IFRI STUDIES

SECURITY STUDIES CENTER FOCUS STRATÉGIQUE No. 132

FEBRUARY 2026

Mapping the MilTech War
Eight Lessons from Ukraine's Battlefield

Bohdan KOSTIUK
Daryna-Maryna PATIUK
Anastasiya SHAPOCHINA
Élie TENENBAUM

In partnership with:
EASTERN CIRCLES

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit foundation according to the decree of November 16, 2022. As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience.

Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

This publication is part of Ifri's European and Transatlantic Security Program and benefited from the support of NATO's Allied Command Transformation (ACT).

ISBN: 979-10-373-1167-2

Cover: Donbass, Ukraine, August 13, 2025 – A Ukrainian soldier pilots a Baba Yaga drone
© Jose Hernandez Camera 51/Shutterstock.com

How to quote this publication:

Bohdan Kostiuk, Daryna-Maryna Patiuk, Anastasiya Shapochina, and Élie Tenenbaum, "Mapping the MilTech War: Eight Lessons from Ukraine's Battlefield", *Focus stratégique*, No. 132, Ifri, February 2026.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Site internet : Ifri.org

Focus stratégique

Resolving today's security problems requires an integrated approach. Analysis must be cross-cutting and consider the regional and global dimensions of problems, their technological and military aspects, as well as their media linkages and broader human consequences. It must also strive to understand the far-reaching and complex dynamics of military transformation, international terrorism and post-conflict stabilization. Through the "**Focus stratégique**" series, Ifri's Security Studies Center aims to do all this, offering new perspectives on the major international security issues in the world today.

Bringing together researchers from the Security Studies Center and outside experts, "**Focus stratégique**" alternates general works with more specialized analysis carried out by the team of the Defense Research Unit (LRD or *Laboratoire de Recherche sur la Défense*).

Editorial board

Authors

Bohdan Kostiuk is an Analyst at Eastern Circles specializing in defense technology, geoeconomics, and European strategic autonomy. His recent work addresses China's role in drone production, the security implications of AI, counter-drone systems and European industrial resilience. Previously, he served in diplomatic and editorial roles with Ukraine's Ministry of Foreign Affairs and UA: Ukraine Analytica. He also worked as an analyst at Tech Force UA and the Snake Island Institute, focusing on defense innovation and dual-use technologies. A former fellow at the James Martin Center for Nonproliferation Studies and the Odesa Center for Non-Proliferation, Bohdan holds degrees from Odesa National I. I. Mechnikov University and the University of Toronto's Munk School of Global Affairs. He is a member of the Younger Generation Leaders Network and an expert with the Open Nuclear Network.

Daryna-Maryna Patiuk is a Ukraine analyst and director of operations at Eastern Circles. She co-authored a Ukraine newsletter focused on institutional transformation and disruptive innovative technologies, wrote for *Diplomatie* magazine, including on *New Maritime Warfare*, *The War of Drones*, and *The Russian Orthodox Church as an Infowar Tool*, and co-organized three research trips to Ukraine on the innovation ecosystem. She brings international public relations experience spanning the private, academic, and public sectors in Ukraine and Paris. Her work includes strategic communications projects for international brands, business schools, cultural institutions, and government bodies. Notably, she led brand development for the Strategic Leadership Program for defense and political leaders and the Strategic Architect Program at Kyiv-Mohyla Academy Business School. Daryna holds a degree in Sociology from the National University of Kyiv-Mohyla Academy and in Sciences Po in International Relations (PSIA) on International Development and European Studies.

Anastasiya Shapochkina is the founder and director of Eastern Circles, a French think tank on geoeconomics of energy and defense in Eastern Europe, focusing on Ukraine. Anastasiya worked for 10 years in the energy industry, where she analyzed nuclear, renewable energy, utilities, oil & gas, e-mobility markets, and developed international consortia for European research projects. At Eastern Circles, her expertise includes Russia-China energy relations, European energy security, Russia-India and Ukraine-

Turkey defense industry relations, Ukraine-Europe cooperation and the need for sovereign autonomy in defense. She has been lecturing on Russia-Europe relations at Sciences Po Paris since 2012, and is a frequent contributor for BBC, France 24, TF1, RFI, LCI and other media. Anastasiya has a Master's degree from Georgetown University School of Foreign Service.

Élie Tenenbaum is the director of Ifri's Security Studies Center. After years of focusing on irregular warfare, counterinsurgency and counter-terrorism, his research now leads him to cover more general strategic issues, in particular European security and defense policy. He holds a PhD (2015) in History and graduated from Sciences Po (2010). He has been a visiting fellow at Columbia University (2013-2014) and spent a year at the War Studies Department, at King's College London (2006); he has taught international security at Sciences Po and international contemporary history at the Université de Lorraine. He is the author of numerous articles and books on history and strategy, including *The Twenty-Year War: Jihadism & Counter-Terrorism in the 21st Century*, with Marc Hecker (Robert Laffont, Prix du Livre Géopolitique 2021).

Acknowledgement

The authors thank the soldiers, commanders, MilTech developers, business and civil society leaders in Ukraine and in Europe who gave their time and shared their views on the development of defense technologies in Ukraine and on the lessons NATO countries can learn from it. Special thanks to Colonel Hennadiy Kovalenko for his feedback on the report draft, and Dignitas, Military Innovation Center of the Ukrainian Armed Forces, and military brigades.

Executive summary

This report maps out the evolution of key technologies that have emerged or developed in the last 4 years of the war in Ukraine. Its goal is to derive the lessons the North Atlantic Treaty Organization (NATO) could learn to strengthen its defensive capabilities and prepare for modern war, which is large-scale and conventional in nature.

Through open-source research, defense technology data analysis, and in-the-field interviews in Ukraine and in NATO countries with the military, industry, civil society and government actors, the report dives into 8 groups of technologies.

The rise of autonomous warfare: UAVs, USVs and UVGs

Key takeaways: The Unmanned Aerial Vehicles (UAVs) evolved in 8 phases in the last 4 years, transforming from simple reconnaissance tools into sophisticated, partially AI-coordinated weapon systems. They have sparked the electronic warfare (EW) arms race between Russia and Ukraine, which in turn was rendered obsolete with the emergence of the fiber-optic cable drone in 2024. The following year, machine learning and Artificial intelligence (AI) integration emerged as the strategic game-changer and signaled the race toward AI coordination of multiple systems and eventually decision-making.

Ukraine's naval-drone campaign reflects a transition from improvised, isolated uncrewed surface vessels (USVs) strikes to a coordinated, multi-domain operational system. While it does not bring naval domination, it allowed to push back a far more superior enemy and secure vital export corridors.

The Unmanned Ground Vehicles (UGVs) in Ukraine deliver supplies, evacuate casualties, mine, demine, and strike targets, but remain experimental and experience last-mile challenges due to high battlefield transparency and setbacks in communication.

Lessons learned:

- Domestic drone production defines Ukraine's future technological progress and scale-up capacity. To build and sustain such production, greater supply chain autonomy is key, as well as built-in scaling capacity and autonomous AI capabilities.

- Systematic battlefield data collection for the training of Chinese and Russian AI models poses a risk for NATO to lose a technological competition.
- Ukrainian USVs are a lesson to small and mid-size countries in how to secure a strategic advantage at sea without a military fleet. NATO should integrate USVs into its strategy and doctrine.
- USVs are complementary to conventional maritime weapons and a counter-USV strategy.
- Sea denial and strategic impact are achievable without a conventional navy when unmanned systems are integrated into a multi-domain concept that links USVs, UAVs, missiles, and cyber/EW.
- To maintain its technological advantage, NATO should build a long-term strategy of not only cooperation with Ukraine, but also its gradual integration into the European MilTech ecosystem.
- Ukraine's UGV development demonstrates that warfare has shifted from large platforms to adaptive swarms of low-cost systems. Innovation is in adaptation capacity, not in any one design.

Electronic warfare

Key takeaways: The ubiquity of electronic equipment and reliance on the electromagnetic spectrum (EMS) for coordination and precision fire has transformed EW from a specialized function into a combined arms system, able to affect not only drone, but also artillery and missile precision. Russian modernization of its satellite navigation hardware imposed forces a shift toward intelligent EW methods like spoofing (transmitting false coordinates) and sending corrupted data packets to overload receiver logic. Yet, EW efficiency is contested by a combination of much simpler (fiber optic cable) and more sophisticated technology (computer-vision drones).

Lesson learned: Electronic warfare has become a continuous, software-driven contest embedded at the tactical level, where adaptability, integration, and spectrum management matter more than centralized, high-power jamming systems.

Artificial Intelligence

Key takeaways: AI in the Ukraine war has been used mainly as an enabler rather than an independent decision-maker. In practice, AI on the battlefield of the Russo-Ukrainian war refers to software that accelerates data processing, target identification, and navigation under combat conditions, while human operators retain control over lethal decisions. Most frontline applications rely on narrowly defined functions such as

computer vision for terminal guidance, route correction, and target tracking, especially where electronic warfare disrupts communications.

The main operational value of AI has been the compression of the decision cycle. Systems that filter drone feeds, satellite imagery, and sensor data allow commanders to act on processed information instead of raw inputs, while semi-autonomous drone functions reduce pilot workload during the most vulnerable phases of flight. Rather than true autonomy or large-scale swarming, current use emphasizes limited teaming between humans and machines, prioritizing reliability, speed, and cost over full automation.

Lessons learned: The Ukrainian experience shows that AI is most effective as a tool for speeding up analysis and coordination, not for replacing human decision-making. Practical gains come from integrating AI into existing systems to reduce workload and reaction time rather than pursuing full autonomy. Current limits in communication and reliability mean that small-scale human-machine teaming is more viable than autonomous swarms.

Space-based technologies for the Ukrainian battlefield

Key takeaways: Space-based capabilities have shifted from a strategic enabler to a tactical dependency in Ukraine. Commercial satellite communications, navigation, and Earth-observation systems now underpin day-to-day battlefield operations, enabling distributed command and control, drone warfare, precision fires, and resilience under sustained attack. The scale of deployment—tens of thousands of terminals and near-continuous commercial Intelligence, Surveillance, and Reconnaissance (ISR) coverage—has effectively created a space-enabled "Internet of the Battlefield," without which Ukrainian forces would be unable to sustain their current operational tempo. –

At the same time, Ukraine's reliance on commercial space services has revealed critical vulnerabilities. Single-provider dependence, exposure to electronic warfare, geofencing risks, and adversarial adaptation have turned space into a contested operational domain rather than a sanctuary. Ukrainian adaptation has therefore shifted toward hybrid, software-defined architectures that combine multiple space and terrestrial bearers, accept degraded connectivity as the norm, and push processing and decision-making to the tactical edge. The central lesson is that resilience now lies less in owning space assets than in designing flexible, redundant architectures able to fight through disruption.

Lesson learned: Modern land warfare is now structurally dependent on space-based services, but resilience comes from hybrid, multi-layered architectures rather than reliance on any single constellation or provider.

Combat software and the march toward integration

Key takeaways: Ukraine's combat effectiveness has relied heavily on software as an integration layer, compensating for material inferiority, heterogeneous equipment, and constant disruption. Systems such as Kropyva, Delta, and associated tools have compressed sensor-to-shooter timelines, enabled decentralized command, and managed unprecedented volumes of ISR data. The decisive factor has not been visibility alone, but the ability to filter, prioritize, and act faster than the adversary under conditions of information saturation.

Over time, these tools have evolved from volunteer-driven applications into a modular, federated combat management ecosystem linking sensors, shooters, communications, and decision-support across echelons. Rather than a single monolithic battle management system, Ukraine demonstrates the value of open, adaptable architectures that tolerate partial failure, function under degraded connectivity, and integrate new tools rapidly. The key shift is from situational awareness as "seeing the battlefield" to command as "managing cognitive load and decision speed."

Main lesson learned: In modern high-intensity warfare, software integration and information management—not platform performance—are the primary drivers of operational tempo and combat effectiveness.

Air defense: counter-UAV systems

Key takeaways: From 2022 to 2025, counter-drone warfare in Ukraine shifted from traditional, centralized air defense toward flexible and economically sustainable solutions. Early in the war, legacy missile systems were effective against large drones but quickly became impractical once small, cheap drones appeared in large numbers. On the frontline, defense increasingly relied on local action and physical protection rather than formal air defense networks. Simple measures such as improvised armor, small arms fire, and later interceptor drones proved more adaptable than complex systems. Tactical innovation consistently emerged at the unit level, often faster than formal procurement could respond, reshaping how drones were detected and destroyed.

In the deep rear, air defense evolved from severe financial imbalance to relative parity. Initial reliance on expensive missiles against low-cost drones created an unsustainable model. Over time, Ukraine reduced this gap by combining passive sensors, mobile gun teams, and low-cost interceptor drones into a layered system able to absorb mass attacks. As offensive drones became cheaper, stealthier, and harder to jam, defenses moved away from electronic warfare toward physical detection and interception.

Lesson learned: modern air defense must prioritize scale, cost control, and integration across many simple systems rather than dependence on a small number of high-end weapons.

The salvo competition: economic approach to air defense

Key takeaways: Hundreds of drones and scores of missiles and guided bombs a night in Ukraine and numerous drone incursions to Europe through 2025 triggered the need to reevaluate the approach to air defense. As European responses have shown so far, the main weakness of NATO air defense can be its cost, unsustainable in the face of mounting domestic budget challenges in key European countries.

The war in Ukraine has transformed counter-UAV from a niche air-defense function into a central determinant of operational and strategic endurance. The mass employment of cheap, expendable drones—used for reconnaissance, strike, deception, and saturation—has exposed the unsustainability of missile-centric air defense architectures when confronted with salvo dynamics. Early reliance on high-end interceptors created prohibitive cost-exchange ratios, forcing rapid adaptation toward layered defenses that combine guns, mobile fire teams, low-cost interceptors, passive sensors, and selective use of advanced missiles against high-value threats.

Ukraine's response demonstrates that effective counter-UAV is an ecosystem rather than a single capability. Success depends on tight integration between multi-spectral detection (acoustic, thermal, radar), automated data fusion, human-machine teaming, and economically viable kinetic effectors. As electronic warfare has become increasingly ineffective against fiber-optic and autonomous drones, physical interception has returned to the forefront, supported by AI-enabled cueing and decentralized command. Counter-UAV has thus evolved into a continuous, high-tempo battle of adaptation in which sustainability, manpower, and integration matter as much as technical performance.

Lesson learned: In a drone-saturated battlespace, air defense effectiveness is defined by sustainable cost-exchange ratios and integrated ecosystems, not by reliance on high-end interceptors alone.

Deep strike capabilities

Key takeaways: Ukraine's deep-strike campaign has evolved from sporadic, opportunistic attacks into sustained, multi-layered pressure on Russian depth, logistics, and force generation. Constrained by limited access to Western long-range systems, Ukraine combined asymmetric UAV campaigns with a narrow set of conventional precision-strike capabilities to

impose cumulative operational and economic costs. Success has been defined less by single-strike destruction than by repetition, disruption, and forcing the adversary to defend widely and continuously.

