented, strike-oriented and hybrid (multi-role) categories. Each category generates different risk profiles in terms of detectability, warning time, potential damage and psychological effect, which must be reflected in zone-specific defensive requirements.

## The role and general characteristics of military camps

Military camps provide the fundamental physical and organisational framework for the operation of deployed forces. Their primary purpose is to create, in a concentrated manner, the conditions necessary for the accommodation, command and control, logistical support, and sustainment of military forces within a given operational area.<sup>16</sup>

A military camp should therefore not be interpreted merely as a place of accommodation, but rather as a complex facility that simultaneously supports combat, support and service activities. The purpose of military camps is essentially twofold. On the one hand, they must ensure the living and working conditions of personnel, including rest, medical support and community functions. On the other hand, they must ensure the operation of infrastructure that supports the execution of operational tasks, such as command and control systems, logistics storage facilities, energy and water supply, and basic security functions.

Therefore, the fundamental task of military camps is to support the achievement of operational objectives, and their planning and deployment depend on:<sup>17</sup>

- the duration of the operation
- the nature and intensity of threat sources
- the size, organisation and mission of the deployed forces
- host nation support (in the case of expeditionary operations)
- geographical factors (geological, climatic, meteorological, etc.)
- the composition of forces stationed in the camp (national, multinational, host nation)
- and numerous other factors (political, health and epidemiological conditions, the quality of home nation support, etc.)

In NATO doctrine, the protection of military camps is closely linked to the concept of mission assurance, whereby infrastructure resilience and force survivability are treated as prerequisites for sustained operational effectiveness.

From a spatial perspective, military camps cannot be regarded as point targets. They are typically large, functionally segmented areas, whose footprint may range from a few hectares to several square kilometres, depending on the size of the deployed forces, the operational environment and the intended duration of the camp. Within camps, zones of different purposes are present, each characterised by distinct infrastructure requirements, activity patterns and military value. This internal segmentation is of decisive importance from the perspectives of vulnerability and defence.

<sup>16</sup> NATO Standard ATP-3.12.1.4 Deployed Forces Infrastructure.

<sup>17</sup> BAKOS 2021 (translated by the author).

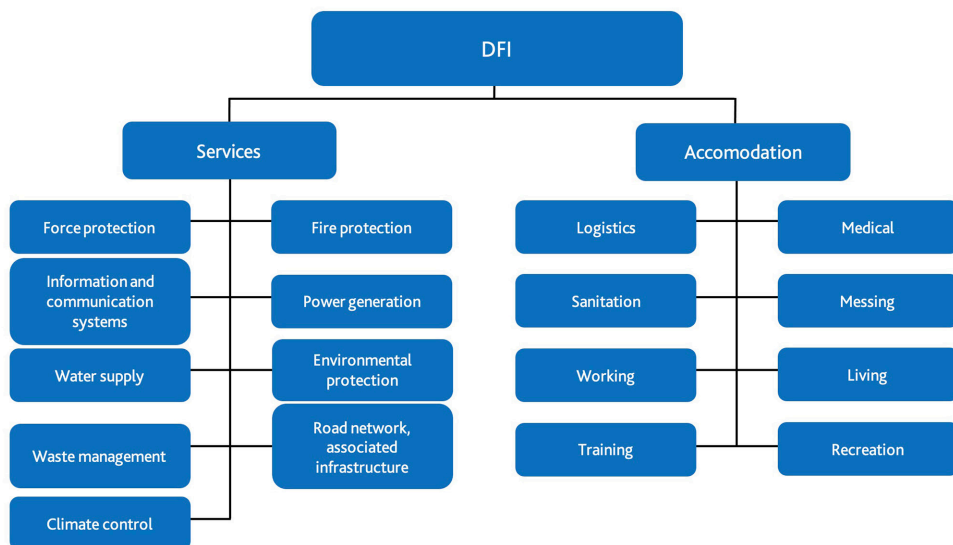


Figure 1: Deployed Forces Infrastructure  
 Source: compiled by the author based on NATO Standard ATP-3.12.1.4

From a temporal perspective, military camps typically operate at the same location over extended periods. This relative static nature provides advantages for friendly forces in terms of sustainment and organisational efficiency; however, it simultaneously increases detectability and the risk of targeted attacks. Routine movements, temporal patterns, and infrastructure usage practices that develop during camp operations may, over time, become predictable to a hostile observer.

Another characteristic of military camps is their strong dependence on interconnected systems. The failure of certain subsystems, such as energy supply, communications, or water supply (particularly in arid environments) may have a disproportionate impact on the overall operational capability of the camp. Consequently, a camp should be understood not merely as a physical object, but as a network of functional elements in close mutual interaction.

