HDR 2025, Nr. 1, 80–91.

Krisztián Végh, Norbert Daruka

THE CHALLENGE OF TECHNOLOGY-ENABLED UNMANNED AIRCRAFT SYSTEMS

DOI: 10.35926/HDR.2025.1.7

ABSTRACT: *Emerging Disruptive Technologies (EDTs) are fundamentally reshaping modern warfare, particularly in the field of military defence against drones. The rapid development of unmanned systems is creating new challenges that need to be met with innovative solutions. Technologies such as artificial intelligence, quantum computing, directed-energy weapons, and cyber warfare tools can play a key role in neutralising enemy drone threats. Artificial intelligence-based sensors and decision support systems can enable rapid detection and categorisation of drones, while directed energy weapons, such as lasers and microwave systems, can provide an efficient and cost-effective solution for their destruction. In addition, information operations tools such as electronic jamming and hacker attacks can be used to disrupt or take control of autonomous systems. The integrated use of these technologies could revolutionise the way we defend against drones and enable new strategies in modern theatres of war.*

KEYWORDS: *artificial intelligence, autonomous devices and systems, defence capability*

ABOUT THE AUTHORS:

- *Krisztián Végh is a PhD student at the Ludovika University of Public Service and a senior officer at the Defence Staff Operations Directorate. (ORCID: 0000-0001-6969-968X; MTMT: 10096868)*
- *Norbert Daruka (PhD) is the branch head of the Scientific Research Centre of the HDF Transformation Command. (ORCID: 0000-0002-7102-1787; MTMT: 10039981)*

INTRODUCTION

Europe's security environment is fundamentally shaped and influenced by the Russo-Ukrainian War, illegal migration, the potential for a parallel influx of terrorism, and, more broadly, by the conflicts in the Middle East. The lessons learned and conclusions drawn from these armed conflicts have a direct or indirect impact on the direction of domestic training and research and development. It is imperative that these lessons learned at the national level are brought into line with NATO's thinking in order to ensure that the policy developed by the Alliance can be properly supported.

The Russo-Ukrainian War brought to the surface a series of phenomena that had already been forgotten during the peace support operations of the past decades, such as the issue of extensive minefields[1] or the large-scale, planned attacks against critical infrastructure[2]

1 Csurgó et al. 2024.
2 Kovács 2024.

serving the population of the target country. Perhaps the most striking phenomenon of the ongoing armed conflicts is the emergence of the mass use of drones. They can be encountered in almost any type of military activity, and nations have accordingly begun to examine how they can be integrated into their own systems. It is also a natural and everyday issue that the web reports daily on successful drone attacks against armoured targets, naval vessels, and personnel as well.

THE EDT AND NATO

Technological progress has always shaped the characteristics of warfare, from the invention of gunpowder to the advent of nuclear weapons. However, the 21st century is seeing innovation on a scale and at a speed previously unimaginable. Rapid advances in artificial intelligence, robotics, biotechnology, quantum computing, and the potential of cyberspace are radically transforming the way we think about threats and the military strategies and weapons systems that respond to them. However, these 'disruptive technologies' not only pose new types of serious threats to international peace and security, but also offer new opportunities for shaping the warfare of the future.

In the coming years, and even within a decade, given the pace of development, the evolution of advanced military technologies will be shaped by four basic overarching characteristics: the rise of increasingly intelligent, interconnected, decentralised, and digital solutions. As a consequence of these trends, future military systems will increasingly operate autonomously, be interconnected in close networks, be able to operate in multiple operational environments (i.e., land, air, sea, cyber, and space) simultaneously, and perform their missions with extreme precision.

Technological innovations will increasingly become dual-use, meaning that a significant proportion of developments will come from the civilian, commercial sector and will be incorporated into military applications. This process will not only accelerate the integration of new solutions into the defence sector but will also enable their cost-effective and widespread deployment.

The emerging technology-enabled capabilities will contribute significantly to the effectiveness of NATO's military operations and organisational functioning. These tools and systems already support the five key development directions set out in the Alliance's Basic Concept for Warfare:

- gaining cognitive superiority, enabling faster and more accurate decision-making;
- integrated, multi-domain defence, ensuring coordinated cooperation among various forces and operational levels;
- multidimensional command and control capabilities enabling coordinated command and control of various operational environments;
- multi-level resilience to respond and adapt rapidly to crisis situations;
- a broad sphere of influence and projection of power to ensure NATO's strategic presence and responsiveness around the world.