The Ukrainian experience highlights the decisive role of economics, availability, and survivability in deep strike. Scarce, high-end missiles deliver decisive effects but cannot be scaled, while lighter, cheaper systems impose persistent pressure despite limited payloads. The effective deep-strike posture, therefore, emerges from a layered mix of capabilities rather than from any single weapon system. This logic challenges traditional Western concepts that equate deep strike primarily with exquisite precision munitions.

Main lesson learned: Effective deep strike in modern war is a campaign logic built on layered, economically sustainable systems, not a capability defined by a single class of high-end weapons.

Table of contents

Introduction

The war in Ukraine has served as a real-world laboratory for 21st-century conflict, fundamentally reshaping the doctrine of modern warfare. It has demonstrated that a highly adaptable force, leveraging accessible, networked, and often commercial-grade technology, can effectively contest a larger, conventionally superior opponent. The battlefield integration of dual-use tools—from cheap, mass-produced drones and resilient satellite communication links to AI-enhanced software—is no longer a supporting factor, but a core element of modern military power.

This conflict reveals a profound shift: success on the modern battlefield depends less on the individual capability of legacy "platform" weapons and more on the systemic interaction and synergy of interconnected technologies—an operational ecosystem encompassing air, land, maritime, and digital spaces. The lessons from Ukraine underscore a new logic of warfare defined by speed of innovation, rapid adaptation, and seamless technological integration.

The report analyses the military technology (MilTech) development and defines emerging technology trends in the Russo-Ukrainian war and their influence on future warfare. Each part of the report concludes with lessons for the North Atlantic Treaty Organization (NATO) on specific technologies and covers the technological developments between 2022 and 2025.

Ukraine's MilTech ecosystem—often referred to as a wider Defense Technology, or DefTech, environment[1]—is a dynamic network comprising government bodies, industry players, and civil society actors that has undergone significant transformation since 2022. At the state level, the Ministry of Digital Transformation has been pivotal, spearheading the creation of Brave 1, a specialized agency that serves as the primary entry point for over 2,000 private start-ups and small-to-medium enterprises. Brave 1 assists these companies in finding investors and international partners, providing state grants, facilitating NATO equipment codification, and connecting innovators with government procurement lists. The ecosystem is further supported by the official organizations between the Ministry of Defense (MoD) and Ukrainian Armed Forces, which focus on scaling up frontline priorities through R&D funding and testing solutions

1. MilTech is about designing and producing war-specific weapons and equipment, whereas DefTech is about the end-to-end system (industrial, procurement, integration, and scaling processes) that turns technologies into fielded defense capabilities. See K. Kistol, "Defence-tech vs. Mil-tech. What's the Difference?", Defence Builder Accelerator, July 21, 2024, available at: https://defencebuilder.com.

on the battlefield to gain a military advantage through asymmetric innovation.

The industrial landscape has shifted from dominance of legacy state companies to a renaissance of the private sector, characterized by a rapid surge in autonomous and digital technologies, electronic warfare (EW) systems, and robotic platforms. While state-owned enterprises have been reorganized into the Ukrainian Defense Industry (UDI) joint-stock company to improve compatibility with Western partners, the private sector drives much of the current innovation. This ecosystem prioritizes the mass production of workable, affordable and modular solutions over perfect luxury products, allowing Ukraine to increase the share of domestically made weapons used on the frontline from 10% in 2022 to 40% in late 2024. Despite this growth, the industry faces a financial crunch, as the government currently has the budget to purchase only about one-third of the country's total domestic production capacity.

Central to this innovation cycle is the Armed Forces of Ukraine, which act as the primary user and feedback provider, ensuring that technology evolves daily to counter rapidly changing Russian advancements. Civil society non-governmental organizations (NGOs) like Come Back Alive, the Prytula Foundation, and Dignitas/Victory Drones play an unprecedented role by not only fundraising heavy equipment but also providing large-scale technical training for hundreds of thousands of personnel. To overcome domestic investment barriers and export restrictions, many Ukrainian deftech entrepreneurs are now opening subsidiaries in Europe to qualify for Western funding while maintaining their battle-proven technological edge. Ultimately, the ecosystem offers European partners a unique value proposition: a partner with high manufacturing adaptability and intimate knowledge of enemy innovations, capable of producing critical technology at a much lower cost than Western counterparts.

This report analyzes eight critical technologies that define modern warfare. They come across three core domains.

Part 1 focuses on the autonomy domain and analyzes the impact of unmanned aerial, ground and surface naval drones (UAVs, UGVs, USVs), electronic warfare countermeasures, and the crucial role of AI-enabled platforms in navigation and intelligence, surveillance, target acquisition, and reconnaissance (ISTAR).

Part 2 examines the information domain, focusing on the strategic value of connectivity (epitomized by Starlink) and the development of situational awareness/information battle management systems like the Delta, which fuse data for real-time decision-making.

Part 3 on adaptation of firepower analyzes the dynamics of deep strike and missile warfare, including the challenges to air and missile defense and the economics of firepower and salvo competition issues.

These findings are based on interviews with Ukrainian military, industrial, civil society and government actors conducted during research trips to Ukraine, specialized conferences and open sources, including military bloggers, think tanks, printed and audio Ukrainian and Western media, and specialized reports by relevant research centers, and peer review journals.

Research methodology limitations included the sensitive nature of the Ukrainian defense industry during active hostilities. As a result, not all approached companies were willing to participate in interviews or share technical data due to the country's regulation on data sharing and the need for data protection, operational security, and user security (on the frontline). Furthermore, fast-paced technology innovation in the fields of drones, Artificial Intelligence (AI), and electronic warfare in particular means that tactical lessons can become outdated within weeks.

The rise of autonomous warfare

The contemporary battlefield in Ukraine is defined by an unprecedented technological transformation, where unmanned systems have become the dominant force, altering both combat tactics and operational security. Drones now supplant traditional scouting, with lightweight platforms like the Mavic 3 and Autel Evo 3 Pro handling frontline reconnaissance, while larger systems perform deeper penetration. 70-80% of all combat in selected sectors along the frontline is led by unmanned aerial vehicles (UAVs), primarily First Person View (FPV) drones and strike drones (or "bombers"), signifying a shift from traditional firepower, resulting in the inability of both adversaries to establish any form of air superiority over the battlefield.[2]

This drone saturation has made visual and thermal observation omnipresent, superseding radio-frequency detection, with multiple enemy UAVs continuously observing every kilometer of the front. Consequently, traditional tactics have changed: soldiers now operate in small groups of 2-3 personnel to avoid forming lucrative targets. Overhead cover has become vital, and any land maneuver is deadly due to battlefield transparency, impairing logistics and evacuations.

Starlink remains a critical backbone for communication. However, its latency and vulnerabilities require alternative systems for short-range communication. The use of fiber-optic cables for drone control has partially neutralized EW equipment.

Both sides are in a race to reverse-engineer and copy each other's innovations, creating an arms race scramble for technological advantage.[3] The next ongoing development in drone technology is the rise of robotic platforms, which combine several autonomous and conventional weapons systems with battlefield management systems. The focus has shifted from individual drone technology developments to coordination mechanisms between multiple aerial, ground and naval platforms.

In contrast to the Unmanned Aerial Vehicles (UAVs) and naval drones, the Unmanned Ground Vehicles (UGVs) remain in the adaptation phase, even though successful applications exist in kill-zone evacuations and

2. Interview by Eastern Circles with unmanned systems control platoon commander Captain Oleksandr Yabchanka, Ukraine, November 12, 2025.
2. Ibid.

logistics. Whilst aerial and maritime drones have transitioned to a platform coordination development logic, ground systems are still adapting core technologies to meet current battlefield conditions.[4]

Unmanned platforms

Unmanned Aerial Vehicles (UAVs)

The evolution of UAVs in the Russo-Ukrainian war progressed through 8 distinct phases from 2022 to 2025, transforming from simple reconnaissance tools into sophisticated, AI-coordinated weapon systems. This part doesn't include analyses of fixed-wing drones for Intelligence, Surveillance, and Reconnaissance (ISR) strike, and important function-type (relays and com' drones), while more focuses on contact line drones.

- Beginning in spring 2022, commercial DJI Mavic drones revolutionized battlefield awareness by enabling Ukrainian forces to detect Russian columns beyond the horizon (8-10 km range), fundamentally disrupting the Cold Warlegacy of armored warfare tactics, including the development of the Main Battle Tank (MBT) design, the advent of mass mechanization, and the introduction of Anti Tank Guided Missiles (ATGMs).
- Russia responded with large-scale electronic warfare systems mounted on trucks, prompting Ukrainian adaptations including signal amplifiers, remote antennas, and dual batteries that extended range to 10.5 km by autumn 2022.
- Early 2023 marked a paradigm shift with the introduction of First Person View (FPV) drones capable of direct strikes, adding kinetic engagement to reconnaissance capabilities—transitioning the battlefield to "continuous detection -> forecast/control -> strike".
- This sparked an escalating EW arms race throughout 2023, with jamming systems miniaturizing from multi-ton trucks to personal 1-30 kg devices, while SIGINT identified drone frequencies for targeted jamming.
- The emergence of fiber-optic-guided drones in 2024 fundamentally undermined frequency-domain warfare, where such systems were employed. The use of physical optical cables (5-15 km) removed the EW attack surface, compelling a transition from electronic suppression to predominantly kinetic countermeasures.
-

4. Interview by Eastern Circles with Ukrainian expert on defense industry in Ukraine, Kyiv, December 2025.

- Simultaneously, attacking drones evolved into heavy bombers ("Baba Yaga") carrying 20-40 kg payloads, establishing logistics as the third core UAV function alongside reconnaissance and fire engagement.
- By 2025, machine learning and AI integration emerged as the tactical gamechanger: target auto-acquisition systems, robot-versus-robot combat scenarios (AI-guided FPVs attacking AI-defended ground platforms).
- It set out the race toward full AI coordination of multiple systems—where command centers could receive data from all reconnaissance drones, analyze situations, and autonomously task FPVs, ground robots, and artillery within seconds rather than minutes.

This evolution increased drone-inflicted casualties from under 10% in 2022 to over 70-80% by 2025, with production scaling from tens of thousands to millions per year between 2023 and 2025. Future strategic advantage now hinges on whoever achieves mass AI integration first—a race where Russia and China's combined resources and battlefield data collection pose an existential challenge to Ukraine and NATO. This advantage will depend on the development of AI applications from situational awareness today to autonomous decision-making, with increased strike, precision and efficiency rates.[5]

The evolution of aerial warfare in Ukraine between 2022 and 2025 demonstrates a profound shift in how frontline forces approach the contest between unmanned systems and air defense along the line of contact, due to the weakness of both adversaries in the air domain. What began as a conflict defined by high-altitude assets and a centralized, heavy radar-guided missile system transformed into the air battle of mutual denial.

In the first months of 2022, large and slow platforms like the Bayraktar TB2 were hard to counter by expensive, layered Soviet-era air defense architecture, facilitating reconnaissance and strike missions, contributing to the degradation of the mechanized columns advancing toward Kyiv and assisting in the recapture of Snake Island in the Black Sea.[6]

Ukraine entered the full-scale invasion in 2022 with very little home production.[7] By 2025, the proliferation of cheap FPV drones and unjammable fiber-optic technologies, operating in a larger system, which includes also fixed-winged ISR/strike platform (like Furya, Leleka-100 and others), relays and communication drones, forced a radical decentralization of defense, pushing protection down to the individual soldier and vehicle

5. Interview by Eastern Circles with unmanned systems control platoon commander Captain Oleksandr Yabchanka, Ukraine, November 12, 2025.

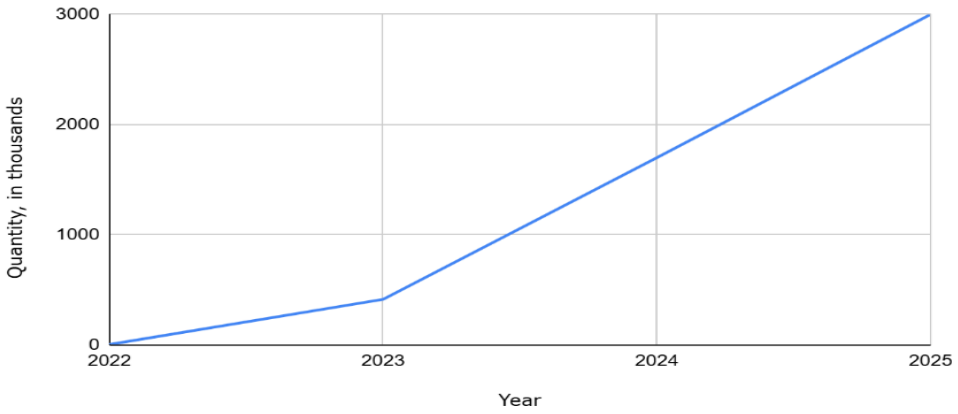
6. D. Khachatryan, "In Search of Bayraktar: From Myth to Margin in Modern Warfare", EVN Report, February 20, 2022, available at: https://evnreport.com.

7. S. Hacaoglu and O. Ant, "Ukraine Buys More Armed Drones from Turkey Than Disclosed", Bloomberg, December 3, 2021, available at: www.bloomberg.com.

through kinetic interceptors, specialized infantry weapons, and physical barriers rather than reliance on massive surface-to-air batteries.

Alongside these larger platforms, Ukraine relied heavily on commercial off-the-shelf (COTS) quadcopters, particularly DJI systems such as the Mavic series, which had been commandeered for military purposes since 2014.[8] These inexpensive platforms were rapidly modified to carry small munitions and became central to reconnaissance and light strike operations across the front.

Chart 1: The growth of FPV production in Ukraine



Source: B.Kostiuk, "Strategic Adaptation and the Rise of Sustainable Air Defense", Eastern Circles, January 12, 2025, available at: www.easterncircles.com.

2024 saw a sharp rise in FPV and small UAV production on both sides. Ukrainian defense companies produced over 2 million FPV drones in that year, and more airframes began to carry simple onboard autonomy.[9] Even modest navigation and aiming algorithms raised hit rates against moving vehicles and entrenched positions compared to purely manual control. Both sides experimented with swarms and carrier platforms as they tried to exploit this mass. Ukrainian units began flying small groups of drones in coordinated attacks, usually three to 8 platforms working together against one local objective, and tests showed that larger formations were technically feasible if control and deconfliction could be maintained.[10] As drone use expanded, tactical adaptation spread down to the level of infantry weapons.

