INFO FLASH
Finabel
The European Land Force
Commanders Organisation

FINABEL - THE EUROPEAN LAND FORCE COMMANDERS ORGANISATION

NOVEMBER 2025

INFOFLASH

Meeting the Drone Challenge: The Future of UAVs in Hybrid Warfare

WRITTEN BY

FEDERICO FAVIA

EDITED BY

JACKSON ELDER

SUPERVISED BY

ELISE ALSTEENS & KEVIN WHITEHEAD

Introduction

Technological progress is a decisive driver of change in military affairs, and disputes involving unconventional methods reflect the new reality of war and conflict management in the 21st century (Sprengel, 2021, p. 9). Unmanned Aerial Vehicles (UAVs) are no exception: commercially designed for agriculture, aerial mapping, or even recreational purposes, they have been increasingly deployed in military contexts over the past three decades (Alley-Young, 2024). UAVs, commonly referred to as drones, are aircraft without a human pilot on board, "remotely controlled by an operator on the ground, or pre-programmed to fly specific routes" (Nelson and Gorichanaz, 2019, p. 3), and have thus become a powerful asset pushing the boundaries of existing defence capabilities.

The recent wave of unsettling airspace incursions across NATO territory has drawn attention to the threat of UAVs to national security. In September, the Polish military, backed by NATO allies, shot down suspected Russian drones that had entered Polish airspace from the direction of Ukraine (Charlish et al., 2025). Following the incident, Romania and Estonia also reported similar violations, while sightings of suspicious drones affected flights and airport operations in Denmark (Edwards, 2025). Dismissing Moscow's denials of responsibility, several European leaders have called for a firm response to Russia's hybrid campaign to sow division and unsettle citizens of the EU (Hubenko, 2025). To accelerate investment and close capability gaps, on October 16, 2025, the European Commission presented the Defence Readiness Roadmap 2030, which includes the flagship Drone Defence Initiative, signalling an eagerness to address drone proliferation as a critical transnational security concern.

Building resilience in this matter, however, requires broader awareness of how drones are redefining the threat landscape. This paper begins by reviewing the most prominent types and applications of UAVs, with a focus on those deployed in the Ukrainian battlefield. Versatility and cost-effectiveness make drones invaluable assets for hybrid operations with a reduced military footprint; moreover, they benefit from dual-use innovations that blur the boundaries of civil and military applications. Non-state and criminal actors thus have increasing access to sophisticated aerial tactics, providing hybrid strategies with an additional layer of ambiguity and deniability, which complicates risk assessment and the development of adequate responses. This paper concludes by assessing future trajectories in drone-enabled threats, arguing that the accelerating convergence of AI, nanotechnology, and swarm engineering will spearhead technological advancements in drone manufacturing (Raheja, 2025), necessitating further adaptation of defence systems.

Overall, the proliferation of UAVs is likely to influence Europe's quest for defence readiness. The Commission's Roadmap duly underscores the need for technical and industrial capacity to deliver efficient countermeasures at scale. Nonetheless, Russia's provocative hybrid drone campaign is ultimately testing the credibility and resolve of the EU to engage in active deterrence and enforce sovereignty.

2. Types and Use Cases of Military UAVs

In the face of geopolitical tensions and budgetary constraints, tapping into private sector innovations equips militaries with off-the-shelf commercial solutions that can be adapted to defence purposes, thereby leveraging unique opportunities to enhance national security (Aebi et al., 2025, p. 2). The versatile application of UAVs duly exemplifies the defence ecosystem's heightened interest in dual-use technologies, driven by cost and risk calculations. First, drones are relatively inexpensive to assemble and deploy; those that violated Polish airspace were made of plywood and are estimated to have cost approximately US$12,000 each (Spray, 2025). More advanced models can reach a few hundred thousand US dollars, still considerably less expensive than standard air and missile defence. NATO's response to the incursion in Poland required instead the use of expensive missiles and interceptors, indicating a lack of cost-effective countermeasures (Edwards, 2025). Drones also enable the streamlining of resource-intensive operations by requiring less fuel, manpower, and equipment (McLean, 2014). Finally, pilotless vehicles entail a lower risk of personnel loss in direct aerial confrontations or hostile environments.