Despite their wide applicability, these new technologies also present a number of challenges. NATO, and therefore our country, must seriously consider the operational, interoperability (cooperation), ethical, legal, and moral issues that they raise. Innovations, therefore, not only create opportunities but also require complex problems to be solved in order to ensure that the technological advantage will truly benefit the Alliance in the not-too-distant future.

NATO's Strategic Concept 2022[3] stresses that EDTs are changing the character of conflict, increasing their strategic importance, and becoming key areas of global competition. Technological advantage will increasingly influence success on the battlefield. Accordingly, the Allies are committed to fostering innovation and increasing investment in EDT to preserve NATO's interoperability and military superiority.

The Alliance is currently focusing on nine[4] priority technology areas[5] for EDTs:

– Artificial Intelligence;
– Autonomous systems;
– Quantum technologies;
– Biotechnology and Human Enabling Technologies;
– Space technology;[6]
– High-speed systems;
– New materials and manufacturing processes;[7]
– Energy and propulsion technologies;
– Next generation communication networks.

In these areas, NATO is developing detailed plans to accelerate responsible innovation and the rapid deployment of modern technologies, improving decision-making processes and strengthening transatlantic defence and security innovation in line with the democratic values of Allies and respect for human rights.

Therefore, the Alliance aims to develop responsible, innovative, and flexible policies to address these technologies, in close cooperation with the industrial and scientific community, within national and allied frameworks.

THE IMPACT OF TECHNOLOGY ON THE MILITARY USE OF DRONES

At the end of the 20th century, we had no idea that the warfare of the next century would be radically changed by the emergence and spread of new, so-called emerging and disruptive technologies. Of course, the military operations currently underway have also made a significant contribution to this. Advances in artificial intelligence (AI), 3D printing, and autonomous systems are significantly changing the way military equipment is developed, operated, and used. This is particularly evident in the field of aerial drones – officially known as UAVs[8] – that have become key players in modern warfare. The implications of these technologies for drones are examined in more detail below.

[3] *NATO 2022 STRATEGIC CONCEPT* – Adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022.
[4] In 2019, only seven were in the focus of NATO.
[5] NATO/OTAN Official website 2024.
[6] See more: Edl – Szenes (eds.) 331.
[7] Ember et al. 2024.
[8] UAV: Unmanned Aerial Vehicle.

Artificial Intelligence and Automation of Decision-Making

The use of artificial intelligence is revolutionising the autonomy and responsiveness of drones. AI-equipped UAVs are capable of real-time data analysis, target recognition, and, to a limited extent, even tactical decision making. This is particularly advantageous in hostile environments where rapid response can be vital. AI-driven systems reduce the need for human intervention, which not only shortens response times but also minimizes the risk to human resources. However, this also raises ethical and legal issues, especially if the decision to destroy a target is left to machine algorithms.

3D Printing and Manufacturing Flexibility

3D printing allows drones to be manufactured quickly and cost-effectively, especially in field environments, such as those seen near the front lines in the Russo-Ukrainian War. This technology can be used to produce not only complete vehicles, but also parts and special accessories, significantly increasing operational flexibility. With 3D printing, militaries can customise a great majority of parts and equipment,[9] such as drones for a specific mission – be it reconnaissance, transport, or even attack –, and quickly replace lost or damaged assets. This technology offers a strategic advantage, especially for smaller countries or non-state actors that do not have a large military industry.

It should be noted that standard or improvised explosive devices dropped from drones have proven to be highly effective weapons in the aforementioned conflict. Their effectiveness lies in the unmanned aerial vehicle itself and its triggering device, as it ensures productivity. Additive manufacturing technology also makes it possible to assemble parts or bodies of functionally different sizes, using so-called interposable elements. This makes it possible to assemble a hand grenade fuse and a mortar shell body into a hybrid weapon that can be launched/dropped from a drone.

Autonomous Systems and Swarm Operations

The development of autonomous systems allows the coordinated cooperation of drones in the form of "swarm operations". In these operations, hundreds or even thousands of small drones can make collective decisions, communicating with each other and adapting to the environment. Autonomous swarm operations pose new challenges to the enemy, as conventional weapons are difficult to defend effectively against highly mobile, decentralised units.