8. A. Thomas, "Drones sur le champ de bataille : quelles leçons tirer de leur emploi par les forces ukrainiennes ?" [Drones on the Battlefield: What Lessons Can Be Learned from Their Use by Ukrainian Forces?], Fondation pour la Recherche Stratégique (FRS), June 2022, available at: www.frstrategie.org.
9. N. Sobenko, "Зеленський: 2024 року Україна виробила 2,2 мільйона FPV-дронів, у 2025-му зробить більше" [Zelensky: Ukraine Produced 2 Million FPV Drones in 2024], Suspilne, February 23, 2025, available at: https://suspilne.media.
10. Y. Kuzmenko, "Умєров: Україна перша у світі запровадила технологію 'рою дронів'" [Umerov: Ukraine First in the World to Launch Swarm Drone Technology], Suspilne, September 23, 2024, available at: https://suspilne.media.

Table 1: UAV evolution 2022 vs 2025 of contact line drones

Characteristics	2022	2025
Drone type	Mavic (ISR)	Mavic, FPV, bombers, etc.
Functions	reconnaissance	Reconnaissance, strike, logistics, evacuation
Mavic range	8-10 km	10-15 km (with amplifiers)
Optic fiber	-	Massive use of optic fiber drones
AI	NA	Guidance, recognition, coordination
Losses from drones	<10%	>70% of casualties on the frontline
Production (both sides)	Thousands by end of 2022	Millions/year

Ukraine experimented with fiber optic drones beginning in 2022, but had a hard time scaling up production, while the Russians saw the technology and ramped up production beginning in November 2024.[11] They sent command and video signals along a thin cable instead of through the radio, which made them immune to jamming or spoofing and left no radio signature to detect, while also degrading flight performance by making the systems heavier, slower and more difficult to control. The drones can fly just above ground level, through trenches or streets, and even inside buildings, yet keep a stable connection. Russian fiber-optic drones fly 10-25 km, now reaching 50 and even 65 km according to selected reports.

Key lessons learned – frontline UAV and FPV

- The development of the small UAV enterprise on the Ukrainian battlefield must not be interpreted as the replacement of traditional airpower: on the contrary, it is both a natural evolution of the land battlefield in the face of the available technology and of the weakness of both adversaries in the air domain. Air power and the dronization of land warfare are not mutually exclusive.
- Maintaining a UAV offensive and defensive advantage requires continuous adaptation, including in the EW and AI fields. Two lessons to keep this advantage are domestic production and training.
- Domestic production dependence on Chinese components (chips, magnets, motors, batteries) creates acute supply chain vulnerabilities

11. "Дрони на оптоволокні: особливості, переваги та недоліки" [Drones on Fiber Optics: Features, Advantages and Disadvantages], Taifun.army, May 20, 2025, available at: https://taifun.army.

for both Russia and Ukraine. Chinese export restrictions have shown the importance of an autonomous production strategy along the supply chain of most in-demand technology (drones, C-UAV, EW).

- Modern weapons like UAVs are part of a complex system, including fixed-wing drones for ISR and strike, relays and communication drones, and a system of integration that makes them interoperable. This system is most effective alongside weapon systems. NATO countries are running the risk of downplaying the tactical role of drones and the urgency of acquiring this technology by centering the discussion on quantity, firepower inferiority or short upgrade cycles. Instead, NATO should focus on drone-related training, both of its engineers and operators, not to fall hopelessly behind Russia.
- The biggest lesson Ukraine has derived from the war is the need to train people early, as the training cycles cannot be shortened. The training itself should focus not on developing a new life-long skill, but on growing hands-on, creative expert teams. The key skill is the ability to adapt, innovate, and improve in several fields simultaneously. This requires creating a safe space to experiment within the military (as Russians and Americans started already, and as Europeans need to start doing as well).[12]
- Russia's faster production scaling capabilities provide an advantage to Moscow at present. If NATO is to face Russian military threat, it has to invest in modular production capacities, which it can ramp up when needed.
- The technological edge that will give tactical superiority on the battlefield now hinges on whoever achieves the first mass AI application in drone warfare, from situation awareness, reconnaissance, navigation, communication, and one-pilot swarms control at scale, and automated decision-making, shortening the kill chain to seconds.[13] This is why autonomy is a key advantage in future wars, grasped by Ukraine, and not to be underestimated by NATO European allies.
- Systematic battlefield data collection for the training of Chinese and Russian AI models poses a risk for NATO to lose the technological competition if they fail to accelerate their own autonomous drone programs and recognize that this conflict is defining the future character of warfare itself.
- Closer long-term cooperation with Ukraine is a guarantee not only that NATO's arsenal will reflect the demands of modern war, but its training and strategy will do so, too.

12. Interview by Eastern Circles with Pavlo Horyachev, UAV&UGV Instructor, Engineering expert, Dignitas Fund, Ukraine, December 10, 2025.
13. Ibid.

Unmanned Surface Vehicles (USVs)

Ukraine's naval-drone campaign reflects a transition from improvised, isolated uncrewed surface vessels (USV) strikes to a coordinated, multi-domain operational system.[14] It can be divided into three stages between 2022 and 2025:[15]

- **2022-2023:** Ukraine develops and successfully tests its naval drones against Russian military ships. Two key models emerge: SeaBaby, whose development by a private company is supervised by Ukraine's Security Service (SBU) and Magura, whose developer works closely with Ukraine's Main Intelligence Directorate (GUR). During these stages, Ukraine conducted few ad hoc USV raids, often designed as one-off attacks against single targets.[16]
- **2023-2024:** USV development incrementally allows the employment of groups of drones. This approach enabled successful, more complex operations against Russian targets.
- **2024-2025:** the management of several groups of tens of USVs simultaneously is made possible, each group with a different function. USV operations develop into planned, multi-axis strikes that combine USVs with UAVs and under-water drones, cruise missiles, electronic-warfare capabilities, mounted turrets shooting targets up to 400 meters away, mounted small-caliber missiles and C-UAV systems, which use USV as a take-off platform, including for SOF operations.[17]

These developments allowed Ukraine to diversify its target set.[18] Initial efforts focused on Russian naval vessels in port and at sea, but later operations included logistics infrastructure, air-defense assets, "shadow fleet" ships, helicopters and fighter jets sent to neutralize Ukrainian naval drones. This expanded the campaign from localized sea denial to broader economic and operational impacts.

USV impact in the Black Sea

Open-source assessments indicate that Ukraine has disabled or destroyed 1/3 of the pre-war Black Sea Fleet through a mix of USVs, missiles, and UAVs, including major vessels such as the cruiser Moskva (with Neptune

14. C. Buchatskiy, "The Black Sea's Asymmetric Blueprint: Operational Lessons from Ukraine for 21st-Century Naval Forces", Snake Island Institute, October 10, 2025.
15. Interview by Eastern Circles of Oleksiy Honcharuk, Co-founder and Head of the Board UFORCE, Ukraine, January 2025.
16. R. Romaniuk, What We Will Fight with in World War III? New Ukrainian Weapons. [Чим воюватимуть у третій світовій? Нова українська зброя.] Лабораторія. Kyiv 2025; C. Buchatskiy, "The Black Sea Asymmetric Blueprint", Snake Island Institute, October 10, 2025.
17. Interview by Eastern Circles with Oleksiy Honcharuk, Co-founder and Head of the Board UFORCE, Paris, January 7, 2026.
18. T. Pak, "Taiwan's USV Development and Strategic Learning from Ukraine", Center for Maritime Strategy, June 6, 2025.

missiles), the landing ship Caesar Kunikov, and the corvette Ivanovets (through USV attacks).[19] These losses, combined with repeated strikes on infrastructure in Crimea, have forced Russia to pull key combatants to safer ports like Novorossiysk and sharply curtailed amphibious and blockade operations near Ukraine.

USV operations have also contributed to reopening limited grain export routes by reducing Russian freedom of maneuver and creating persistent risk to Russian warships and supporting vessels along key export lanes. Recent USV "wolf-pack" (multiple autonomous or semi-autonomous naval drones (USVs/UUVs) in coordinated swarms to overwhelm enemy defenses, mimicking wolf pack hunting tactics) attacks against Russian "shadow fleet" oil tankers demonstrate that Ukraine can now threaten economically critical shipping far from its coastline, raising the strategic cost of Russia's Black Sea operations.[20]

Over time, USVs did not result in the Russian loss of the Black Sea. However, they enabled Ukraine's Black Sea presence and the freedom of navigation, contributing to the establishment of a roughly 100-nautical-mile risk zone for the Russian navy off occupied Crimea. USVs also restricted Russian military action ability in the Black Sea and led to the repositioning of Russian vessels away from the Crimea, mainly to Novorossiysk.[21] The Ukrainian model of USV technology integration, doctrine, and military-government-industry coordination can be used by other small and mid-size countries to counter larger navies.

Main technologies

Ukraine's USV ecosystem now includes several families of naval drones such as the MAGURA V5 series, Sea Baby, and other indigenous or adapted platforms, many configured as explosive one-way attack craft with long range and high payload capacity. These USVs are increasingly integrated with ISR and strike networks, using UAVs for targeting, commercial satellite and Starlink for control, and land-based anti-ship missiles (e.g., Neptune variants and Western systems) to exploit gaps opened by USV attacks.[22]

Electronic warfare, camouflage, and low-signature designs have been used by Ukraine to evade Russian radars and coastal defenses, while simple

19. G. E. Howard, "Hunter and Prey in the Black Sea: Ukrainian USVs Target the Russian Shadow Fleet in a Return to Unrestricted Warfare", Ukrainian Congress Committee of America, December 2, 2025, available at: www.lucorg.com.
20. Interview by Eastern Circles with Oleksiy Honcharuk, Co-founder and Head of the Board UFORCE, Paris, January 7, 2026.
21. H. P. Midttun, A. Frolova, A. Klymenko, and A. Ryzhenko, "The Impact of Ukraine's Asymmetric Approach on Russian Sea Power in the Black Sea: Complex Evaluation of the Russia Black Sea Fleet Capabilities", Centre for Defence Strategies, April 2024.
22. Snake Island Institute, op. cit.

commercial components keep costs low and enable rapid iteration of hulls, propulsion, and warhead configurations.

Satellite communication by Starlink remains a key pillar of USV connectivity. Using UAVs as repeaters is possible, but far less used due to greater distances at sea than on land or in the air.

Table 2: Illustrative outcomes and technologies

Aspect	Ukrainian outcomes and tools
Fleet attrition	About one-third of the Russian Black Sea Fleet disabled or destroyed via combined USV, missile, and UAV campaigns.
Geographic effect	De facto 100-nautical-mile buffer limiting Russian operations near Ukraine's coast and Crimea.
Key ship losses (examples)	Moskva (Neptune missile strike), Ivanovets and Caesar Kunikov (USV-centric attacks), plus multiple support and patrol vessels.
Core USV platforms	MAGURA V5 family, Sea Baby and similar explosive USVs, often networked with UAV ISR and land-based missiles.
Targets beyond warships	Oil tankers in the "shadow fleet," logistics ships, port and air-defense infrastructure in Crimea and Novorossiysk.

Source: Eastern Circles, based on own interviews and the. C. Buchatskiy, "The Black Sea's Asymmetric Blueprint: Operational Lessons from Ukraine for 21st-Century Naval Forces", Snake Island Institute, October, 2025.

Russia's countermeasures—booms, nets, small arms, and ad hoc patrol craft —have struggled against combined attacks, underlining the advantage of attritable, fast-evolving unmanned systems over slow-to-adapt traditional defenses. However, Russian countermeasures continue to evolve alongside Ukrainian USVs, and their development makes Novorossiysk a challenging objective for Ukrainian naval drone operators.[23]

Key lessons learned – USV

- Sea denial and strategic impact are achievable without a conventional navy when unmanned systems are integrated into a multi-domain concept that links USVs, UAVs, missiles, and cyber/EW.
- Defensive operations with USVs have yielded a favorable cost-value ratio for Ukraine, destroying far more expensive and complex Russian

23. Interview by Eastern Circles with Oleksiy Honcharuk, Co-founder and Head of the Board UFORCE, Paris, January 7, 2026.

military vessels (and more recently, helicopters and jets) with relatively cheaper USVs.

- However, USVs alone are not enough to dominate the sea. A combination of USVs and conventional military vessels is needed for this purpose.
- The role that can be played by the USVs and multi-function robotic platforms to strengthen NATO sea and coastal security has to be integrated into the NATO naval doctrine and strategy.
- The development of this sector also underscores the necessity to review the integrated port/coastal defense to increase the security of maritime infrastructure and economic shipping routes, whose vulnerabilities will be exploited in future conflicts.
- The key innovation lesson from the use of the USVs for Ukrainians has been not about replacing one type of weapons with another, but about preparing the teams capable to integrate innovation to enhance conventional military and special operations.[24]

Unmanned Ground Vehicles (UGVs)

The 4 years of war in Ukraine have made the battlefield ultra-transparent, X-rayed by UAVs, and no longer usable by tanks or large armored vehicles, which have become easy targets. Instead, Ukraine is increasingly using unmanned ground vehicles (UGVs)—compact robotic systems—to deliver supplies, evacuate casualties, mine, demine, and strike targets. Drones combined with the lack of medium- and high-altitude air superiority on both sides made large-scale mechanized operations in Ukraine unfeasible.

Ukraine's current UGV technologies in Ukraine are at a technology-testing phase, rather than finalized and developed systems. This limitation is due to the evolving operational environment. Rapid changes on the battlefield compel manufacturers to continuously refine existing solutions or develop new ones, as the battlefield is a living laboratory to identify further roles, refine communication systems, and understand the limits of autonomy under electronic warfare (EW) pressure.[25]

UGV development

UGVs are treated as disposable, adaptive tools, not yet durable assets. Their chief advantage is cost efficiency (in comparison to large-scale, often vehicle-mounted or fixed-site army vehicles) and reduced human risk: losing a robot is better than losing a soldier. Despite their growing

24. Interview by Eastern Circles with Oleksiy Honcharuk, Co-founder and Head of the Board UFORCE, Paris, January 7, 2026.
25. Interview with Ukrainian developer of UGV, Kyiv, December 2025.

resilience (many UGV models can function after several FPV drone strikes), it is still hard for them to reach the *last mile*, where UAV reconnaissance makes UGVs visible and vulnerable to attacks.

The UGV accessibility of the "frontline zone" of 50-60 km, including the "kill zone" of 20-30 km area where any movement is detected and targeted due to drones-enabled visibility, is further complicated by the landscape fast changing by the fighting, debris, destroyed equipment and corpses, all representing obstacles to overcome for a UGV, with a risk of being stuck and failing its logistics or evacuation mission.[26]

The main objective behind further UGV development in Ukraine for frontline soldiers now is to increase their use as offensive weapons, with the help of mounted automatic turrets, to sustain defensive frontline positions and facilitate logistics, evacuations and rotations.[27]

Technological bottlenecks

The central constraint for UGV operations is communication reliability. Maintaining stable control links in contested EW is the defining challenge. Ukrainian developers have tested several solutions:

- Mesh networks to maintain redundancy due to the difference in terrain elevation;
- UAV-based relay systems to extend operational range—although these are easily detected;
- Satellite communication (Starlink mostly) now mitigates range issues despite obvious limits, such as loss of connection under foliage.