Modern drones generally fall within two distinct classes: the fixed-wing drone is shaped like a small aeroplane and can fly long distances at high speed, but requires runways for take-off and landing; the rotor model is shaped like a small helicopter and has less endurance, but is highly manoeuvrable and can take off or land in vertical flight (Ayamga et al., 2021).

Military drones can be categorised by the specific mission they carry out within battlefields:

- Intelligence, Surveillance & Reconnaissance (ISR): a key role for UAVs is to serve as persistent "eyes in the sky", mapping terrain, scanning for threats, or monitoring ground activity to provide early warnings (Satapathy, 2025). High-altitude, long-endurance (HALE) drones with high-resolution cameras and thermal sensors are particularly well-suited for these tasks (Sahoo, 2025), covering vast distances and spending hours hovering at least 30,000 feet over hard-to-reach areas without endangering soldiers. Neutral conflict observers can also employ drones as assets to monitor ceasefire agreements (Organization for Security and Co-operation in Europe [OSCE], 2018). ISR missions have been a common application of UAVs throughout the war in Ukraine. Available evidence (Edmonds and Bendett, 2023, p. 3) suggests that even before the full-scale invasion in 2022, Russia attempted to gather visual intelligence on Ukraine's critical infrastructure as preparation for subsequent targeted strikes and to inform its aggressive strategy of cyberattacks against power grids and ITC networks (Dickson and Harding, 2025). Moreover, Kyiv has deployed drones to track enemy infiltration and troop build-ups along the border (Zoldi, 2025).

- Precision Strike and Combat Operations: Militaries use armed UAVs to carry out high-accuracy attacks by guiding missiles and smart bombs directly to selected targets such as enemy leaders or infrastructure. During the Donbas war in 2014, Russia used UAVs in combination with heavy rocket artillery to destroy nearly two battalions of the Ukrainian army in Zelenopillya, killing 37 soldiers (Slobozhanskiy, 2018). This type of deployment allows Russia to leverage the lethality of its artillery assets while keeping them on domestic soil. On the Ukrainian side, armed drones provide air support to ground troops during engagements through "loitering munitions" missions - remaining airborne over a designated zone and striking viable targets (Beebe, 2025). This strategy enables the Ukrainian military to compensate for numerical inferiority and strike enemy forces with precision and lethality, inflicting significant damage to Russian oil refineries and weapon factories (Kushnikov, 2024).

- Electronic Warfare (EW) and Cyber Operations: Modern UAVs can be equipped to disrupt enemy operations by jamming their radars and communication systems. Facing challenges due to Russia's advanced EW capabilities of spoofing GPS to mislead drones, Ukraine is developing solutions such as frequency-hopping technology to shield its vehicles from interference and interception (Zoldi, 2025). Another common application consists of gathering electronic signals intelligence (SIGINT) for strategic planning. SIGINT works by capturing signals from radio, satellite, or other sources, after which data is processed through decryption and decoding in order to gain a strategic edge over the enemy's intentions and behaviour patterns (Stoner, 2025).

- Electronic Warfare (EW) and Cyber Operations: Modern UAVs can be equipped to disrupt enemy operations by jamming their radars and communication systems. Facing challenges due to Russia's advanced EW capabilities of spoofing GPS to mislead drones, Ukraine is developing solutions such as frequency-hopping technology to shield its vehicles from interference and interception (Zoldi, 2025). Another common application consists of gathering electronic signals intelligence (SIGINT) for strategic planning. SIGINT works by capturing signals from radio, satellite, or other sources, after which data is processed through decryption and decoding in order to gain a strategic edge over the enemy's intentions and behaviour patterns (Stoner, 2025).

The versatility and cost-effectiveness of UAVs mean that 'drone wars' are already a reality within modern battlefields. At present, drones inflict about 70 per cent of all Russian and Ukrainian casualties, and both sides are scaling up production, aiming to assemble up to four million drones in 2025 (Santora et al., 2025). Overall, UAVs have disrupted conflict dynamics by empowering actors in an asymmetrical manner that was previously impossible. The following section explores how their proliferation has contributed to altering the security architecture and threat perception in the context of hybrid warfare.