Overall, military camps constitute complex, large-area installations operating for defined periods of time and do not form a homogeneous target system. These characteristics justify examining threats to camps – particularly the employment of unmanned aerial vehicles – through a functionally differentiated approach and tailoring defensive measures to the differing roles and vulnerabilities of internal zones.

### Conceptual structure of counter-drone protection for deployed forces

Smaller and lighter drones are particularly exposed to meteorological effects and, due to their structural design, are inherently fragile; however, these characteristics also create

opportunities for counter-drone defence. An integrated and layered counter-drone system must therefore be designed with these factors in mind. The conceptual structure is based on an approach that identifies those UAS components whose attack or disruption can effectively contribute to counter-drone protection. These components include the operator/GCS,<sup>18</sup> the data link and the platform itself.

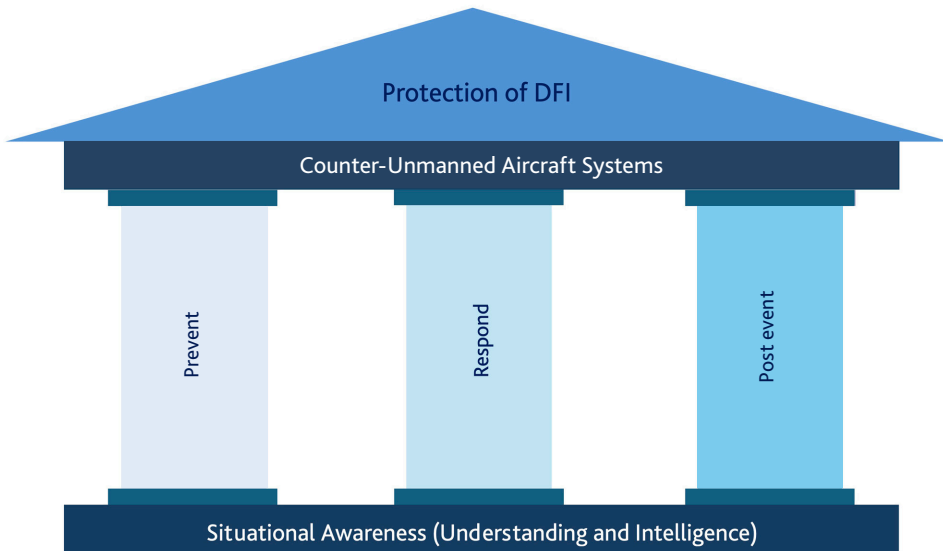


Figure 2: Conceptual structure of counter-drone defence

Source: compiled by the author based on NATO Standard ATP-117

Within the toolset of counter-drone defence, the first segment supports detection tasks. Through these sensors, the defence “perceives” the presence of drones, their movement, direction, as well as their altitude and speed. Such sensors may operate on RF,<sup>19</sup> EO,<sup>20</sup> IR,<sup>21</sup> ACC,<sup>22</sup> or radar principles, either as standalone systems or in combined configurations. Visual detection solutions may also be employed, which are indispensable under battlefield conditions; however, taking into account potentially adverse weather conditions, the detection range achieved by visual means often does not exceed 300–500 metres, providing only a very limited response time.

<sup>18</sup> GCS: Ground Control Station.

<sup>19</sup> RF: Radio Frequency.

<sup>20</sup> EO: Electro-Optical.

<sup>21</sup> IR: Infrared.

<sup>22</sup> ACC: Acoustic.

The next defensive segment is drone identification. This task set enables the differentiation of friendly drones from hostile ones through the application of technical solutions and procedures. The technical core of this function may be provided by an identification friend or foe-type system, that is, equipping friendly drones with transponders that allow them to be recognised by friendly system elements.

Within the neutralisation segment, a distinction must be made between non-kinetic and kinetic effectors. Non-kinetic means primarily fall into the category of jamming systems. These are electromagnetic or other advanced-technology devices employed with the purpose of disrupting, blocking, or taking over control between the drone and the operator/GCS. Such systems may be stationary (permanently installed), deployable, mobile, or handheld.

The purpose of kinetic means is the physical destruction of hostile drones or the infliction of damage sufficient to render them inoperable. These may include, among others, conventional air defence assets, net-launching devices, interceptor drones, small arms and directed-energy weapons.

From the perspective of counter-drone zones, maintaining the “greatest possible distance” and thus, achieving the most optimal defensive solution means keeping the threat posed by drones away from the airspace of a given area. Accordingly, I argue that the conceptual structure of counter-drone zones should be developed from the outside inward, beginning with the prevention or denial of hostile or malicious drone employment.