The maturity of these solutions remains uneven; operationally, most UGVs still rely on manual or semi-autonomous control (more frequently) within line-of-sight ranges and need constant maintenance on the frontline because of the threat intensity.[28]

Integration limits and AI use

Air-ground integration is functional but rudimentary—UAVs often guide or observe UGVs, yet full tactical coordination is rare. AI applications in Ukraine tend to emphasize target tracking, logistics under comms loss, and visual contrast detection for fire correction, but not autonomous lethal engagement.

Thermal and visual signatures remain unsolved vulnerabilities. Hot engines, batteries, and motors make UGVs easily detectable on thermal

26. Interview with a front-line infantry serviceman in Ukraine, December 8, 2025.
27. Interview with a front-line drone unit operator, December 15, 2025.
28. Interview with Ukrainian developer of UGV, Kyiv, December 2025.

images. Cost-effectiveness considerations (700,000 USD per system on average) do not allow for extensive work on thermal camouflage.[29]

Table 3: Main UGV Types deployed in Ukraine

Type	Price Range (USD)	Primary Function
Logistical carriers ("Mule", Murakha)	$3,000–$95,000	Supply delivery, ammo transport to forward positions
Casualty evacuation ("Ratel Ht" platforms)	$20,000–$70,000	Wounded extraction under fire, short-range medevac
Reconnaissance scouts (Sirko-S1)	$8,000–$25,000	Route scouting, thermal/visual intel relay to UAVs
FPV-Enabled strike UGVs (Karakurt)	$50,000–$70,000	Direct assault, loitering munitions on ground targets
Multi-Role hybrids ("Lyut", Protector, D-21-12R)	$30,000–$100,000+	Combined logistics/recon/strike with modular payloads

Sources: Market-Brave1; Braveinvetors; Bibliotech.ua, 2035.

Key lessons learned – UGV

Ukraine's UGV experience highlights a partiality to sound, practical solutions rather than over-engineering:

- **Ukraine's UGV development demonstrates that warfare has shifted from large platforms to adaptive swarms of low-cost systems.** Real innovation lies in the rate of adaptation, not in any single robotic design.
- **Reject "Wunderwaffen" thinking**. Over-engineered Western systems use only a fraction of their potential in field conditions. Ukraine's approach favors pragmatic field usability over perfection.
- **Prioritize scalable ecosystems**. Integration with existing logistics, EW, and drone networks matters more than achieving "ideal specs."
- **Scale to threat, not prestige**. The economic logic (producing dozens of UGVs instead of or alongside one tank) defines resource-conscious warfare.
- **Test continuously**. Technologies evolve fastest "at the point of change": engineers, soldiers, and repair crews share direct feedback loops.

29. Interview with Ukrainian developer of UGV, Kyiv, December 2025.

- **Adapt doctrine to resource reality**. Units typically field 2-3 robots per 30 soldiers. They cannot risk losing one robot to save another, limiting UGVs to specialized tasks (casualties evacuation, munition transport, or surveillance).
- Ukraine is not (yet) producing mature robotic technology but rather battle-tested methodologies for rapid prototyping, field feedback, and resource-efficient scaling. In that sense, UGVs serve as a visible embodiment of Ukraine's broader defense innovation model: **learn fast, build cheaply, adapt instantly**.[30]

Electronic warfare

As radio-controlled systems like UAVs and USVs came to dominate the battlefield, and connectivity pervades every weapons system into an "Internet of the Battlefield" (IoB), control of the electromagnetic spectrum (EMS) has become ever more important, jamming communications, blinding drones off course, and confusing navigation. Units that could detect and adjust frequencies in real time survive longer. The lesson is that every weapon now depends on protection against interference. Success in electronic warfare requires both technical skill and flexibility at the lowest tactical level. Adaptation, not equipment alone, gave Ukraine an advantage.

One needs to distinguish here between different forms of EW:

- individual electronic attack (jamming a weapons system like a UAV);
- wide range electronic attack (jamming communications on a specific sector);
- SIGINT to locate and listen in on communications;
- spoofing and cyber-enabled signal hacking.

The ubiquity of electronic equipment and reliance on the EMS for coordination and precision fire have transformed EW from a specialized function into a combined arms domain. Mastery of the EMS is a determining factor in military competitiveness.

Russia maintains a highly centralized, hierarchical electronic warfare (EW) system that creates perimeter suppression zones, utilizing powerful multi-kilowatt complexes at the army and fleet levels which effectively blind satellite communications at the altitude above 2 km, affording Russia an advantage in aviation and missile strikes. In response, Ukrainian EW

30. Interview with Ukrainian developer of UGV, Kyiv, December 2025.

primarily focuses on the "operational contact" zone near the front and is less centralized, leading to coordination challenges.[31]

Concurrently, Russia is systematically modernizing its satellite navigation hardware, employing highly resilient phased or modular antennas with increased element counts and sophisticated Russian processors to make classic, broadband Intelligence, Surveillance, and Reconnaissance (GNSS) jamming largely ineffective; this evolution forces a shift toward intelligent EW methods like spoofing (transmitting false coordinates) and sending corrupted data packets to overload receiver logic.[32]

Furthermore, the modern battlefield is witnessing a "race of intelligence" in the face of EW. Contemporary UAVs integrate compact computing modules, and AI accelerators conduct tens of tera-operations per second to enable machine vision and target recognition. Add to this the rise of autonomous swarms, where groups of drones function like "predatory packs" to find and strike targets, and you are facing a future where completely robotic, AI-driven systems hunt humans and equipment, demanding symmetric AI countermeasures for defense.[33]

Key lessons learned – EW

- **EW is essential for survivability and maneuverability:** EW is now critical for the protection of forces in maneuver and enabling successful operations. In Ukraine, EW has shifted from a niche force multiplier to a company-level asset. The ability to disrupt enemy kill-chains (e.g., denying GNSS and communications) is an essential capability for enabling maneuver without unacceptable rates of attrition.
- **Shift to distributed, software-defined systems:** The proliferation of software-defined radios (SDRs) enables these devices to perform a wide range of EW tasks. SDRs, attached to appropriate antennas, transform military vehicles and even widespread UAVs into potential EW baseline positions for integrated sensing. This distribution enhances electronic reconnaissance and improves the survivability of EW teams.
- **EW countermeasures against precision munitions:** EW can significantly degrade the effectiveness of precision rounds; for instance, the effectiveness of Excalibur precision artillery rounds dropped from 70% accuracy to just 6% accuracy at the height of Ukraine's 2023 offensive due to Russian EW efforts. This capability extends to disrupting

31. R. Oberle and D. Patiuk, "Electronic Warfare in the Russian War on Ukraine", Eastern Circles, December 15, 2025, available at: www.easterncircles.com.
32. Interview with NDI POT Scientific Research Institute of Advanced Defense Technologies, Sikorsky KPI, Kyiv, December 4, 2025.
33. Ibid.

a munition or targeting system to ensure a strike misses friendly forces.[34]

- **The rise of adaptive payloads and algorithmic warfare:** EW is moving toward adaptive payloads (software-based attacks) rather than fixed jamming frequencies. The ability to record enemy waveforms allows software to examine and program precise countermeasures. Algorithmic warfare enables the mass generation of bespoke EW payloads to reduce the required jamming power for a specific effect. This requires EW systems to be constantly updated to keep pace with the adversary's rapidly evolving navigation and communications protocols.
- **Synchronization and deconfliction are critical:** Jamming foreign military signals risks collateral damage and fratricide, as jammers can interrupt friendly communications and collapse friendly networks. Consequently, EW effects must be carefully synchronized and deconflicted with other arms, often requiring coordination down to the platoon level. When EW and communications systems use the same SDRs, technical deconfliction becomes theoretically possible, ensuring protocols avoid overlap.
- **Need for cognitive EW systems:** Current budget-friendly EW systems may soon fail to counter rapidly evolving enemy communication technologies. Ukraine must proactively plan for cognitive EW systems that dynamically select frequencies and data protocols; alongside high-powered microwave weapons capable of physically disabling adversary electronic components.[35]

Artificial Intelligence

There are numerous definitions of Artificial Intelligence (AI) formulated by military authorities, helping to clarify how the military sees its scope of application. AI is commonly characterized as coming in three types: narrow ("weak) AI, which excels at specific tasks and represents most current applications; general ("strong") AI, which would outperform humans across all intellectual tasks; and Artificial Super Intelligence (ASI) would surpass humans in nearly everything, including creativity, logic, wisdom, and social skills.[36]

In the Ukrainian war theater, AI functions primarily as a process accelerator rather than a decision-maker without a clear definition and distinction between "autonomy" or "autonomous weapons system". In

34. Interview with Dignitas experts, October 2024.
35. Interview with NDI POT Scientific Research Institute of Advanced Defense Technologies, op. cit.
36. I. Szabadföldi, "Artificial Intelligence in Military Application—Opportunities and Challenges", *Land Forces Academy Review*, Vol. 26, No. 2, June 1, 2021, pp. 157–65, available at: doi.org.

Ukraine, these terms are used to name any platforms equipped with basic autonomous functions.[37]

When analyzing modern military technology in the Russo-Ukrainian war, it is helpful to view computer vision as the sensory foundation for terminal guidance, acting as the "eyes" that process visual data in real time. In practice, this capability is built using Machine Learning (ML), which provides the specific tools to "train" the drone to recognize targets amidst the noise of the battlefield. While Artificial Intelligence serves as the broader theoretical framework for autonomous decision-making, it is the practical application of ML-driven computer vision that allows a drone to identify targets and navigate independently once a pilot's connection is severed. AI offers significant potential for autonomous route planning and tactical adaptation by learning from battlefield experience. It excels at synthesizing vast amounts of data from radars, thermal sensors and GPS to provide a comprehensive operational picture.

However, for the specific task of terminal guidance, computer vision currently outperforms complex AI algorithms due to its speed and cost-effectiveness. In critical combat moments where decisions must be made instantly, computer vision allows for the rapid identification of small or distant objects even in poor visibility conditions without requiring the expensive hardware necessary for deep learning models. The most effective drone systems combine these technologies by using computer vision to capture the immediate visual reality and Artificial Intelligence to make strategic decisions based on that data. Yet for the final strike phase, systems like the VGI 9 rely primarily on computer vision because its deterministic algorithms ensure a reliable and immediate link between detecting a hostile object and engaging it.[38]

So, the general term for "AI" in Ukrainian vocabulary refers to a set of specific software tools that automate the collection of data and the terminal phase of kinetic strikes (known as "last mile targeting systems"). These devices function as companion computers equipped with a camera and a microcomputer that are installed alongside the UAV standard avionics rather than replacing them. Much like an aircraft autopilot, they allow the pilot to hand over control during the final few hundred meters of an attack, which is the critical phase where radio links are often severed by EW or terrain. Due to the complex integration required, these systems are tuned to specific airframes and cannot be swapped in the field.

37. K. Bondar, "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare", Center for Strategic and International Studies (CSIS), March 6, 2025, available at: www.csis.org.

38. "Розумні дрони України: роль штучного інтелекту та машинного зору на фронті" [Ukraine's Smart Drones: The Role of Artificial Intelligence and Machine Vision on the Front], VGI-9, May 2, 2025, available at: https://vgi.com.ua.

Consequently, teams do not carry a universal array of sensors but instead select specific configurations based on the mission profile. They choose between day or night sensors and specific attack algorithms designed for chasing, intercepting or diving onto targets, depending on whether they are hunting ground vehicles or aerial threats. Finally, it is important to distinguish that not all last-mile targeting relies on AI in its broadest sense. While basic systems use simple computer vision to track contrast without the need for training, advanced teams are now fielding systems that utilize true machine learning to classify and distinguish between specific object types, ensuring the drone stays locked even in cluttered or obscured environments.[39]

The war generates unmanageable volumes of data from satellite imagery, intercepted radio calls, and drone feeds. AI tools like Palantir MetaConstellation[40] or the Ukrainian Delta system act as filters. They instantly scan thousands of hours of footage to identify enemy troop movements or specific vehicles. This automation compresses the decision loop from days to minutes by presenting commanders with processed targets rather than raw data.[41]

Evolution of technology

The evolution of this technology began with Phase I, which focused on civilian integration between early 2022 and late 2023. Palantir Technologies, a data analytics firm led by CEO Alex Karp, has significantly supported Ukraine during the war with Russia.[42] Several Ukrainian agencies have employed Palantir's data and artificial intelligence software, including the Ministries of Defense, Economy, and Education. The software is utilized for various purposes beyond battlefield intelligence, such as collecting evidence of war crimes, demining efforts, resettling displaced refugees, and combating corruption. Palantir provided its services to Ukraine free of charge, emphasizing its commitment to supporting its defense efforts.[43]

Clearview AI, a U.S. facial-recognition company, has also contributed to the Ukrainian war effort by providing its tools to more than 1,500 Ukrainian officials. These tools have been used to identify over

39. Authors' interview with the expert on developments on the Ukrainian frontline.
40. G. Grylls, "Kyiv Outflanks Analogue Russia with Ammunition from Big Tech", *The Times*, December 24, 2022, available at: www.palantir.com.
41. N. Kava, "DELTA стала цифровою зброєю на фронті, український ШІ за 2 секунди виявляє ворожу техніку" [DELTA Has Become a Digital Weapon at the Front, Ukrainian AI Detects Enemy Equipment in 2 Seconds], RBC-Ukraine, October 8, 2025, available at: www.rbc.ua.
42. V. Bergengruen, "Tech Companies Turned Ukraine into an AI War Lab", *Time*, February 8, 2024, available at: https://time.com.
43. "Palantir and Ministry of Digital Transformation of Ukraine Strike Reconstruction Partnership", Palantir IR, May 25, 2023, available at: investors.palantir.com.