3. The Drone Advantage in the Grey Zone

Unmanned drones are an invaluable asset in the hybrid sphere. As early as the 19th century, military theorist Carl von Clausewitz recognised the chameleon-like character of war, dominated by non-linear, unpredictable interactions (Beyerchen, 1992, p. 75). In modern hybrid conflicts, engaging in unconventional military strategies implies a "small military footprint [...] to control the risk of escalation, and contain the political costs and damage" associated with the direct, undisguised use of force (Sprengel, 2021, p. 9). Accordingly, the warfare capabilities championed by UAVs are ideal for upholding this approach.

The first key aspect to consider is the expanding variation in UAV deployment methods. In fact, beyond static categorisations, a drone is apt to perform numerous tasks with only minor reconfigurations, transitioning seamlessly between multiple purposes. As a stark example, the high-resolution cameras and sensors of ISR drones can be leveraged to facilitate precision strikes from artillery or other aircraft by painting targets with laser designators; if needed, those same drones can then transition to search and rescue operations, scanning combat zones for survivors (Satapathy, 2025). This multi-role capability makes it challenging for the opponent to gauge the true objective of offensive missions. Finally, the high degree of autonomy grants what Sprengel (2021, p. 11) refers to as 'technical deniability': rejecting responsibility and blaming an outcome on the system and its components. All these features feed ambiguity and deception as part of the covert use of force typical in hybrid warfare scenarios, rendering drones ideal instruments for tailored operations in the grey zone.

Compounding the threat of multi-role capability is the fact that dual-use innovations are blurring the lines between civilian and military applications, thereby complicating risk assessment and readiness (Mendoza et al., 2021, p. 3). On the one hand, the additional challenge lies in distinguishing between hostile UAVs and innocuous commercial drones and minimising false positives. This endeavour faces legal and logistical hurdles in several EU countries, where tight regulatory frameworks constrain active defence measures (Clapp, 2025, p. 10; Lațici, 2019). Electronic jamming and kinetic intercepts pose risks of unintended consequences, including collateral damage and privacy breaches, particularly in densely populated areas or near critical infrastructure (Chauhan et al., 2025, p. 9). On the other hand, the militarisation of civilian technologies is leading to commercial drones being increasingly weaponised, so that non-state actors too can harness sophisticated aerial strategies. Regions plagued by insurgencies and instability have witnessed an increase in targeted assassinations, kamikaze-style strikes, and infrastructure disruption by reconfigured drones (Yaacoub et al., 2020, p. 15). This trend once again fits the hybrid dimension of conflict realities, which is populated by a combination of state, non-state, and criminal actors, adding an unpredictable dimension to the threat landscape. Relying on mercenary actors equipped with powerful UAV capabilities for false flag or proxy attacks appears attractive to hybrid campaigns as a way to hinder the opponent's decision-making on the attribution of aggressive activities; such an advantage even hints at private, proxy entities soon offering custom UAV operations in conflict zones (Sprengel, 2021, p. 26).

It is no coincidence that Russia has a long history of relying on private military companies such as the Wagner Group, non-governmental organisations, or hacktivists as auxiliary assets in hybrid warfare and intelligence activities, essentially "incorporating criminality into its statecraft" (Rekawek et al., 2025, p. 9). The full-scale invasion of Ukraine marked a turning point, after which Russia intensified its hybrid operations both to retaliate against the West and to compensate for the limitations of its conventional military power. Finding itself deprived of trained undercover operatives as a wave of Russian diplomats was expelled from Europe (Walsh, 2022), Moscow activated a fallback plan to sustain its hybrid campaign. It mobilised 'single-use' agents - Russian-speaking civilians in vulnerable socio-economic situations recruited online and assigned simple sabotage tasks in exchange for payment (Rekawek et al., 2025, p. 16). In parallel, Russia has leveraged the expertise of organised crime to escalate the sophistication of its activities, including repurposing smuggling drones to orchestrate vandalism acts and sabotage operations across the Estonian border (Epner et al., 2024; Rekawek et al., 2025, p. 26). Arguably, the risk of destabilisation faced by Europe becomes exponential if criminal networks are also exploited as proxies for hybrid threat actors, because this strategy further enhances operational flexibility, grants manpower, and an additional layer of deniability.