Among the means applicable to this layer is the existence of legal regulations that prohibit the use of drones either locally or regionally. While this approach may not appear straightforward during the conduct of expeditionary operations, it can nevertheless be managed in cooperation with local authorities within the framework of host nation support. Through such measures, unintended or non-hostile intrusions into the airspace of the deployed infrastructure may be excluded, thereby potentially avoiding the initiation of defensive fires.

The toolbox of preventive measures may also include – within a permissive environment – the option of conducting preemptive strikes against the operator/GCS. However, this already falls within the domain of weapons employment and, more specifically, the ROE.<sup>23</sup>

If the means represented by this first group prove inadequate, the optimal objective becomes the neutralisation or forced landing of drones already airborne. A fundamental prerequisite for this is the availability, deployment and C2<sup>24</sup> integration of the previously described sensor systems, as well as their linkage to appropriate effector systems. The selection and deployment of these sensors must ensure that the time available between the detection, tracking, identification of incoming drones and the decision-making and execution of effects is sufficiently long. This is, of course, a theoretical but necessary objective, which ultimately depends on the capabilities of the available sensor systems.

The generation of effects is, by nature, the result of a decision – either machine-based or human – and, similarly to sensors, the associated means are integrated into C2 systems. Their effectiveness depends on the range (engagement distance) of the effectors, the established

---

<sup>23</sup> ROE: Rules of Engagement.

<sup>24</sup> C2: Command and Control.

decision-making mechanisms, and the level of automation and autonomy of the defensive systems. As a matter of principle – at least at the conceptual level – the employment of non-kinetic effectors should be planned first, particularly over urban, densely populated, or built-up areas, in order to avoid collateral damage. Under optimal conditions, with suitable weather and the availability of technical capabilities, the drone threat may be eliminated or significantly reduced at distances of up to several tens of kilometres through the use of non-kinetic systems.

In cases of ineffectiveness – for example, against drones controlled via optical fibre – the role of kinetic effectors becomes increasingly important, as they represent one of the final “lines of defence”.

The effectiveness of counter-drone measures is also critically dependent on decision-making timelines, delegation of authority and rules of engagement. Delays or ambiguities in authorisation may significantly reduce the practical utility of even highly capable technical systems.

All of the above outlines an optimal scenario in which available resources permit the full implementation of these measures. Experience, however, indicates that this is rarely the case. Accordingly, preparing for – and accounting for – the possibility that established defensive systems may not be capable of achieving 100 percent effectiveness in drone detection, identification, or neutralisation, the construction of a “last line of defence” becomes necessary in order to protect forces and assets. This task group essentially encompasses the full spectrum of passive defensive measures. Such measures include fortification and hardening. The targets requiring protection in this manner consist of point targets or more extensive facilities that form part of the deployed forces’ infrastructure and which – taking into account the objectives of the operation – must be protected under all circumstances.

These may include:

- accommodation and rest areas
- work areas and command posts
- infocommunications centres
- areas providing life-support services (with particular emphasis on drinking water, food supply, climate control and energy supply)
- logistics storage areas (with particular emphasis on ammunition, fuel and weapons material)
- training areas

All of the above measures must be comprehensively complemented by the exploitation of camouflage and deception measures, as well as by the implementation of additional security procedures.

## Summary

This study examined the complex nature of the drone threat facing deployed military forces and analysed the conceptual and practical frameworks of potential defensive responses. It can be stated that the rapid technological development and mass employment of UAVs have

fundamentally transformed the security environment of military camps, particularly due to their static nature, large spatial footprint and long-term presence.

In my assessment, the drone threat affecting military camps cannot be considered homogeneous, as it is fundamentally shaped by the differing functions, military value and vulnerability of the internal functional zones. Drawing on the NATO Deployed Forces Infrastructure concept, I propose interpreting military camps as complex systems that can be subdivided into infrastructure units and zones providing essential services. In my evaluation, among infrastructures serving personnel accommodation, work areas and infocommunications nodes constitute particularly sensitive targets, as they simultaneously perform human, command-and-control, and information-related functions. Consequently, the drone threat in these areas manifests not only in kinetic forms, but also through information and electronic operations. The fact that drones have become capable of performing all these functions is reflected in the data presented in the tables containing the most characteristic drones employed during the Russo–Ukrainian conflict.

In my view, effective counter-drone defence cannot be interpreted solely as a technical issue. The foundation of defence must be provided by intelligence and reconnaissance, which enable the continuous assessment of existing and anticipated drone threats. Without detailed knowledge of drone types, ranges, control methods and employment procedures, counter-drone systems inevitably become reactive and, over time, ineffective. Accordingly, I propose that the development of counter-drone defence should always be carried out in parallel with the specific threat, continuously adapting to its evolution.

Future research should focus on validating the proposed zone-based counter-drone framework through scenario-based analysis and simulation, as well as on examining its applicability in multinational and host-nation-supported operational environments.