230,000 Russians on Ukrainian soil, aiding in linking them to alleged war crimes. Clearview AI has benefited from Ukrainian engineers, contributing to improving its product.[44]

The collaboration between tech companies like Palantir and Clearview AI and the Ukrainian armed forces alongside with war necessity signaled a new operational phase from 2024 to the present. This period is characterized by a distinct transition from the use of basic facial recognition software to the deployment of specially trained models for terminal guidance modules in Ukrainian drones and their integration with the Delta situational awareness system.[45]

By leveraging this private sector expertise, Ukraine aims to position itself as a global research and development lab where companies can address complex operational challenges and validate their products in real war conditions. Following this pattern, Ukraine made AI a foundational element of its defense strategy. The country concentrated on enabling the creation of autonomous reconnaissance drones and combat platforms that operate effectively even in electronically contested environments.[46]

A prime example of this capability is the Saker Scout, which is an indigenously produced drone capable of independently identifying up to sixty-four types of military targets, including heavy armor, and transmitting coordinates for strikes despite enemy jamming.[47] This hardware is supported by sophisticated software ecosystems like the Griselda intelligence system, which processes vast amounts of data from satellites and drones in mere seconds, and the GIS Arta system, which significantly reduces the time between target detection and artillery engagement.[48][49] Furthermore, the Delta situational awareness system utilizes cloud technologies and AI to integrate these diverse data streams and coordinate operations across units.[50]

44. V. Bergengruen, "Ukraine's "Secret Weapon" Against Russia Is Clearview AI", *Time*, November 14, 2023, available at: https://time.com.
45. O. Yan, "Україна використовує штучний інтелект для розвідки поля бою" [Ukraine Uses Artificial Intelligence for Battlefield Reconnaissance], Militarnyi, September 13, 2025, available at: https://militarnyi.com.
46. Y. Pidhayna, "Стрибок ШІ в Україні: від бойових дронів з комп'ютерним зором до невідворотності регулювання галузі та ШІ-міністра в уряді" [AI Leap in Ukraine: From Combat Drones with Computer Vision to the Inevitability of Industry Regulation and an AI Minister in the Government], Mind.ua, October 17, 2025, available at: mind.ua.
47. J.-J. Mercier, "IA de combat : Saker entre en scène" [Combat AI: Saker Enters the Scene], Areion24, January 30, 2024, available at: www.areion24.news.
48. D. Zikusoka, "How Ukraine's 'Uber for Artillery' Is Leading the Software War Against Russia", New America, May 25, 2023, available at: www.newamerica.org.
49. K. Tupikov, "Ukrainian AI-Enforced Defense Tech Griselda Raises USD 600K to Enhance Situational Awareness", ITKey Media, March 21, 2025, available at: itkey.media.
50. "Технологічна перевага на полі бою: в Україні офіційно впровадили систему DELTA з елементами ШІ" [Technological Advantage on the Battlefield: Ukraine Officially Introduces DELTA System with AI Elements], ArmyInform, August 6, 2025, available at: https://armyinform.com.

On the ground, Ukrainian developers have introduced robotic combat solutions such as the DevDroid automated turrets and the Droid TW complex.[51] These systems utilize computer vision to detect and track hostile forces autonomously, day or night, while allowing operators to remain at a safe distance. While Russian forces are also integrating automatic guidance into platforms like the Lancet loitering munition, Ukraine has established a leadership position in the combat application of FPV drones. By incorporating AI, these inexpensive platforms can navigate without GPS to bypass electronic warfare and execute terminal attacks in a semi-autonomous mode once a target is locked.[52]

Assessments of drone swarming remain mixed. Ukraine has experimented with elements of swarm-like coordination, but current battlefield use is largely limited to small groups of UAVs rather than full-scale autonomous swarms. In practice, these systems enable limited autonomous teaming, allowing several drones to coordinate routes, roles, and timing, thereby reducing operator workload rather than fully replacing human control.[53]

The Ukrainian company Swarmer is a promising developer in this space. Its software translates human-defined objectives into tactical actions and is trained on data from more than 82,000 combat missions to approximate experienced pilot behavior in real time. Ukrainian units using the system typically deploy three to eight drones simultaneously, which falls short of the hundreds of platforms often associated with "true" swarming in military theory.[54]

Despite successful demonstrations and plans to scale to larger formations, frontline military personnel remain cautious.[55] Key constraints include maintaining reliable communications in contested environments, network saturation, increased platform costs, and the difficulty of deploying AI systems in highly dynamic combat conditions. As a result, drone swarming in Ukraine currently represents an emerging and experimental capability rather than a mature, scalable battlefield solution.

At the same time, the widespread deployment of ground-based robotic systems or unmanned ground vehicles (UGVs) with artificial intelligence technology has not yet occurred. Most often, this is because integrating artificial intelligence into a ground drone is even more challenging. Since it

51. "Droid TW: роботизований кулемет, наче з фантастичного фільму" [Droid TW: A Robotic Machine Gun Like Something Out of a Sci-Fi Movie], Ministry of Defence of Ukraine, April 25, 2025, available at: https://mod.gov.
52. F. Botton, "The Fourth Law: FPV & AI", Helicomicro, September 9, 2025, available at: www.helicomicro.com.
53. A. MacDonald, "AI-Powered Drone Swarms Have Now Entered the Battlefield", *The Wall Street Journal*, September 2, 2025, available at: www.wsj.com.
54. L. Palchynska, "Ukrainian Startup Swarmer Raises $15M Series A to Scale Battlefield AI for Drone Swarms", Vestbee, September 16, 2025, available at: www.vestbee.com.
55. Authors' interview with the military personnel on the frontline.

moves across terrain that can constantly change due to the nature of combat operations, training AI models becomes extremely difficult, time-consuming, and expensive. However, AI is expected to address staffing shortages. As an example, the founder of Rovertech Borys Drozhak explained that with proper planning and effective implementation of an AI program, a single operator could control multiple drones simultaneously.[56]

Along with being a Living Lab for AI Warfare, these developments raise concerns about the proliferation of advanced technologies and their possible misuse by adversaries.[57] The fusion of technology and warfare in Ukraine is a significant shift in the character of war. The implications for the future of conflict and the role of tech companies as influential actors in military decision-making still need to be studied and explored. The experience in Ukraine illustrates the critical role of AI-enabled systems in modern conflict and can be useful for NATO.

Lessons learned - AI

- **Adopt practical mechanisms, not just ready-made local solutions:** It is important to recognize that NATO nations possess a significantly more mature understanding and classification of military AI than Ukraine. While the Alliance has firmly established development plans and doctrinally integrated AI strategies, Ukraine operates primarily as an agile experimenter, often without clear definitions or a centralized strategy. Consequently, NATO should focus on absorbing the practical mechanisms of AI application demonstrated in the war rather than simply adopting specific local solutions. The Alliance must update its doctrines based on these emerging technologies while remaining mindful that potential future conflicts are unlikely to replicate the specific geography, climate, or countermeasures of the Ukrainian war theater.
- **AI is a process accelerator, not a commander:** The successful integration of systems from US companies like Palantir or Meta, or the development of French-based ComandAI in Ukraine, proves that the primary value of AI in current warfare is compressing the decision loop from days to minutes. AI tools function as advanced filters that scan thousands of hours of drone footage and satellite imagery to present commanders with processed targets rather than raw data. NATO should view these capabilities primarily as tools for "cognitive endurance" and data fusion that support human decision making rather than systems that replace human authority. This distinction is vital because in the absence of a legal framework for machine responsibility, the final

56. Interview by the author with Borys Drozhak, founder of Rovertech.
57. R. Fontes and J. Kamminga, "Ukraine: A Living Lab for AI Warfare", *National Defense*, March 24, 2023, available at: www.nationaldefensemagazine.org.

accountability for lethal force must remain left to a human operator.

- **Realistic autonomy means teaming rather than swarming:** Assessments of drone swarming must remain grounded in technical reality. The text notes that current operations are limited to small groups of 3 to 8 drones rather than massed autonomous swarms due to communication constraints. The lesson for NATO is to focus development on "automated teaming" that reduces operator workload, allowing one person to control multiple assets rather than pursuing the immediate goal of fully autonomous uncrewed formations, which remain experimental and vulnerable in dynamic combat conditions.

Muddling through battlefield transparency: the C4ISR revolution

Space-based technologies for the Ukrainian battlefield

Space-based technologies have been a decisive enabler of Ukraine's battlefield resilience and effectiveness, compensating for structural disadvantages in mass, depth, and legacy ISR by providing persistent connectivity, navigation, and surveillance under extreme contestation. From the outset of the invasion, the survival of Ukrainian command and control depended on rapid access to commercial satellite services, while the subsequent proliferation of drones and precision fires turned space into a tactical dependency rather than a purely strategic enabler. Over the course of the war, these technologies evolved from ad hoc emergency solutions into an integrated space-enabled warfighting ecosystem, increasingly targeted and contested by Russian electronic warfare and strike campaigns. This section, therefore, examines, in turn, the role of Satellite Communications (SATCOM) and the emergence of an "Internet of the Battlefield", the contestation and adaptation of Position, Navigation Timing (PNT) services provided by GNSS, and the growing operational importance of commercial and hybrid space-based ISR.

SATCOM and the Internet of the battlefield

At the outset of the invasion, Russia sought to paralyze Ukraine's national communications through cyber operations (notably the KA-SAT attack), physical destruction of infrastructure, and extensive EW activity.[58] Ukraine's terrestrial networks were heavily degraded, and governmental SATCOM capacity was insufficient to sustain command continuity.

Starlink's first deployment became a strategic inflection point with initial deliveries (Feb–Apr 2022) of approximately 5,000 terminals, supplied through SpaceX, USAID, and private donors.[59] These terminals supported national command continuity, restored government-to-government communications, and enabled Ukraine to reconstitute C2 after Russia's failed

58. M. Kerttunen, K. N. Schuck, and J. Hemmelskamp, "Major Cyber Incidents KA-SAT 9A", European Repository of Cyber Incidents (EuReRepoC), October 10, 2023, available at: https://eurepoc.eu.
59. R. Guarantz, *Satellites in the Russia-Ukraine War*, Carlisle (PA): U.S. Army War College Press, 2024.

decapitation attempts. At this stage, Starlink usage was strategic and operational, not yet integrated tactically. Terminals were scarce; units often exposed them in the open with minimal signature management, creating vulnerabilities that would become apparent only later.

By summer 2022, the number of terminals exceeded 20,000, including large shipments coordinated by Poland—soon to become the largest single-state financier of Starlink support to Ukraine. This scaling transformed Starlink from a strategic stopgap to an operational communications layer, enabling distributed operations, secure messaging architectures (see "Combat software" section below), UAV teams to maintain links under EW pressure. Still, tactical employment remained uneven, with doctrinal integration emerging only later.[60]

By early 2023, public Ukrainian government statements estimated around 42,000 operational terminals across: military units (majority share), hospitals and critical infrastructure, energy operators, humanitarian and private-sector users.[61] This period marks the transition from improvised connectivity to a space-enabled C2 ecosystem. Units increasingly embed Starlink terminals in trenches, bunkers, or armored shelters, while fire support coordination and drone reconnaissance became inseparable from SATCOM usage. The Ukrainian Armed Forces began structuring dedicated digital teams ("operator-signalmen") responsible for managing and protecting battlefield connectivity.

By this time, Russian forces had begun systematically targeting Starlink emissions with artillery, Lancet loitering munitions, and counter-battery fire—exploiting the visual (white housing) and thermal signature of terminals.[62] Ukrainian mitigation practices—burying terminals, adding camouflage and insulation became standard procedure by 2023.

Network maturity

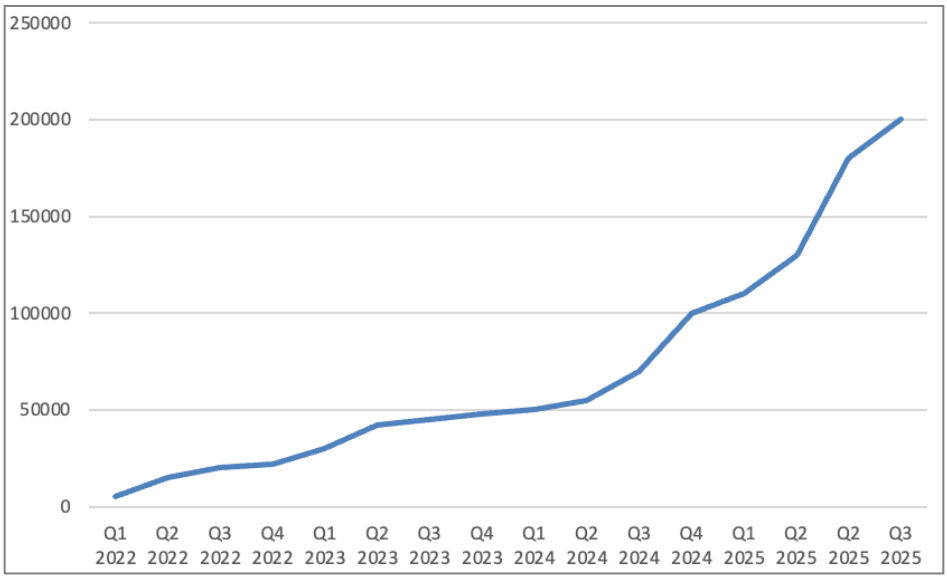
By early 2024, over 50,000 terminals were active nationwide, reaching as many as 200,000 in October 2025.[63] making Ukraine the highest-density Starlink environment in the world, effectively operating a nationwide dual-use tactical-strategic SATCOM grid, capable of supporting thousands of concurrent drone operators, precision-fire cells, and distributed C2 nodes. Such density created massive operational benefits:

- **Resilience:** Russia's large-scale jamming campaigns (Crimea, Kherson, Kupyansk axis) did not collapse Ukrainian C2;

60. P. Gros, V. Tourret, Y. Michel, and G. Garnier, "Enseignements de la guerre russo-ukrainienne", Rapport n°235/FRS/Conflits2035, Paris: Fondation pour la recherche stratégique/Institut français des relations internationales, November 18, 2024.
61. M. Fedorov, Ministry of Digital Transformation briefing, February 2023.
62. Interviews with Ukrainian experts, Kyiv, September 2025.
63. G. Tskhakaia, "Space and the Data Domain: Lessons from Ukraine", Washington, D.C.: Center for Strategic and International Studies, 2025.

- **Tactical autonomy:** platoons and companies could operate with real-time ISR support and rapid long-range strike coordination;
- **Kill-chain acceleration:** SATCOM enabled sub-5-minute sensor-to-shooter cycles across drones, artillery, FPVs, and long-range systems.

Chart 2: Estimated Starlink terminals deployed to Ukraine since 2022



Source: "Starlink and the Early Months of the Ukraine War", The Washington Post*, June 2022; R. Guarantz,* Satellites in the Russia-Ukraine War*, Carlisle (PA): U.S. Army War College Press, 2024; G. Tskhakaia, "Space and the Data Domain: Lessons from Ukraine", Washington, D.C.: Center for Strategic and International Studies, 2025; T. Pultarova, "SpaceX Starlink Internet Isn't Fast Enough for Ukraine's Combat Robots", October 27, 2025.*

Ukraine's near-total reliance on Starlink for strategic and tactical connectivity, alongside the changes in the U.S. global aid approaches, has generated significant operational, political, and industrial vulnerabilities, pushing Kyiv and its European partners to explore alternative SATCOM architectures, including the United Kingdom-European OneWeb constellation.

Mitigating dependency

The principal risk lies in single-provider dependence: activation zones, bandwidth prioritization, and even service continuity ultimately depend on the decisions of one commercial actor, exposing Ukraine to possible restrictions, pricing shifts, or geopolitical pressure. This dependence also creates a systemic target for Russian EW and cyber operations, since degrading one constellation could disproportionately affect Ukrainian C2 and drone operations.