4. Future Trajectories in Drone-enabled Threats

The rapid pace of technological advancements in drone warfare entails that success is a matter of continuous adaptation to adversarial countermeasures (Gray et al., 2025). Russian forces are attacking Ukrainian troops with 'sleeper' UAVs, adapted to "operate in a low-power standby mode for extended periods" (Stepanenko, 2025, p. 8). After landing in a concealed position, these drones can power down and stay electronically silent for days through a hibernator module, before being remotely activated again to launch a surprise strike on enemy targets. Instead of radio-frequency emissions, Russian sleeper UAVs utilise a fibre-optic tether to maintain their route and remain undetectable to EW devices (Khomenko, 2025).

The misuse of innovative military technologies often outpaces the ability of states to develop expedient countermeasures, making it essential to examine future trajectories of drone-enabled threats to anticipate acute vulnerabilities in defence systems. For example, the promising application of nanotechnology holds the potential to facilitate the miniaturisation of key components, bypassing traditional detection frameworks. Nano-drones are set to take advantage of physical environments that are hardly accessible to traditional sensor arrays, as bio-inspired designs that mimic the flight patterns of insects help them blend in with their natural surroundings (University of Lincoln, 2021; Hart, 2024). Such capacity for environmental integration could have profound implications for prolonged, detection-free surveillance and reconnaissance operations.

Furthermore, drone swarming hints at the evolution from single aircraft to coordinated multi-vehicle systems that operate as a collective intelligence. Unlike conventional deployments, where each aircraft is individually controlled, swarming involves multiple UAVs "working together autonomously, sharing information, making collective decisions, and adapting to changing conditions in real-time" (Raheja, 2025, para. 2). Research institutions and military organisations have conducted numerous demonstrations that highlight swarm capabilities. In 2017, the U.S. Department of Defense tested swarms of drones launched from fighter aircraft, exhibiting the ability to overwhelm radar and interception systems through sheer numerical superiority (Snow, 2017). Looking forward, integrations championed by artificial intelligence and machine learning algorithms will enable swarms to optimise their own performance and to develop increasingly complex coordination through trial and experimentation (Raheja, 2025).

Swarming is underpinned by a logic of scalability (swarms operate effectively whether composed of a few or hundreds of units) and resilience: distributed intelligence ensures that no individual drone controls the entire system, and the swarm functions even if single vehicles are neutralised (Raheja, 2025). Therefore, defensive efforts will revolve around cutting-edge interception solutions capable of addressing decentralised threats. Nonetheless, technological progress in the direction of drone saturation likely marks a broader paradigm shift in aerial warfare away from precision and toward sheer volume (Jensen and Atalan, 2025). Whether an individual UAV hits its target matters less than the compound effect of straining defence resources and pushing adversarial resistance to the limit. In a battlefield dominated by inexpensive, mass-produced unmanned systems, the burden is on the defence to showcase preparedness. This shift must inform Europe's adaptation strategy to the threats posed by Russia. Within the war in Ukraine, improvisation in technology development through expedient procurement and deployment has allowed Kyiv to buy valuable time (Burrows, 2025). Yet, Ukraine will remain dependent on consistent financial support from the EU beyond intermittent aid packages to build a layered and economically sustainable air defence. In the context of Moscow's hybrid warfare strategy, EU Member States are expected to strengthen their defence posture by delivering interoperable innovations, combined with the rapid mass production of low-cost counter-drone technology (European Commission, 2025, p. 1). Rising criticism against the initial proposal of a 'drone wall' on Europe's eastern flank (Gray et al., 2025) derives precisely from scepticism related to the complexity of the initiative and the feasibility of implementing it with enough scale and speed to ensure readiness in the face of a fluid, multi-faceted threat landscape.