Challenges and Risks

While these technologies offer significant benefits, they also carry serious risks. Drones with AI and autonomy can be the target of cyberattacks, and the consequences of a possible hack of the control system could be severe. 3D printing makes it easy to manufacture drones, even for non-state actors, such as terrorist organisations, creating new security risks.[10] In addition, the issue of autonomous decision-making raises serious legal and ethical dilemmas: who

[9] Ember 2022a; Ember 2022b.
[10] Ember 2025.

bears responsibility in the event of an attack with civilian casualties if it is carried out by an AI-controlled device?

Artificial intelligence, 3D printing, and autonomous systems are revolutionising the potential applications of military drone technology. These developments will enable faster, more efficient, and cheaper operations, but also create new risks and moral dilemmas. Future theatres of war are likely to be increasingly shaped by these technologies, and militaries will have to adapt to new realities not only from a technological but also from a strategic and ethical perspective.

THE DIVERSITY OF DRONES

In the process of examining both the Russo-Ukrainian and the Middle East conflicts, and the lessons learned from them, several aspects have come to the fore, sometimes predicting significant changes in characteristics for the future. The emergence of drones may be familiar to the UAV category, but the development of autonomous ground[11] and waterborne[12] assets is also underway.

This article focuses on the NATO Class I category.

Table 1 *Classification of drones for military and civilian use (based on Government Decree 38/2021 (2.2.2011) and NATO ATP-117, edited by the authors)*

National		NATO		Theoretical range	Application height	Application level
Category	Take-off weight	Class	Subclass			
E	> 600 kg	Class III	HALE	No limitation	65,000 ft	Strategic
			MALE		45,000 ft	Operational
D	150–600 kg	Class II	Tactical 150–600 kg	~200 km	18,000 ft	Tactical
C	25–150 kg	Class I	Small > 15 kg	~50 km	5,000 ft	Tactical
B1, B2	4–25 kg		Mini < 15 kg	~25 km	3,000 ft	Tactical
A1, A2	< 4 kg		Micro < 2 kg	~5 km	200 ft	Tactical

Almost all the above categories play a role in the Russia-Ukraine conflict, which is not surprising given the decades-long history of military R&D in drones and autonomous systems. A study[13] on the subject found that drones have become increasingly autonomous over time and have been widely linked to other weapons systems, their emergence having a profound impact on military doctrines and organisations. In terms of their characteristics, the drones used in the Russo-Ukrainian conflict can be divided into two broad categories: military or civilian use, and single-use or reusable, in terms of their design.

Military drones are basically designed for combat use (even though many may have a non-destructive role),[14] which means that they are equipped with various protection devices

[11] Global Defence News – Army Recognition Group official website.
[12] Northrop Grumman website.
[13] Pettyjohn 2024.
[14] Kovács – Ember 2022; Ember – Kovács 2022.

and can withstand jamming and cyber activities, which makes them difficult to detect and counter effectively. The operators of such devices undergo specific training, and their replacement is a significantly time-consuming task. The preferred reusable military drones of the Russian side were initially the Orlan-10 and various versions of the Zala, while the Lancet and Shahed versions of the single-use drones are also noteworthy. The Ukrainian side preferred the Leleka-100, Furia, and PD-1 types for reusable missions, and the Switchblade 300 and Warmate for kamikaze missions. Of course, both sides have MALE[15] devices in their systems, together with Forpost and Orion on the Russian side and the infamous TB2 on the Ukrainian side.

The division between single-use and multi-use is also valid for commercially available modified so-called “FPV”[16] drones. The emergence of known devices in their current form and known use dates back to the early 2000s, mainly for use by non-state actors and certain terrorist groups.[17]

The term FPV was probably coined as an analogy for small UAVs with modified explosive devices published on popular online video-sharing sites. However, we are convinced that this type of simplification is not appropriate for a correct assessment and interpretation of the threat they pose and, for this reason, almost certainly for the design of C-UAS[18] with appropriate effectiveness. Accordingly, we also consider it important to briefly describe the division of modified drones. Among the multiple-use devices, there are those with a triggering device, capable of delivering grenades against infantry and armoured vehicles, and those capable of carrying small arms or armour-piercing devices or incendiary agents. The one-way group is made up of guided or omnidirectional cluster munitions and drones with EFP[19] charges. Also included in this group are kamikaze drones capable of carrying modified armour-piercing grenades, the so-called improvised FPV loitering munitions.