In response, Ukraine has tested OneWeb's Low Earth Orbit (LEO) services, whose key advantages include European political control, strong partnerships with the United Kingdom and European Union, and a resilient LEO architecture less vulnerable to geofencing disputes. In April 2025, the

Paris-based firm's CEO announced that OneWeb terminals had been in Ukraine for about a year, paid for by the German government, and that some 5,000 to 10,000 terminals were expected to be deployed to Ukraine.[64]

However, disadvantages remain significant: OneWeb's terminal ecosystem is less mature, with fewer ruggedized tactical units; its user equipment is bulkier than Starlink's lighter field terminals; and its network throughput and user density remain insufficient for Ukraine's massive tactical demand, especially for drone teams and real-time video feeds. Moreover, OneWeb's service footprint and distribution channels are still optimized for commercial rather than battlefield use, limiting plug-and-play adoption by front-line units. As a result, while OneWeb offers political sovereignty and redundancy, it cannot yet replace Starlink as the backbone of Ukraine's battlefield internet but represents a necessary step toward multi-constellation resilience and reduced strategic dependence.[65]

Despite OneWeb's opportunities, mitigating dependency on Starlink is less about replacing a constellation than about redesigning the communications architecture that sits beneath it. As detailed in recent Ukrainian analysis, the path toward technical independence does not hinge on identifying a single alternative provider with comparable scale and bandwidth, but on abstracting Starlink into a modular connectivity layer within a broader, hybrid communications ecosystem.[66] Ukrainian forces have progressively adapted their software, workflows, and command-and-control practices to assume intermittent, degraded, or contested connectivity, rather than persistent high-bandwidth access. This includes combining LEO SATCOM with terrestrial cellular networks, radio relays, mesh networking, and local edge processing, so that Starlink becomes one bearer among many rather than a single point of failure. In this model, resilience is achieved not through ownership of space infrastructure but through software-defined adaptability, redundancy, and local autonomy under conditions of connectivity loss.

At the same time, Ukraine's reliance on Starlink has revealed structural vulnerabilities with implications far beyond the Ukrainian theatre, including for NATO and U.S. military planning. Chinese simulations demonstrating the potential to disrupt Starlink coverage through the coordinated use of large numbers of drone-mounted jammers challenge the assumption that constellation size alone guarantees resilience, and highlight the growing threat posed by distributed, low-cost electronic

64. L. Press, "OneWeb Can't Come Close to Replacing Starlink in Ukraine, but It Could Complement It", CircleID, June 19, 2025, available at: circleid.com.
65. Ibid.
66. "The Path to Technical Independence from Starlink in Ukraine", Skylinker, 2024, available at: www.skylinker.io.

warfare against space-enabled communications.[67] Western intelligence believes Russia is developing an experimental anti-satellite system that would release vast numbers of tiny pellets in low Earth orbit to damage or disable many Starlink satellites at once, but experts say using it would likely create widespread, uncontrolled debris that could also cripple Russian, Chinese, and civilian satellites and trigger severe disruption in space.[68]

A further risk lies in adversarial adaptation and technology leakage: evidence that Starlink components have appeared on Russian *Molniya* ("Lightning") drones underscores how commercial technologies supplied under restrictive or non-transferable conditions can still be repurposed and weaponized by opponents.[69] Taken together, these developments reinforce a core lesson from Ukraine: reducing dependency on commercial SATCOM requires not only provider diversification, but also architectural flexibility, EW resilience, and control over the downstream use of commercial components.

Key lessons learned – SATCOM

- Terminal proliferation transformed SATCOM from a strategic fail-safe (2022) to an end-to-end warfighting infrastructure (2025). Scale matters: 5,000 terminals enable survival; 200,000 enable digital warfare.
- Tactical C2, drone warfare, and artillery lethality now depend structurally on persistent battlefield internet. This dependency did not exist in early 2022.
- Starlink-specific vulnerabilities (color, thermal signature, EM detectability) required field adaptation and redesign, demonstrating that commercial hardware is not battlefield-ready by default.
- Overdependence on a single commercial constellation creates strategic risk, prompting Europe to accelerate sovereign alternatives (OneWeb, IRIS²).
- Russia's EW forced continuous adaptation, showing that SATCOM resilience is a dynamic contest, not a static capability.

67. J. Richards, "Can Starlink Be Blocked? Chinese Simulation Shows 1,000 Drones Can Jam Satellite Internet Over an Area as Large as Taiwan", TechRadar, 2024, available at: www.techradar.com.
68. J. Leicester, "Starlink in the Crosshairs: How Russia Could Attack Elon Musk's Conquering of Space", AP News, December 22, 2025, available at: https://apnews.com.
69. S. Beskrestnov, Telegram post on Starlink components identified on Russian Molniya UAV, 2024, available at: https://t.me.

PNT and GNSS navigation

At the outset of the war, both sides depended on GPS, GLONASS, and commercial correction services for artillery geolocation, UAV navigation, and the synchronization of digital mapping and command-and-control systems. Initially, most Ukrainian and Russian systems lacked hardened GNSS receivers, making them vulnerable to spoofing and jamming. Russia rapidly deployed large-scale EW systems (e.g., Pole-21, R-330Zh) to disrupt Ukrainian precision fires and UAV operations.

Ukrainian drones and PGMs experienced frequent navigation drift, especially in contested areas such as Kherson, Izium, and Donbas. From late 2022 onward, Russia expanded GNSS jamming coverage along the frontline and deep inside its territory (around Moscow, Belgorod, Crimea, and major airbases to protect from Ukrainian deep strike attempts). This degraded JDAM-ER guidance, 155 mm guided ammunition (like Excalibur), accuracy, loitering munition navigation, and Blue Force Tracking systems. In response, Ukrainian systems have increasingly tried to incorporate multi-constellation receivers combining GPS/Galileo/GLONASS, anti-spoofing algorithms, fallback inertial navigation (IMU) systems for drones, and vision-based navigation (optical flow, terrain matching).

These mitigations were not widespread in 2022, but by 2025, they were embedded in nearly all new Ukrainian UAV and precision-guided munition designs. The proliferation of FPV drones also created unprecedented demand for precise, stable GNSS, making PNT contestation a daily tactical concern rather than a strategic one. Russian EW thus became a counter-drone as well as counter-artillery tool, shaping maneuver and tempo.

Key lessons learned - PNT and GNSS navigation

- GNSS denial has become a persistent feature of modern high-intensity conflict, not an episodic effect;
- Precision-guided munitions cannot rely on GNSS alone: hybrid guidance (inertial measurement, electro-optics) is essential;
- PNT resilience improved dramatically between 2022 and 2025, driven by the drone war and artillery duels;
- Nations without sovereign PNT architectures face structural vulnerabilities when exposed to large-scale EW contestation.

Role of space-based ISR

The proliferation of commercial satellites has given Ukraine unparalleled access to ISR data, fundamentally altering the tactical execution of combat operations and complementing persistent UAV-based ISR with operational-

level surveillance, which some have come to designate as a new level of "battlefield transparency".

In early 2022, commercial Earth Observation (EO) satellites (Maxar, Planet) provided strategic imagery that revealed Russian troop movements and supported operation or strategic-level targeting. However, Ukraine lacked a structured data-fusion architecture to integrate national, allied, and commercial ISR at scale. Usage was often episodic rather than continuous, and dissemination to tactical echelons remained ad hoc. Russia has allegedly equally used commercially available ISR to target Ukraine.[70]

Over time, Ukraine has worked towards operating a hybrid space-based ISR ecosystem combining continuous commercial imaging, SAR as a tactical asset and accelerated data fusion and automation. With the proliferation of LEO constellations (PlanetScope, BlackSky, Capella, ICEYE), revisit times shrank from hours (2022) to minutes (2025). In August 2022, the Prytula Charity Foundation contracted Finnish-Polish microsatellite operating firm ICEYE to provide Ukraine's government and armed forces access to one of ICEYE's satellites with SAR capabilities, plus access to the broader constellation for higher revisit over critical areas.[71]

This enabled rapid target development for ATACMS and air-launched SCALP/Storm Shadow cruise missile strikes; real-time maritime situational awareness enabling attacks on the Black Sea Fleet; and continuous tracking of Russian logistics networks.

Combat software and the march towards integration

Information systems in general and "combat software" more precisely have been central to Ukraine's ability to survive and fight effectively in a sensor-saturated, drone-dominated battlespace, where speed of decision and coordination increasingly outweigh platform performance. Faced with fragmented communications, heterogeneous equipment, and constant electronic warfare, Ukrainian forces relied on software as an integration layer to compress kill chains, manage information overload, and sustain decentralized operations. Over time, what began as volunteer-driven, single-purpose applications evolved into a progressively integrated software ecosystem linking sensors, shooters, and commanders across echelons. This section traces that evolution through three analytical lenses: weapons-systems software enabling faster and more survivable fires, situational

70. "Are Airbus Satellite Images Helping Russia Wage War?", *Der Spiegel*, 2022, available at: www.spiegel.de.
71. Y. Kovalevska, "Супутник ICEYE: що саме купив Притула і як воно допоможе ЗСУ" [ICEYE satellite: what exactly Prytula bought and how it will help the AFU], BBC News Ukraine, August 19, 2022, available at: www.bbc.com.

awareness and information-management platforms such as Delta, and the emerging transition toward a modular combat management architecture.

Weapons systems software

Many of the most influential Ukrainian weapons systems software tools have roots in the post-2014 conflict in Donbas. Following Russia's first invasion and annexation of Crimea, Ukraine faced acute shortfalls in legacy Soviet C2, artillery fire control, and ISR integration. In response, a volunteer-NGO-military ecosystem emerged, experimenting with lightweight digital tools to compensate for material inferiority and doctrinal rigidity.[72]

One of the earliest and most influential developments was GIS Art/ Kropyva, initially developed in the mid-2010s as a volunteer-driven digital artillery fire-control and mapping tool. Kropyva allowed artillery units to replace paper maps and manual calculations with tablet-based geospatial awareness, enabling faster target acquisition and fire correction. Its early success rested on three features that would later become defining characteristics of Ukrainian combat software: (1) low hardware requirements, (2) offline/low-bandwidth functionality, and (3) continuous bottom-up iteration driven by frontline feedback.[73]

The 2022 invasion forced an abrupt transition from limited, uneven adoption to mass operational reliance on weapons systems software. Ukrainian artillery, drone units, and maneuver elements faced two immediate imperatives: shorten sensor-to-shooter timelines and survive in a counter-battery and drone-saturated environment.[74] During this phase, several software tools became ubiquitous or expanded rapidly:

- **Kropyva:** the backbone of digital artillery fire control, used to calculate firing solutions, manage unit locations, and integrate observer inputs;
- **Armor:** a more specialized fire-coordination and armored-unit support tool, focused on reducing coordination latency between reconnaissance, command, and fires;
- **Vezha:** supporting UAV video streaming, annotation, and relay to fire units;
- Supplementary tools for ballistic calculation, drone mission planning, and target grids, often developed at the unit level.[75]

72. K. Bondar, "How Ukraine's War Is Reshaping C4ISR", The Hague, The Hague Centre for Strategic Studies (HCSS), 2025.
73. P. Gros, V. Tourret, Y. Michel, and G. Garnier, "Enseignements de la guerre russo-ukrainienne", op. cit.
74. K. Aniskina, "Бойові Софти На Службі Сил Оборони: Поточний Стан Галузі Спз, Проблематика Та Актуальні Виклики" [Combat software in the service of the Defence Forces: the current state of the SPZ industry, issues and current challenges], Kyiv, May 2025.
75. Ibid.

By 2024-2025, the tactical environment is denser, more EW-contested, and characterized by extreme heterogeneity (ammunition lots, national propellant charges, mixed donor systems). In this context, software becomes an adaptation layer that reduces the friction created by coalition-driven diversity. For instance, Ukrainian artillery officers note that Kropyva updates can include pre-loaded adjustments to account for common national variants in propellant charges, mitigating accuracy/efficiency penalties generated by mixed supply.

At the same time, specialized weapons systems software has been professionalized. The software "Armor" (for armored units and indirect fire tasks) aims at reducing coordination time from roughly 25+ minutes to 5-7 minutes, a significant advantage when survivability depends on speed. Beyond the code, its diffusion model matters: the Armor team combined software fielding with structured training; one account indicates that over 15,000 service members were trained through instructor-supported courses, enabling rapid onboarding even for minimally experienced users.[76]

Weapons systems software is increasingly fused with ISR exploitation and performance monitoring. Updated versions of Vezha no longer merely displayed drone feeds but supported target tagging, timeline reconstruction, and post-strike assessment, feeding data back into Delta dashboards (see below). This enabled commanders to track unit effectiveness, ammunition expenditure, and response times, embedding weapons software into a broader data-driven approach to combat management. By 2025, Ukrainian weapons systems software comprised a family of interlinked tools, rather than a single application.[77]

Key lessons learned – Weapons systems software

- Ukraine's combat software advantage is cumulative, not sudden: it reflects a decade-long learning curve since 2014, rooted in NGO and volunteer innovation rather than formal procurement alone.
- Weapons software now functions as a compensator for material and organizational heterogeneity, particularly in artillery and fire coordination.
- Institutionalization matters: the transition from volunteer tools to trained, standardized usage (e.g., ARMOR) produced measurable gains in speed and survivability.
- Weapons systems software is no longer separable from ISR and data platforms; it is embedded in an end-to-end digital kill chain.

76. J. Watling, "Emergent Approaches to Combined Arms Manoeuvre in Ukraine", Royal United Services Institute, 2025.
77. Ibid.

- The Ukrainian case challenges Western acquisition models, showing that iterative, user-driven software development under combat conditions can outperform monolithic BMS programs.

Situational awareness and information management

As with weapons systems software, Ukraine's situational awareness software ecosystem predates the full-scale invasion and has its roots in the post-2014 Donbas conflict. The initial challenge was not merely the absence of modern ISR assets, but the lack of a digital layer capable of aggregating, visualizing, and disseminating battlefield information across units operating with degraded communications and limited institutional C2.[78]

A central actor in this early phase was the Aerorozvidka NGO, which emerged as a volunteer drone reconnaissance group and progressively evolved into a hybrid military–civilian innovation hub. Between 2015 and 2019, Aerorozvidka developed early forms of digital situational awareness tools to fuse UAV feeds, geolocation data, and unit reports. These efforts were motivated by operational necessity rather than formal doctrine, prioritizing speed, accessibility, and interoperability with civilian hardware (smartphones, tablets, commercial drones).[79]

These early experiments laid the conceptual foundations for Delta in 2017, which began as a digital mapping and coordination tool rather than a formal military system–with limited institutional reach nor security accreditation. Still, it was tested during the international exercises Sea Breeze and Rapid Trident and received interoperability qualification by NATO (which sponsored some of its earlier development through its NATO Trust fund) as early as 2019[80]. The Aerorozvidka approach emphasized: decentralized data input from frontline units, cloud-based sharing to overcome fragmented command chains and communications systems, user-driven iteration, with rapid feedback loops from operators to developers.