5. Conclusion

By consistently lowering the financial and human costs of warfare, UAVs have redefined the operational and strategic contours of modern conflict. Their adaptability across ISR, combat, electronic warfare, and logistical domains exemplifies how dual-use technologies are blurring the traditional boundaries between civilian and military innovation. The diffusion of drone capabilities to non-state actors and private proxies points to a decentralisation of violence that undermines established security architectures and further complicates response. Indeed, UAVs thrive precisely because they embody ambiguity. Their modularity, deniability, and low visibility render them uniquely suited for hybrid warfare, where attribution, escalation control, and legality are deliberately obscured. Looking forward, the accelerating convergence of AI, nanotechnology, and swarm engineering will intensify these dynamics.

The paradigm shift induced by drone proliferation should guide Europe's quest for strategic autonomy in defence. The Defence Readiness Roadmap, published in October, highlights the awareness that preparedness will depend on interoperable innovation, mass production of affordable countermeasures, and rapid adaptation (European Commission, 2025, pp. 6-7). Yet, what is being tested by the recent drone incidents is not just the boundaries of

Europe’s airspace, but its political resolve to enforce sovereignty (Olafsen, 2025). Russia intentionally exploits the grey zone through a provocative strategy to achieve its goals, knowing a conventional conflict would see it underpowered compared to NATO. In response, European governments have often employed deterrence by denial, reluctant to impose sufficient costs due to fears of escalation (Deni, 2024). This approach, however, may have outlived its utility and instead risks serving as a bureaucratic shield against decisive action, at times when every hesitation signals vulnerability.

Bibliography

Aebi, T., Pankov, A., Malkov, A., Merhaba, A. & Stella, C. (2025). *Unlocking the strategic power of dual-use technologies*. Arthur D. Little Viewpoint. https://www.adlittle.com/sites/default/files/viewpoints/ADL%20Dual%20use%20technologies%202025.pdf

Alley-Young, G. (2024). Drone (Unmanned aerial vehicle). EBSCO Knowledge Advantage. . https://www.ebsco.com/research-starters/music/drone-unmanned-aerial-vehicle

Ayamga, M., Akaba, S. & Nyaaba, A.A. (2021). Multifaceted applicability of drones: A review. *Technological Forecasting and Social Change, 167.* https://doi.org/10.1016/j.techfore.2021.120677

Beebe, E. (2025, August 22). Loitering Munitions 101: What They Are and Why They Matter. IDGA. https://www.idga.org/command-and-control/articles/loitering-munitions-101-what-they-are-why-they-matter

Beyerchen, A. (1992). Clausewitz, Nonlinearity, and the Unpredictability of War. *International Security, Vol. 17, No. 3.* https://www.jstor.org/stable/pdf/2539130.pdf?refreqid=fastly-default%3Adbfe234789b9da175508a520ba4d4e90&ab_segments=&initiator=&acceptTC=1

Burrows, E. (2025, September 24). *How Europe can defend itself against Russian drones and electronic warfare*. PBS News. https://www.pbs.org/newshour/world/how-europe-can-defend-itself-against-russian-drones-and-electronic-warfare

Charlish, A., Kelly, L. & Erling, B. (2025, September 10). Poland downs drones in its airspace, becoming first NATO member to fire during war in Ukraine. Reuters. https://www.reuters.com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato-member-fire-during-war-2025-09-10/

Chauhan, D., Kagathara, H., Mewada, H., Patel, S., Kavaiya, S. & Barb, G. (2025, March 12). Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies. IEEE Access Volume 13. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10924170

Clapp, S. (2025, May). *Military drone systems in the EU and global context: Types, capabilities and regulatory frameworks*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772885/EPRS_BRI(2025)772885_EN.pdf

Deni, J.R. (2024, July 8). NATO's in denial about deterrence by denial. Politico. https://www.politico.eu/article/nato-us-army-chinese-government-defense-war-europe-allies-cold-war-russia-poland/