DRONE DETECTION AND IMPACTS

When examining C-UAS activities, it is essential to review the UAS[20] architecture in order to identify weak or vulnerable points when designing an effective countermeasure.

Simplified, a small category UAS consists of an operator, a remote-control device, a C2[21] link, and the UAV device and its payload. Larger systems are complemented by GCS,[22] some kind of launch platform, and MCE[23] elements. GCS and MCE consist of physical infrastructure such as trucks, containers, or buildings, usually housing the computer that runs the applications needed to run the whole system. All of this is, of course, operated exclusively by properly trained professionals.[24]

15 MALE: Medium Altitude Long Endurance.
16 FPV: First Person View – the operator sees what the drone “sees”. Usually designed for drone competitions and aerial photography, they are significantly more powerful than conventional quadcopters.
17 Végh 2024.
18 C-UAS: Counter-Unmanned Aircraft Systems.
19 EFP: Explosively Formed Penetrator.
20 UAS: Unmanned Aircraft Systems.
21 C2: Command and Control.
22 GCS: Ground Control Station.
23 MCE: Mission Control Element.
24 See more: Joint Air Power Competence Centre 2021.

Research into the vulnerability of UAS components has been a multi-year process, and the following breakdown helps to understand the issue.[25]

Detectability

Radar visibility is measured by the RCS[26] provided by the device. For UAVs in the smaller categories, this cross-section is relatively low; the plastic materials used in their construction and the relatively low operating altitude pose additional challenges for conventional radars.

Their visibility in the IR[27] spectrum for IR detection tools, the high-temperature components of conventional propulsion systems, and the combustion products emitted during fuel combustion provide a cross-section that can be adequately detected. The electric propulsion of smaller drones makes this method more difficult, but the temperature of the drone is different from its surroundings, so IR can be a shorter-range detection method.

Going off topic, it should be mentioned that there are also examples of protection against drones in industrial installations. The above method may be a solution to eliminate safety risks.[28] The excessive bandwidth of 5G networks enables the transmission of large information-gathering data streams of high-resolution video from surveillance drones.[29]

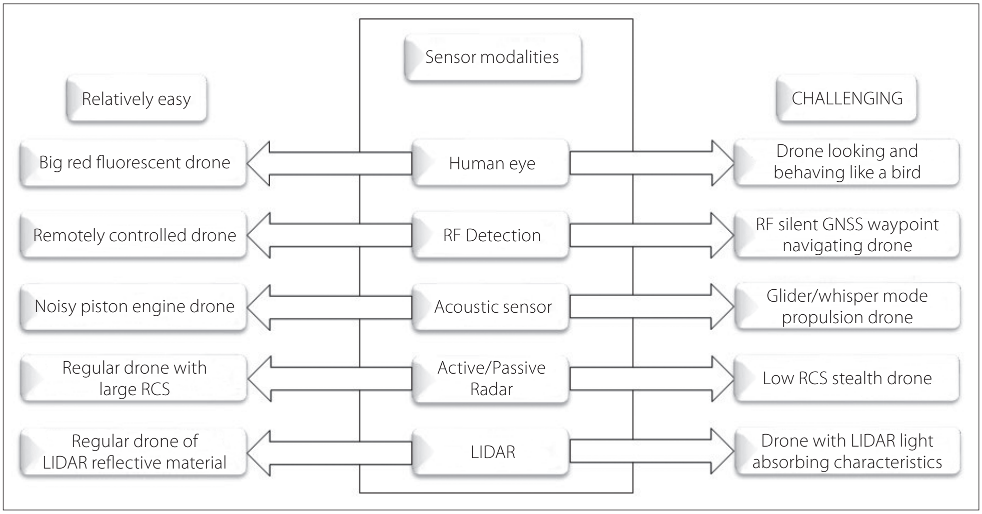

Figure 1 *Sensor modalities (based on NATO ATP-3.3.8.1, edited by the authors)*

Acoustic detection systems are usually ground-based and are used to identify the altitude and speed of the UAV. The noise level of a drone with a 70-dB sound output measured at a distance of one metre is "merged" with the roughly 20-dB sound level generated by the

25 Haider 2021.
26 RCS: Radar Cross-Section.
27 IR: Infrared.
28 Szávay – Őszi 2025.
29 Tóth 2025.

environment at a distance of about 300 metres, which can therefore mask the drone's presence from human hearing. Acoustic detection of smaller devices is therefore of very low effectiveness and may only be suitable for shorter distances.