The full-scale invasion in February 2022 transformed Delta from a niche innovation into a national-level situational awareness backbone. Russian strikes on fixed command posts and communications infrastructure forced Ukraine to adopt distributed command and control,

78. "Strategic Approaches to Advancing Military Technology in Ukraine Amidst Evolving Security Challenges (2025-2030)", Kyiv, Ministry of Defence of Ukraine, 2025.
79. P. Gros, V. Tourret, Y. Michel, and G. Garnier, "Enseignements de la guerre russo-ukrainienne", op. cit.; K. Aniskina, "Бойові Софти На Службі Сил Оборони: Поточний Стан Галузі Спз, Проблематика Та Актуальні Виклики", op. cit.
80. S. Morfinov, "Delta для ЗСУ: Що відомо про новітню систему управління української армії" [Delta for the Armed Forces of Ukraine: What is known about the Ukrainian army's latest command and control system], BBC Ukraine, February 12, 2023; A. Shynko, "ЗСУ відновлюють розформовану Хомчаком Аеророзвідку" [The Armed Forces of Ukraine are restoring the Air Reconnaissance unit disbanded by Khomchak], October 22, 2021.

creating urgent demand for a shared digital common operating picture (COP) accessible across echelons.

During 2022, Delta's primary role was to aggregate reports from UAVs, artillery observers, and intelligence units, visualize friendly (blue force tracking) and enemy positions on a shared digital map so as to enable rapid dissemination of targeting and warning information. However, adoption was uneven across brigades, interoperability was still difficult, leading to the widespread use of manual workarounds (e.g., screenshots transferred between apps).

A qualitative shift occurred in 2023 when Delta was formally authorized by the Ukrainian Ministry of Defence, gaining institutional legitimacy and access to more secure hosting environments (although the system was implemented at all Defence Forces only in August 2025).[81] This marked Delta's evolution from a "map" into an information management platform, increasingly aligned with NATO data standards and coalition ISR-sharing requirements. At this stage, Delta began to serve as an integration format rather than a standalone application: other software tools such as ISR feeds (Vezha), chat functions, drone coordination modules, were connected to it as modules, using Delta as the visual interface.

By 2024–2025, Delta had evolved into a "platformized ecosystem" designed to manage the extreme data density of a drone- and sensor-saturated battlefield. It now includes various modules such as Monitor (situational awareness module compliant with NATO COP standards), Vezha (UAV video streaming and exploitation), Mission Control (drone mission tasking and deconfliction), Target Hub (target lifecycle management), Element (crypted messaging software), Nextcloud-type repositories (data storage and sharing), etc.

This architecture reflects a strategic shift: situational awareness is no longer about seeing the battlefield, but about managing information flows and cognitive load. Ukraine processes tens of terabytes of ISR data daily, including UAV video, satellite imagery, acoustic sensors, and textual reports. Delta's role is thus to filter, prioritize, and contextualize information, not merely display it.[82]

Key lessons learned – Combat software

- Ukraine's situational awareness advantage is rooted in a decade-long volunteer innovation cycle, particularly driven by Aerorozvidka's early ISR experiments after 2014.

81. "Бойова система DELTA впроваджена на всіх рівнях Сил оборони України" [The DELTA combat system has been implemented at all levels of the Ukrainian Defense Forces], Ministry of Defence of Ukraine, August 6, 2025, available at: https://mod.gov.ua.
82. K. Bondar, "How Ukraine's War Is Reshaping C4ISR", op. cit.

- Delta's decisive value lies in its role as an integration format, not as a single application: it connects weapons software, ISR feeds, and communications into a usable COP.
- The transition from 2022 to 2025 marks a shift from visibility to information management – from "seeing more" to "deciding faster under data saturation."
- Institutional adoption and security hardening were critical inflection points, enabling DELTA to scale from ad hoc use to national-level C2 support.
- Future conflicts will hinge on platforms that manage cognitive load, not merely sensor coverage, placing situational awareness software at the core of combat effectiveness.

Toward a combat management architecture?

By 2025, Ukrainian experience increasingly points toward a "combat management system" not as a single, centralized C2 application, but as a modular architecture connecting sensors, decision nodes, and effectors across domains. Most advanced Ukrainian Defense Tech advocates now explicitly argue for a "battle management architecture" that would be both modular and open so as to enable rapid tailoring and plug-and-play integration of sensors, AI algorithms, comms, fire control, and logistics in a "kill web". This future architecture would be shaped by three principles learned on Ukraine's battlefield:

- **Resilience under disrupted electro-magnetic spectrum (EMS):** a combat management approach must tolerate intermittent links and EW pressure. The architecture needs to favor semi-autonomous platforms that can cope with connectivity discontinuities and distributed networks via edge computing (processing on peripheral devices), so tactical units can operate when higher echelon connectivity is degraded.
- **Data sovereignty and vendor-lock risks:** reliance on external providers and opaque cloud dependencies create strategic exposure. Secure localized cloud options, cryptographic mechanisms (compatible with international standards) but independent of foreign providers, and broader "data sovereignty" design principles.
- **Automation to manage sensor saturation:** as the battlefield will produce more data beyond human cognitive skills, the move toward AI processing within ISR workflows (e.g., automated prioritization and integration of findings into command systems), indicating how "combat management" increasingly means *managing attention* and *allocating fires* under information overload.

A practical indicator of this trajectory is the growing integration between specialist tools and platforms: Griselda is described as integrated with Delta, Kropyva, Armor, and even the US *ATAK* ecosystem, suggesting an emerging "federated combat management" reality rather than a single-vendor battle management system.

Deep fighting: air and missile defense and deep precision strikes

Air and missile defense

The Russo-Ukrainian war is increasingly extending beyond the battlefield, shifting from initial socioeconomic impacts to direct military pressure on NATO territory.[83] While frontline states like Romania and Poland have reported multiple incursions,[84] the scope of the threat in 2025 expanded, albeit under a less attributable and kinetic form, to include Germany, France, Belgium, and the Netherlands.[85] This escalation reached a critical phase on September 10, 2025, when 19 Russian One-Way Attack (OWA) vehicles violated Polish airspace.[86] This incident exposed a severe economic vulnerability in NATO's Integrated Air and Missile Defense (IAMD)[87] Intercepting the threat required Dutch F-35 to fire missiles costing nearly $2 million each against "Gerbera" decoys worth only $10,000.[88]

The challenge is amplified by mass-produced FPV drones launched from sea platforms,[89] which conduct reconnaissance over deep-rear military sites[90] and paralyze civil airports.[91] Beyond surveillance, there is growing concern regarding the potential use of these systems as direct strike weapons. Consequently, experts argue that the current defensive architecture on the eastern flank of NATO is unsustainable and requires a new approach based on Ukrainian operational lessons.[92]

---

83. "EU Response to Russia's Invasion of Ukraine", European Council, accessed December 1, 2025, available at: www.consilium.europa.eu.
84. B. Erling and A. Charlish, "Polish Army Says Object Entered Poland During Russian Attack on Ukraine", Reuters, August 26, 2024, available at: www.reuters.com.
85. W. de Jager, "61 European Drone Sightings Analysed: Here's What We Know", Dronewatch, November 29, 2025, available at: www.dronewatch.eu.
86. A. Charlish, L. Kelly, and B. Erling, "Poland Downs Drones in Its Airspace, Becoming First NATO Member to Fire During War", Reuters, September 10, 2025, available at: www.reuters.com.
87. "Integrated Air and Missile Defense", NATO, accessed December 1, 2025, available at: www.nato.int.
88. T. Safronov, "Shooting Down Russian Drones in Poland Cost NATO Millions", Militarnyi, September 11, 2025, available at: https://militarnyi.com.
89. W. Murray, "Ukraine War Briefing: Shadow Fleet Is Launchpad for Russian Drones Harassing Europe", *The Guardian*, October 8, 2025, available at: www.theguardian.com.
90. L. Kayali, "Top EU Weapons Firm Warns of Drone Threat to Production Lines", Politico, October 23, 2025, available at: www.politico.eu.
91. M. Drummond and L. Russell, "Airport Drone Sightings: What We Know", Sky News, December 15, 2025, available at: https://news.sky.com.
92. "Drones over Europe—How to Respond" (Chatham House Rule discussion, Embassy of Lithuania, Paris, December 2, 2025).

C-UAV evolution

The 2022 counter-UAV landscape was dominated by conventional, layered air defense architecture. Soviet-era S-300 and S-400 radar and missile systems provided long-range detection and engagement, capable of tracking large platforms like TB2, leading to their short life on the forefront of drone warfare since 2022. Medium-range systems, including the Buk-M1, Buk-M2, and short-range Tor-M1, created a network optimized for different altitudes and targets. The Pantsir-S1, a combined short-range missile and 30mm gun system, proved particularly effective against slow-moving drones and served as a final protective layer around critical infrastructure.[93]

At the platoon level, "Igla" and "Stinger" Man-Portable Air-Defense Systems (MANPADS) presented a different class of counter-drone systems, offering protection against low-altitude threats. Short-range air defense still relied on classic gun systems and improvised protection, with infantry units contributing to whatever they had on hand. Soldiers scanned the sky or the tree line and engaged drones with rifles, machine guns, and other weapons whenever they spotted them. This was not a coordinated, sensor-driven air-defense network but a constant background of local reactions, present in almost every sector and sometimes enough to bring down low-flying quadcopters or loitering munitions.[94]

Vehicle crews started to change the shape of their armor from 2021 into 2022, as Russian and Ukrainian units built steel cages onto tank turrets and self-propelled guns. These "cope cages" were a simple form of spaced armor inspired in part by the Nagorno-Karabakh war and first appeared in Syria.[95] The idea was to make FPV, or top-attack warheads, detonate on the cage instead of directly on the turret roof or engine deck so that the blast and fragments lost energy before reaching critical components. Early cages were crude assemblies of rebar, scrap fencing, and improvised frames, but reports from Ukrainian intelligence later suggested that even these first versions prevented a noticeable share of successful hits and reduced drone-related casualties in 2022.[96]

By 2023, the character of the air threat had shifted significantly. Larger systems like TB2s were increasingly vulnerable to improved air defense, while FPV attack quadcopters became the main offensive tool. Russia was falling behind in 2023 but fast increasing FPV production capacity based on

93. Zvezda, "Военная приёмка. 'Панцирь'. Работа в СВО" [Defence Procurement Acceptance Authority. "Pantsir". Work in the area of Special Military Operation], YouTube, August 31, 2024, available at: www.youtube.com
94. M. Zafra et al., "Ukraine Crisis: Drones", Reuters, March 26, 2024, available at: www.reuters.com.
95. "Syrian Army Uses Local-Made Armour Cage to Increase Protection of T-72 Tanks and ZSU-23-4", Army Recognition, January 28, 2016, available at: www.armyrecognition.com.
96. "What Are 'Cope Cages'? The Bizarre Armor to Outsmart Deadly Drones", *The Economic Times*, August 13, 2025, available at: https://economictimes.indiatimes.com.

Chinese technology, and soon Ukrainian positions started experiencing intensifying daily FPV hits from Russian forces.[97]

The Ukrainian response included new kinetic methods in the air and more mature passive protection on the ground. Ukrainian units began building FPV-based interceptor drones tuned for speed and climb rather than explosive payload. These interceptors used upgraded cameras to find Russian reconnaissance drones such as Zala and Orlan, or Lancet loitering munitions, then rammed them in mid-air. Ground troops also improved their survivability, becoming more disciplined about camouflage, frequently moving guns and vehicles, and placing dummy equipment or thermal decoys to draw fire away from real assets. These measures did not remove the drone threat, but they helped reduce the number of successful reconnaissance runs and forced attacking drone operators to waste time and munitions on the wrong targets.[98]

In 2024, the scale of drone use skyrocketed on both sides, and both offense and defense adjusted. The Russian side has developed specialized ammunition for engaging small tactical drones, including FPV types. The system attaches to an AK-74 or AK-12, converting the assault rifle into a dedicated, short-range anti-aircraft tool.[99]

By late 2024, both the "mothership" aircraft concept and fiber-optic-controlled drones had moved beyond early trials and begun to show practical value. Carrier platforms or "mothership" concepts now have to be considered together with these unjammable drones. Because electronic countermeasures were ineffective against fiber-optic control links, the answer again had to be physical. Ukrainian units installed rotating barriers made from barbed or razor wire to damage or sever cables.[100]

Because fiber-optic drones could not be found through their radio waves, detection leaned more heavily on physical sensing. Ukrainian firms have built systems that combine arrays of microphones with simple infrared illuminators and cameras. The microphones picked up the distinct sound of electric motors and propellers, while the infrared light made drones stand out more clearly on camera at around a kilometer. At the same time, analysts trained algorithms on flight patterns, acoustic signatures, and sensor returns to separate crude decoys from more capable attack drones so

97. M. Z. Chaari, "Analysis of the Power of Drones and Limitations of the Anti-Drone Solutions on the Russian-Ukrainian Battlefield", *Security and Defence*, Vol. 51, No. 3, 2025, pp. 38–73, available at: https://securityanddefence.pl.
98. "Russia's War in Ukraine: Fortification for Drone Warfare", International Centre for Defence and Security (ICDS), September 9, 2025, available at: https://icds.ee.
99. "Русский ответ дронам: 'Дронобой'—оружие, которое меняет правила игры" [Russian answer to drones: "Dronoboy": a weapon that changes the rules of the game], Telegram, August 14, 2025, available at: https://t.me.
100. M. Tyson, "Ukraine's Rotating Barbed Wire Drone Barriers Discovered by Russians", Tom's Hardware, October 5, 2025, available at: www.tomshardware.com.

that missiles, gun ammunition, and interceptor drones were reserved for the most dangerous targets.[101]

Deep rear UAVs and C-UAV evolution

The evolution of rear-area air defense from 2022 to 2025 follows a clear trajectory from economic disparity to parity. In the early stages, the defense relied on multimillion-dollar missiles to intercept cheap loitering munitions, which created a financial crisis for defenders. Over four years, this dynamic shifted through industrial adaptation and innovation. By 2025, the defensive architecture had moved away from reliance on expensive legacy systems toward a sustainable network of acoustic sensors, mobile gun teams, and low-cost interceptor drones that could engage massed threats at a fraction of the previous cost.