Dickson, J. & Harding, E. (2025, September.) *A Playbook for Winning the Cyber War. Part 2: Evaluating Russia's Cyber Strategy*. A Report of the CSIS Intelligence, National Security, and Technology Program. https://www.csis.org/analysis/playbook-winning-cyber-war-part-2-evaluating-russias-cyber-strategy

Edmonds, J. & Bendett, S. (2023, March). Russia’s Use of Uncrewed Systems in Ukraine. CNA Corporation Report. https://www.cna.org/reports/2023/03/Russian-Uncrewed-Systems-Ukraine.pdf

Edwards, C. (2025, September 26). The paradox of Russian escalation and NATO’s response. IISS Online Analysis. https://www.iiss.org/online-analysis/online-analysis/2025/09/the-paradox-of-russian-escalation-and-natos-response/

Epner, E., Weiss, M., Laine, M. & Moora, E. (2024, December 5). The GRU vandals: Moscow’s hired thugs are causing mayhem in Estonia. The Insider Politics. https://theins.ru/en/politics/276891

European Commission. (2025, October 16). Joint Communication to the European Parliament, the European Council and the Council. Preserving Peace – Defence Readiness Roadmap 2030. JOIN/2025/27 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0027

Gray, A., Mukherjee, S. & Hunder, M. (2025, October 15). EU scramble for anti-Russia 'drone wall' hits political, technical hurdles. Reuters. https://www.reuters.com/business/aerospace-defense/eu-scramble-anti-russia-drone-wall-hits-political-technical-hurdles-2025-10-15/

Hart, L. (2024, January 5). Advanced Nano Drones Created from Nanomaterials. Blografi. https://shop.nanografi.com/blog/advanced-nano-drones-created-from-nanomaterials/

Hubenko, D. (2025, October 8). EU's von der Leyen urges response to hybrid warfare threats. DW. https://www.dw.com/en/eus-von-der-leyen-urges-response-to-hybrid-warfare-threats/a-74274875

Jensen, B. & Atalan, Y. (2025, May). Drone Saturation. Russia’s Shahed Campaign. CSIS Briefs. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-05/250513_Jensen_Drone_Saturations.pdf?VersionId=QsQBXrKcuEpHw4yK0EoTr7ZIraS5yTMW

Khomenko, I. (2025, June 18). What are Russia’s “Sleeper Drones"—and Why They Pose a Growing Threat to Ukraine. United24Media. https://united24media.com/latest-news/what-are-russias-sleeper-drones-and-why-they-pose-a-growing-threat-to-ukraine-9236

Kushnikov, V. (2024, May 13). *80% of damage to oil refineries is caused by Liutyi drones*. Militarnyi. https://militarnyi.com/en/news/80-of-damage-to-oil-refineries-is-caused-by-liutyi-drones/

Lațici, T. (2019, October). *Civil and military drones. Navigating a disruptive and dynamic technological ecosystem*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642230/EPRS_BRI(2019)642230_EN.pdf

McLean, W. (2014, June 26). *Drones are Cheap, Soldiers are Not: A Cost-Benefit Analysis of War*. The Conversation US, Inc. https://theconversation.com/drones-are-cheap-soldiers-are-not-a-cost-benefit-analysis-of-war-27924

Mendoza, M.A., Rodriguez Alfonso, M. & Lhuillery, S. (2021). A battle of drones: utilizing legitimacy strategies for the transfer and diffusion of dual-use technologies. Technological Forecasting and Social Change, 166. https://doi.org/10.1016/j.techfore.2020.120539

Nelson, J. & Gorichanaz, T. (2019, April 24). Trust as an ethical value in emerging technology governance: The case of drone regulation. *Technology in Society, 59*. https://doi.org/10.1016/j.techsoc.2019.04.007

Olafsen, M.H. (2025, October 14). *Red Lines in the Grey Zone: Europe's Airspace Under Pressure*. https://voycecommunity.eu/our-work/f/red-lines-in-the-grey-zone-europe's-airspace-under-pressure

Organization for Security and Co-operation in Europe (2018, March 28). *OSCE SMM long-range unmanned aerial vehicles resume monitoring of security situation in eastern Ukraine*. OSCE. Press release. https://www.osce.org/special-monitoring-mission-to-ukraine/376456