The effectiveness of visual detection depends largely on the size and colour of the target object and the general atmospheric and weather conditions. A further challenge in visual detection of drones is the need to distinguish them from various moving objects, such as birds or even a plastic bag caught in the wind. A drone is most likely to be heard before it is detected, and typically, the noise of a nearby drone triggers visual recognition.

Of course, there are other detection options in addition to the methods and tools briefly described above, but our aim is to raise awareness of the complexities and challenges of the detection itself. In short, C-UAS cannot rely solely on one solution, it must range from building situational awareness of personnel based on visual and acoustic detection to the use of radio frequency and laser detection techniques.

Effectors

The C-UAS technology spectrum is extremely diverse and is constantly evolving in response to the complexity and diversity of threats. The counter-technologies currently in use can be broadly grouped into five main categories: radio frequency (RF) jamming, attacks against GNSS,[30] kinetic devices, directed energy weapons (laser-based systems), and high-power microwave weapons.

The purpose of RF jamming is to interrupt the communication between the drone and the operator, typically over Wi-Fi or other freely available bands. GNSS jamming or its more sophisticated form, spoofing, can mislead the UAVs by undermining navigation capabilities by communicating false coordinates. Kinetic countermeasures, such as machine guns or even missile systems, aim at their physical destruction, but their use is almost impossible in urban or civilian environments.

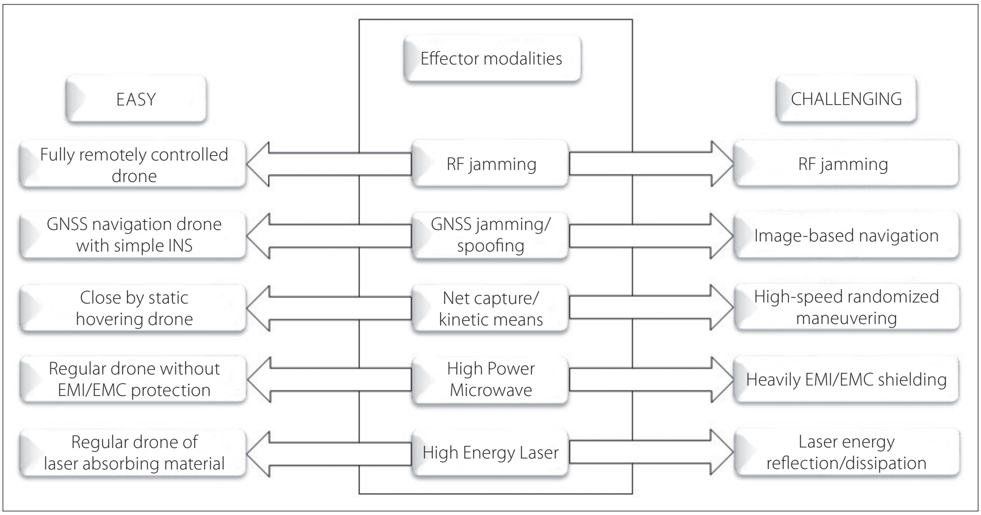

Figure 2 *Effector modalities (based on NATO ATP-3.3.8.1, edited by the authors)*

[30] GNSS: Global Navigation Satellite System.

Advanced laser weapons can use concentrated energy to cause structural damage to a target in a short time, while high-energy microwave systems can destroy UAV onboard systems by electronic overload. The practical application of these directed energy weapons is currently also primarily understood in a military context. In summary, the effective use of anti-drone systems requires an integrated approach combining electronic, kinetic, and informatics tools according to the level and location of the threat.

THE ROLE OF EDT IN C-UAS

The rapid proliferation of UAVs poses new challenges for organisations responsible for airspace security, or even for the military. Sensor technologies for detecting and neutralising drones, such as visual, acoustic, radio frequency (RF), radar, and LIDAR[31] systems, play a key role in addressing these threats. The integration of artificial intelligence (AI) into these systems could bring significant improvements in the effectiveness of drone detection and identification.