In summary, effective counter-drone protection of deployed forces can only be ensured through a threat-driven, zone-specific and adaptive approach. The integration of technical means, procedures, and passive defensive measures, combined with the continuous incorporation of intelligence and reconnaissance information, can jointly establish a sustainable and flexibly developable counter-drone defence for military camps.

## References

- BAKOS, Tamás (2021): A katonai táborok fizikai védelme [Physical Protection of Military Camps]. *Hadtudomány*, 31(E-szám), 186–193. Online: <https://doi.org/10.17047/HADTUD.2021.31.E.186>
- DARUKA, Norbert – SZALKAI, László (2022): The Dangers of Unmanned Aircraft Systems. In DARUKA, Norbert (ed.): *Fúrás-Robbantástechnika Nemzetközi Szimpózium Különkiadás 2022* [International Symposium on Drilling and Blasting Technology 2022]. Budapest: Magyar Robbantástechnikai Egyesület, 247–257. Online: [https://mare.hu/sites/default/files/furas-robbantastechnika\\_nemzetkozi\\_szimpozium\\_2022\\_kulonkiadas\\_mare\\_lektoralt\\_pdf.pdf](https://mare.hu/sites/default/files/furas-robbantastechnika_nemzetkozi_szimpozium_2022_kulonkiadas_mare_lektoralt_pdf.pdf)
- EMBER, István – KOVÁCS, Zoltán (2022): Mini drónok lehetséges alkalmazása tűzszerész műveletekben. *Haditechnika*, 56(2), 18–23. Online: [https://real.mtak.hu/175546/1/HT\\_2022-2\\_cikk\\_04.pdf](https://real.mtak.hu/175546/1/HT_2022-2_cikk_04.pdf)
- KOVÁCS, Ferenc (2024): A kritikus infrastruktúra stratégiai szerepe az orosz–ukrán háborúban [The Strategic Role of Critical Infrastructure in the Russo–Ukrainian War]. *Hadtudomány*, 34(3), 29–39. Online: <https://doi.org/10.17047/HADTUD.2024.34.3.29>

- KOVÁCS, Zoltán – EMBER, István (2021): Aknafelderítés légi eszközökkel [Landmine Detection with Aerial Vehicles]. *Műszaki Katonai Közlöny*, 31(4), 5–20. Online: <https://doi.org/10.32562/mkk.2021.4.1>
- KOVÁCS, Zoltán – EMBER, István (2022): Landmine Detection with Drones. *Revista Academiei Forțelor Terestre / Land Forces Academy Review*, 27(1), 84–92. Online: <https://doi.org/10.2478/raft-2022-0012>
- NATO C-IED COE S265/2023 Report: Use of Explosive-laden Drones and Other Improvised Explosive Devices by Palestinian Militias in the Attacks against Israel from the Gaza Strip.
- NATO Standard ATP-117 Countering Class I Unmanned Aircraft Systems (UAS) Doctrine, Edition A.
- NATO Standard ATP-3.12.1.4 Deployed Forces Infrastructure.
- PETTYJOHN, Stacie (2024): Evolution Not Revolution. Drone Warfare in Russia's 2022 Invasion of Ukraine. *CNAS*, 8 February 2024. Online: <https://www.cnas.org/publications/reports/evolution-not-revolution>
- SZALKAY, Dániel – DARUKA, Norbert – KOVÁCS, Zoltán – EMBER, István (2025): Drónok alkalmazási lehetőségei a hazai folyamőr feladatokban. *Haditechnika*, 59(3), 56–61. Online: <https://kiadvany.magyarhonvedseg.hu/index.php/HT/issue/view/201>
- VÉGH, Krisztián (2024): A repülő IED, mint harctéri innováció [Flying IEDs as Tactical Innovations]. In DARUKA, Norbert – EMBER, István – KOVÁCS, Zoltán T. (eds.): *III. Fúrás-robbantástechnika nemzetközi szimpózium különkiadás 2024* [III International Symposium on Drilling and Blasting Technology 2024]. Budapest: Magyar Robbantástechnikai Egyesület, 80–93. Online: [https://drive.google.com/file/d/1fpsAv\\_ELU1ynR3bE7rPoklhIUVDuRTL/view?pli=1](https://drive.google.com/file/d/1fpsAv_ELU1ynR3bE7rPoklhIUVDuRTL/view?pli=1)
- VÉGH, Krisztián – DARUKA, Norbert (2025): The Challenge of Technology-Enabled Unmanned Aircraft Systems. *Honvédségi Szemle*, 153(Special Issue 1), 80–91. Online: <https://doi.org/10.35926/HDR.2025.1.7>