Raheja, P. (2025, July 2). *Drone Swarms are Coming: The Future of Autonomous Operations*. Autonomy Global. https://www.autonomyglobal.co/drone-swarms-are-coming-the-future-of-autonomous-operations/#:~:text=Drone%20swarming%20represents%20a%20paradigm,to%20create%20complex%20group%20dynamics

Rekawek, K., Lanchès, J. & Zotova, M. (2025, September). *Russia's Crime-Terror Nexus. Criminality as a Tool of Hybrid Warfare in Europe*. GlobalSec. https://www.globsec.org/sites/default/files/2025-09/Russia%E2%80%99s%20Crime-Terror%20Nexus%20Criminality%20as%20a%20Tool%20of%20Hybrid%20Warfare%20in%20Europe.pdf

Sahoo, A. (2025). *What Is a HALE Drone? Uses, Range & Key Benefits*. BonVAero Report. https://bonvaero.com/what-is-hale-drone-uses-and-benefits/

Santora, M., Jakes, L., Kramer, A.E., Hernandez, M. & Sholudko, L. (2025, March 3). *A Thousand Snipers in the Sky: The New War in Ukraine*. The New York Times. https://www.nytimes.com/interactive/2025/03/03/world/europe/ukraine-russia-war-drones-deaths.html

Satapathy, S. (2025). *How are UAVs Used in the Military? Applications, Benefits*. BonVAero Report. https://bonvaero.com/military-drones-use-cases-and-its-types/

Slobozhanskiy, K. (2018). What's going on in Ukraine? Q&A on the Sea of Azov as a new frontier in the undeclared Russian-Ukrainian war. Rubryka. https://rubryka.com/article/q-a-on-the-sea-of-azov/.

Snow, S. (2017, January 9). *Pentagon successfully tests world's largest micro-drone swarm*. MilitaryTimes. https://www.militarytimes.com/news/pentagon-congress/2017/01/09/pentagon-successfully-tests-world-s-largest-micro-drone-swarm/

Spray, A. (2025, September 12). *Gerbera: The Russian drones that infiltrated Poland are made from plywood and foam*. Aerospace Global News. https://aerospaceglobalnews.com/news/russian-cheap-gerbera-drones-breach-airspace-poland/

Sprengel, F.C. (2021, June). *Drones in hybrid warfare: Lessons from current battlefield*. Hybrid CoE Working Paper 10. https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210611_Hybrid_CoE_Working_Paper_10_Drones_in_hybrid_warfare_WEB.pdf

Stepanenko, K. (2025, August 7). *Russian Drone Innovations are Likely Achieving Effects of Battlefield Air Interdiction in Ukraine*. Institute for the Study of War. https://understandingwar.org/research/russia-ukraine/russian-drone-innovations-are-likely-achieving-effects-of-battlefield-air-interdiction-in-ukraine/

Stoner, J. (2025, April 30). *What is SIGINT (Signals Intelligence) & How Does it Work?*. Flyeye. https://www.flyeye.io/drone-acronym-sigint/

University of Lincoln. (2021, November 9). *Insects Inspire the Future of Drone Technology*. Blog Post. https://news.lincoln.ac.uk/2021/11/09/insects-inspire-the-future-of-drone-technology/

Walsh, N.P. (2022, November 16). *Russian spying in Europe dealt 'significant blow' since Ukraine war, MI5 chief says*. CNN World. https://edition.cnn.com/2022/11/16/uk/mi5-chief-russia-spying-iran-china-threats-intl

Yaacoub, J., Noura, H., Salman O. & Chehab, A. (2020, May 8). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things 11*. https://doi.org/10.1016/j.iot.2020.100218

Zoldi, D. (2025, April 23). *Unmanned Aerial Vehicles Shaping the Future of Defense in Israel, Canada and Ukraine*. Autonomy Global. https://www.autonomyglobal.co/unmanned-aerial-vehicles-shaping-the-future-of-defense-in-israel-canada-and-ukraine/