AI-Enabled Sensors

AI-based computer vision technologies play a prominent role in the analysis of visual sensors, the image data collected by cameras. AI can detect and track drones in real time, even against complex backgrounds. For example, DroneOptID is an AI-based software[32] that enables real-time drone detection, identification, and tracking, using optical sensors.

Acoustic sensors, RF sensors, and AI can detect the presence of drones by analysing the distinctive sound patterns emitted by the drones. By processing these sound patterns in real time, AI algorithms can increase the accuracy of detection and reduce the number of false alarms. In one study, AI-based methods have been used to efficiently classify drones with an accuracy of up to 90% by processing both radio frequency and acoustic signals.[33]

Combining data from different sensors, called sensor fusion, increases the reliability and accuracy of detection. AI algorithms can integrate and analyse this heterogeneous data, providing a more comprehensive picture of drone movements and behaviour. "Dedrone-Tracker.AI" is an AI-powered combined system that uses radio frequency, radar, imagery, and acoustic sensors to efficiently detect and track drones. The AI can analyse these signals in real-time, identifying the type of drone and pinpointing its position, filtering out UAVs identified as friendly.[34]

AI and LIDAR technology use laser beams to map the environment, creating an accurate 3D image. By analysing this data, AI can identify drones and distinguish them from other flying objects. Although LIDAR-based drone detection is still evolving, the integration of AI holds promising potential.

Integrating AI into drone detection sensors will significantly increase their efficiency and reliability. The combination of different sensor technologies and AI will enable more accurate and faster detection, identification, and tracking of drones. Integration brings many

31 LIDAR: Light Detection and Ranging.
32 AI-Powered Optical Detection, Identification, and Tracking Software. Drone Shield Limited.
33 Frid et al. 2024.
34 AXON – Dedrone official website.

benefits, but also faces challenges. Data quality, the need for real-time processing, and the reliability of AI models are key factors. Future research should focus on these challenges.

AI-Assisted Effectors

In UAV defence, not only detection but also neutralisation of targets – i.e., the use of effectors – is key. The rise of artificial intelligence opens up the possibility to significantly increase the effectiveness of various soft-kill and hard-kill systems. AI can improve reaction times, identify attack patterns, and automate decision-making. The integration of the main effector types with AI is discussed below.

Radio Frequency jamming is the disruption of communication channels between drones and their controllers, causing drones to become uncontrollable, which can force them to land or return. The effectiveness of RF jamming depends on the control frequency of the drone and the strength of the jamming signal. The integration of AI may include efficiency-enhancing directions such as identifying drone communication protocols in real time, even if they are cryptic or operate at variable frequencies (frequency hopping), or even dynamically optimizing the jamming strategy by considering the environmental spectrum usage and the target's response reactions. It is important to note, however, that RF interference is not selective and can therefore affect other communication systems.

Drone navigation systems often rely on global satellite navigation systems. In GNSS or GPS jamming, navigation signals are blocked, while in deception, false signals are transmitted, which can give the drone incorrect position information, causing it to be diverted or forced to land.

AI significantly increases the accuracy, adaptability, and effectiveness of these techniques. In the case of jamming, AI can analyse the radio spectrum in real time, detect the presence and type of GNSS signals, and optimise jamming power and frequency accordingly. In spoofing, AI can predict the target drone's movements using predictive modelling and then match them to generate credible-looking false navigation signals, avoiding detection by the target system. It also allows automatic target classification, priority management, and coordinated mass attacks, such as against drone swarms. Artificial intelligence thus not only improves the accuracy of jamming and deception but also provides adaptive, energy-efficient, and scalable operation for modern drone defence systems.

Hard-kill devices – such as machine guns, missiles, interceptors, or high-energy weapons (e.g., laser, microwave) – destroy drones in a direct physical way. AI can significantly enhance their effectiveness in target identification, tracking, target prioritisation, and fire control.

AI-based image processing algorithms can distinguish drones from other flying objects in real time, even in complex environmental conditions. Machine learning can adapt to the rapid and unpredictable movement patterns of drones, enabling precise target tracking. In multi-target situations, the system can prioritize threats with the support of AI, neutralizing the most dangerous ones first. By extending automation, autonomous weapon systems can be developed that identify and destroy targets without human intervention. But this raises serious ethical and legal questions: for example, who is responsible for the damage caused by a misidentification, and is it right for a machine to decide whether to take a human life? In the face of these moral dilemmas, it is becoming increasingly accepted that, in AI-supported systems, humans should have ultimate control over the command to fire. AI thus complements, rather than replaces, human decision-making, which is a key consideration, especially in the use of hard-kill tools.

SUMMARY

The rapid development of drone technology and the massive and often unpredictable use of unmanned systems nowadays pose a major challenge to modern warfare, especially in Europe's security environment. The conflict in Ukraine and other regional crises have clearly demonstrated that small, cheap, often commercially sourced drones can have a strategic impact. Confronted with this threat, Europe is facing an increasingly urgent need for modern, effective, and adaptive drone deterrence solutions. Detection, identification, and tracking are key elements of drone defence, for which a variety of sensor technologies are available. The performance of these sensors is significantly enhanced by artificial intelligence. Through machine learning, systems can distinguish drones more accurately from other flying objects, recognise patterns of behaviour, predict their movements, and manage mass target detection and tracking. Soft-kill devices, such as RF jamming, GNSS jamming, and spoofing, interfere with the drone's guidance or navigation. In these cases, the use of AI enables adaptive, targeted, and energy-efficient intervention: the system can map the spectrum situation in real time, pre-model the drone's behaviour, and optimise jamming or spoofing tactics accordingly. Hard-kill methods – such as net throwers, missiles, high-energy lasers, and microwave weapons – have a direct physical effect on the target. AI supports these systems in target identification, tracking, fire control, and threat prioritisation. It also brings to the fore the issue of automation, which raises moral and legal challenges. While autonomous weapons systems can be effective, the international community is increasingly advocating a human-in-the-loop approach, whereby humans have the final decision on the use of lethal force. Future anti-drone systems will certainly work in even closer integration with artificial intelligence. These systems will employ adaptive, networked, real-time decision support solutions that can adapt to dynamically changing threats. The application of AI in the areas of autonomous drone swarm protection, spectrum management, predictive threat analysis, and system cost optimisation will become inevitable. In sum, the future of drone threat protection depends on the deep integration of technological innovation and AI, but this must be done within a strict ethical, legal, and strategic framework.

BIBLIOGRAPHY

- AXON – Dedrone official website: https://www.dedrone.com/ (Accessed: 07/04/2025).
- Csurgó, Attila – Kállai, Ernő – Zsóri, Ferenc: *Az orosz műszaki tevékenység jellemzői az orosz–ukrán háborúban*. Honvédségi Szemle, Vol. 152, No. 3 (2024), 33–45. https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/1198 (Accessed: 09/04/2025).
- Edl, András – Szenes, Zoltán (eds.): *Új űrkorszak kapujában. A világűr biztonsági és katonai kérdései*. Zrínyi Kiadó, Budapest, 2024, p. 331., ISBN 978 963 327 965 6.
- Ember, István (2022a): *3D nyomtató alkalmazási lehetősége egyes speciális robbantási feladatoknál*. In: Daruka, Norbert (szerk.): Fúrás-Robbantástechnika Nemzetközi Szimpózium Különkiadás 2022. Magyar Robbantástechnikai Egyesület, Budapest, 2022, 75–83. (Accessed: 02/04/2025).
- Ember, István (2022b): *Hatásvizsgálati robbantás kumulatív töltetekkel*. Műszaki Katonai Közlöny, Vol. 32, No. 3 (2022), 13–23. Online: https://doi.org/10.32562/mkk.2022.3.2 (Accessed: 02/04/2025).
- Ember, István: *The Possible Impact of the Proliferation of 3D Printers on the Protection of Critical Infrastructure*. Advanced Sciences and Technologies for Security Applications (ASTSA), 2025, 303–312. DOI: https://doi.org/10.1007/978-3-031-78544-3_24 (Accessed: 10/04/2025).

- Ember, István – Kovács, Zoltán: *Mini drónok lehetséges alkalmazása tűzszerész műveletekben*. Haditechnika, Vol. 56, No. 2 (2022), 16–23. DOI: 10.23713/HT.56.2.04 (Accessed: 10/04/2025).
- Ember, István – Kovács, Zoltán – Vég, Róbert – Dénes, Kálmán – Daruka, Norbert: *Additive Use of Special Materials in the Military*. Scientific Bulletin, Vol. 29, No. 2 (2024), 247–255. DOI: 10.2478/bsaft-2024-0026 (Accessed: 01/04/2025).
- Frid, Alan – Ben-Shimol, Yehuda – Manor, Ezer – Greenberg, Shlomo: *Drones Detection Using a Fusion of RF and Acoustic Features and Deep Neural Networks*. Sensors, Vol. 24, No. 8 (2024). https://www.mdpi.com/1424-8220/24/8/2427?utm (Accessed: 09/04/2025).
- Global Defence News – Army Recognition Group official website: *BAE Systems Australia pioneers the future of warfare with new ATLAS CCV UGV*. 2024. https://armyrecognition.com/news/army-news/army-news-2024/bae-systems-australia-pioneers-the-future-of-warfare-with-new-atlas-ccv-ugv (Accessed: 02/04/2025).
- Haider, Andre: *The Vulnerabilities of Unmanned Aircraft System Components*. In: A Comprehensive Approach to Countering Unmanned Aircraft Systems. Germany, 2021. https://www.japcc.org/chapters/c-uas-the-vulnerabilities-of-unmanned-aircraft-system-components/?utm_source=chatgpt.com (Accessed: 09/04/2025).
- Joint Air Power Competence Centre: *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. Germany, 2021. https://www.ulib.sk/files/english/nato-library/collections/monographs/japcc-books/a-comprehensive-approach-countering-unmanned-aircraft-systems.pdf (Accessed: 09/04/2025).
- Kovács, Ferenc: *A kritikus infrastruktúra stratégiai szerepe az orosz–ukrán háborúban*. Hadtudomány, Vol. 34, No. 3 (2024). https://ojs.mtak.hu/index.php/hadtudomany/issue/view/1464/1042 (Accessed: 31/03/2025).
- Kovács, Zoltán – Ember, István: *Landmine Detection with Drones*. Revista Academiei Fortelor Terestre, Vol. 27, No. 1 (2022), 84–92. https://www.armyacademy.ro/reviste/rev1_2022/Kovacs.pdf (Accessed: 09/04/2025).
- *NATO 2022 STRATEGIC CONCEPT*. Madrid, 29 June 2022. https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf (Accessed: 01/04/2025).
- NATO/OTAN Official website: *Emerging and disruptive technologies*. 2024. https://www.nato.int/cps/bu/natohq/topics_184303.htm (Accessed: 01/04/2025).
- NATO STANAG 2663 Countering Class I Unmanned Aircraft Systems (UAS) Doctrine.
- Northrop Grumman website: *Manta Ray*. https://www.northropgrumman.com/what-we-do/sea/manta-ray (Accessed: 02/04/2025).
- Pettyjohn, Stacie: *Evolution Not Revolution. Drone warfare in Russia's 2022 Invasion of Ukraine*. Center for a New American Security, 2024. https://www.cnas.org/publications/reports/evolution-not-revolution (Accessed: 01/04/2025).
- Szávay, István – Őszi, Arnold: *Protection Management Against Drones in Industrial Facilities*. Advanced Sciences and Technologies for Security Applications (ASTSA), Springer, Cham, 2025, 661–672. DOI: https://doi.org/10.1007/978-3-031-78544-3_53 (Accessed: 09/04/2025).
- Tóth, András: *Military 5G as a Critical Information Infrastructure*. Advanced Sciences and Technologies for Security Applications (ASTSA), Springer, Cham, 2025, 723–731. DOI: https://doi.org/10.1007/978-3-031-78544-3_57 (Accessed: 09/04/2025).
- Végh, Krisztián: *A repülő IED, mint harctéri innováció* (Flying IEDs as Tactical Innovations). In: Daruka, Norbert – Ember, István – Kovács, Zoltán Tibor (szerk.): III. Fúrás-robbantástechnika nemzetközi szimpózium különkiadás 2024. Magyar Robbantástechnikai Egyesület, Budapest, 2024, 80–93. https://m2.mtmt.hu/gui2/?mode=browse&params=publication;35463363 (Accessed: 03/04/2025).