The opening phase of the conflict in late 2022 marked the beginning of the Deep Rear war and forced difficult financial calculations regarding air defense. This period was defined by an economic asymmetry that heavily favored the Russian offensive. The campaign began with the widespread introduction of the Iranian-designed Shahed-136 and Shahed-131 loitering munitions, platforms that were rebranded as Geran-2 and Geran-1, respectively, upon their induction into Russian service. These weapons were not characterized by high-edge technology or speed but by their simplicity and cost-effectiveness. Tactical employment focused on saturation strikes, where waves of these munitions were launched simultaneously to overwhelm the fire control channels of Ukrainian air defenses. To evade detection by Soviet-era early warning radars, flight paths were programmed to hug the terrain, often following riverbeds like the Dnipro to remain below the radar horizon.[102]

The defensive response in 2022 highlighted a catastrophic cost-exchange disparity that threatened to bankrupt the defender's missile stockpiles. While Western-supplied systems like NASAMS and IRIS-T SLM achieved high interception rates, the financial logic of the engagement was unsustainable. Research indicates that a single AIM-120 AMRAAM missile fired from a NASAMS battery costs over one million dollars, and an S-300 48N6 interceptor is estimated at approximately $1.3 million.[103] In contrast, the Shahed-136 had an estimated production cost ranging from $20,000 to

101. Y. Andriushchenko, "From Cloning Actors' Voices to Detecting Missiles: Ukraine's AI Scene Contributes to Air Defense", AlgorithmWatch, December 7, 2022, available at: https://algorithmwatch.org.
102. J. Emmett, T. Ball, and N. R. Jenzen-Jones, "Shahed-131/136 UAVs: A Visual Guide", Open Source Munitions Portal, accessed December 5, 2025, available at: https://osmp.ngo.
103. C. Stiles, "Missile Interceptors by Cost", Missile Defense Advocacy Alliance, February 2024, available at: https://missiledefenseadvocacy.org.

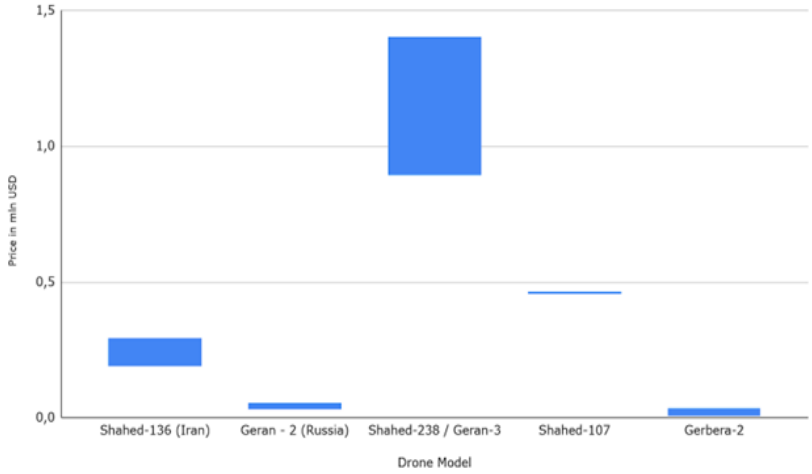
$50,000.[104] This resulted in a cost ratio of roughly 26:1 in favor of the attacker, creating a "cost of inaction" dilemma where defenders were forced to expend scarce strategic assets to prevent tens of millions of dollars in damage to critical and civil infrastructure.[105] To mitigate this financial imbalance and protect urban centers, the Flakpanzer Gepard became a cornerstone of the kinetic counter-drone effort. This West German-designed Self-Propelled Anti-Aircraft Gun is built on the Leopard 1 tank chassis and manufactured by KNDS.[106]

Ukraine also relied on several Soviet-era short-range air-defense gun and gun-missile systems used in counter-drone warfare, including the ZU-23-2, the ZSU-23-4 Shilka, and the 2S6 Tunguska. These systems were originally designed to protect ground forces from low-flying aircraft and proved capable of targeting drones, which had become dominant in the war. As Russian reconnaissance drones and later Shahed-type strike drones became a major threat, Ukraine's partners began supplying additional anti-aircraft guns and modernized variants.[107] Ukraine also captured several Russian Pantsir-S1 gun-missile systems in early 2022. The Air Force confirmed at the time that at least one captured Pantsir had been repaired, supplied with usable ammunition, and employed by Ukrainian forces, with at least one confirmed shoot-down.[108]

The second year of the deep rear war, 2023, was characterized by industrial scale and the acoustic shield, representing a defensive move toward correcting financial imbalance. Russia began the localization of drone production under a $1.75 billion franchise agreement with Iran in the Alabuga Special Economic Zone in Tatarstan.[109] The facility planned to produce 6,000 units by 2025, reducing dependence on external supply chains and enabling a steady pace of nightly strikes instead of occasional large-scale attacks.[110]

104. "Shahed and Geran: The Evolution of Russia's Deep Strikes", Calibre Defence, accessed December 3, 2025, available at: www.calibredefence.co.uk.
105. N. Hollenbeck, M. Altaf, F. Avila, J. Ramirez, A. Sharma and B. Jensen, "Calculating the Cost-Effectiveness of Russia's Drone Strikes", Center for Strategic and International Studies (CSIS), January 2025, available at: www.csis.org.
106. "GEPARD", KNDS Group, accessed December 02, 2025, available at: https://knds.com.
107. S. Kozatskyi, "Від ЗУ-23 до Skynex: якими зенітними гарматами Україна збиває Shaheds" [From ZU-23 to Skynex: which anti-aircraft guns Ukraine uses to shoot down Shaheds], Militarnyi, August 26, 2025, available at: https://militarnyi.com.
108. A. Vodianyi, "Трофейный ЗРК Панцирь-С1 начал работать на оборону и уничтожил первую цель" [Captured Pantsir-S1 SAM system has begun working for defense and destroyed its first target], LIGA.net, July 11, 2022, available at: https://news.liga.net.
109. N. Walsh, K. Polglase, and V. Krever, "Russia's Massive Drone Factory Is Running at Full Tilt with Help from Iran", CNN, August 8, 2025, available at: https://edition.cnn.com.
110. J. Seltzer and J. Caves, "Alabuga Drone Plant Case Study: Key Relationships Enabling Iranian Support for the Russian Military", Iran Watch, November 8, 2024, available at: www.iranwatch.org.

Chart 3: Estimated unit cost of selected Russian UAVs



Source: B.Kostiuk,"Strategic Adaptation and the Rise of Sustainable Air Defense." Eastern Circles, January 12, 2025, available at:www.easterncircles.com.

To handle the growing number of drones without exhausting missile reserves, Ukraine introduced the "Zvook" acoustic network, a system of thousands of passive sensors mounted on towers and utility poles. Using algorithms trained to distinguish the Shahed engine's sound signature from other noise, the system created a real-time detection grid that required no radar emissions.[111] Its data fed into the "Virazh" command system, which directed mobile fire teams equipped with searchlights and heavy machine guns such as the DShK (Degtyaryov–Shpagin large-calibre) or twin-mounted Maxim guns.[112] Introducing this approach shifted the cost balance, allowing Ukraine to bring down drones worth tens of thousands of dollars with inexpensive ammunition while keeping advanced missiles reserved for higher-end threats.

In 2024, the operational landscape shifted from a battle of attrition to sophisticated technology against the sensor war, marked by an escalation in stealth and navigation. The Russian industrial complex at Alabuga began fielding the "Black Shahed", which utilized carbon-infused radar-absorbing materials and black paint to minimize visual and radar signatures during night attacks.[113] Furthermore, the navigation systems were upgraded through the integration of the "Kometa" Controlled Reception Pattern Antenna (CRPA), an adaptive antenna array capable of filtering out

111. O. Tartachnyi, "Українці створили технологію, яка визначає розташування ракети за звуком. Інтерв'ю з ML-інженером Володимиром Сидорським" [Ukrainians created technology that determines the location of a missile by sound. Interview with ML engineer Volodymyr Sydorskyi], SPEKA, October 17, 2023 available at: https://speka.ua.
112. "How Ukraine's New Tech Foils Russian Aerial Attacks", *The Economist*, July 24, 2024, available at: www.economist.com.
113. S. Beskrestnov (Flash), "[Facebook Post regarding the technical analysis of Shahed-136 drone components]", Facebook, December 26, 2023, available at: www.facebook.com.

jamming signals.[114] Recovered debris also revealed the integration of 4G/LTE modems and Starlink, allowing drones to utilize cellular networks for telemetry and perform optical terrain matching independent of satellite navigation.[115] Simultaneously, the Russian side introduced the "Gerbera" decoy drone, a cheaper foam-bodied aircraft designed to saturate air defenses by mimicking the radar cross-section of the lethal Geran-2.[116]

Defensive architecture responded by deepening the integration of artificial intelligence into the sensor-to-shooter loop. The "Safe Skies" and "Virazh" networks were upgraded with algorithms capable of automatically fusing data from acoustic, thermal, and radar sensors to predict flight paths and prioritize targets for Mobile Fire Groups.[117] To counter the new composite material drones, Dutch radar systems deployed in Ukraine received significant upgrades, enabling micro-Doppler processing. This technology allowed radar operators to distinguish the specific modulation of a drone's engine sounds from static clutter or birds, enabling the detection of low-RCS (Radar-Cross Section) targets that would otherwise remain invisible to legacy pulse-doppler radars.[118] The kinetic approach remained vital; in 2024, many ZU-23 platforms mentioned in the 2022 section were equipped with the SkyLock targeting system.[119] This optoelectronic sighting device incorporates a thermal imager and a system for precisely determining the distance and height of a target, providing the operator with a digital image and necessary engagement information.

By 2025, the Deep Rear contest reached a material and tactical peak defined by mass usage and drones' interceptors. The widespread use of polymer structures for offensive weapons and the arrival of dedicated interceptor drones shaped this new reality. Offensive production shifted to extruded polystyrene foam and other polymers for both Gerbera decoys and armed Geran UAVs[120]. This change reduced radar visibility and lowered the cost of decoys to roughly ten thousand dollars per unit[121]. Offensive

114. B. Miroshnychenko, "Тепер не тільки 'шахеди'. Як Росія наростила виробництво ударних БПЛА і чим відповідають українські інженери" [Not only "Shaheds" now. How Russia increased the production of strike UAVs and how Ukrainian engineers respond], *Ekonomichna Pravda*, October 17, 2024, available at: https://epravda.com.
115. O. Ponomar, "Камеры на дронах Шахед" [Cameras on Shahed drones], Ponomar Oleg, October 20, 2024, available at: www.ponomaroleg.com.
116. Y. Talbo, "Un nouveau drone d'attaque russe identifié en Ukraine : le Gerbera" [A new Russian attack drone identified in Ukraine: the Gerbera], Air & Cosmos, August 3, 2024, available at : https://air-cosmos.com.
117. A. Dangwal, "Ukraine's 6000+ EW 'Acoustic Sensors' to Counter Russia's Kamikaze UAVs Get US Military Interested", *The Eurasian Times*, February 13, 2024, available at: www.eurasiantimes.com.
118. A. Haywood, "DSEI 2025—Robin Radar Systems Deploys the LRM Module for IRIS Radar", *EDR Magazine*, September 11, 2025, available at: www.edrmagazine.eu.
119. T. Safronov, "Prytula Foundation Modernizes ZU-23 Anti-Aircraft Guns with SkyLock Systems", Militarnyi, May 13, 2025, available at: https://militarnyi.com.
120. S. Maksymiv, "Sanctions and Capabilities of the Russian Federation: How Did the Shaheds' Filling Change During the Russian Full-scale Invasion of Ukraine?", Trap Aggressor, March 20, 2025, available at: https://trap.org.
121. B. J. Weichert, "Russia's Gerbera Drones Are Giving NATO a Terrible Headache", *The National Interest*, September 27, 2025, available at: https://nationalinterest.org.

capabilities also expanded with the introduction of the jet-powered Geran-3, known as the Shahed-238.[122] This modification was intended to break through the defensive layers formed by mobile fire groups, but also served as an experiment in confronting Ukrainian drone interceptors.[123]

The defensive reaction to this flood of inexpensive, low-visibility, and faster drones was the fielding of specialized interceptor drones, which marked a doctrinal shift in rear-area air defense.[124] Ukrainian drones such as the Sting, Bullet, or the American Merops appeared as low-cost reusable interceptors capable of operating at speeds above two hundred kilometers per hour and at altitudes of up to almost 23 thousand feet (about 7.01 km). These interceptors were directed by radar networks filtered through automated analysis, including AI modules specifically trained to identify Shahed profiles and were designed to collide with or disrupt Russian drones in flight.[125] With unit costs near one thousand dollars, they provided a sustainable economic response to cheap threats and helped establish a favorable cost balance for the defender. By this stage, the rear-area airspace had become a zone of continuous automated engagements in which inexpensive interceptors contested the presence of equally inexpensive offensive drones.[126]

Key lessons learned – C-UAV

- **Economic asymmetry dictates defensive architecture:** The most immediate strategic lesson from the Russian invasion of Ukraine is that financial sustainability must drive air defense procurement. The report highlights a catastrophic cost imbalance observed in 2022, where defenders expended missiles costing over 1 million dollars to intercept loitering munitions costing roughly 20,000–50,000 dollars. This 20-26 to 1 cost ratio creates a strategic vulnerability where an attacker can bankrupt a defender's stockpiles through massed cheap attacks. NATO nations must move away from relying solely on advanced interceptors like the AIM-120C-7 for Class I and II drone threats. The successful Ukrainian adaptation involved shifting to mobile fire teams equipped with low-cost machine guns and searchlights in 2023 and eventually to

122. "Обзор ударного БПЛА 'Герань-3'" [Review of the "Geran-3" strike UAV], Mosregdata, August 3, 2025, available at: https://mosregdata.ru.
123. "Під час атаки по Києву РФ використала новий реактивний 'Шахед', вірогідно російського виробництва – 'Герань-3'" [During the attack on Kyiv, the Russian Federation used a new jet "Shahed", probably of Russian production – "Geran-3"], *Defence Express*, June 11, 2025, available at: https://defence-ua.com.
124. M. Loh, J. Epstein, "Ukraine's Cheap Interceptor Drones Are Rewriting the Air War Playbook", *Business Insider*, October 18, 2025, available at: www.businessinsider.com.
125. T. Safronov, "Ukraine's Interceptor Drones Receive Modules That Automatically Target Shahed Drones", Militarnyi, December 11, 2025, available at: militarnyi.com.
126. T. Burgel, "Guerre en Ukraine : STING, le petit drone à 2 500 dollars qui fait des merveilles face aux Shahed russes" [War in Ukraine: STING, the small 2,500-dollar drone doing wonders against Russian Shaheds], *Geo*, November 7, 2025, available at: www.geo.fr.

specialized drone interceptors costing nearly 1,000 dollars in 2025. Future alliance defense architectures must integrate these low-cost kinetic layers and preserve high-value interceptors for high-end threats.

- **The Fusion of modernized kinetic effectors and multi-spectral sensing:** Effective counter-UAV capabilities require the tight integration of kinetic systems with modern detection grids. The war demonstrated that while conventional systems like the Flakpanzer Gepard or modernized ZU-23 autocannons remain lethal against low-flying drones, their effectiveness is dependent on advanced targeting data. Ukraine paired these kinetic effectors with the Zvook acoustic network which uses thousands of passive sensors to detect engine signatures without emitting radar signals. This combination allows defenders to bypass the limitations of pulse-doppler radars which often miss low-altitude polymer drones like the Gerbera decoy. The lesson for NATO is that kinetic platforms must be linked with acoustic and thermal sensors to form a responsive fire control environment capable of engaging targets that evade traditional radar detection.
- **The necessity of building an ecosystem:** While low-cost drone interceptors represent a breakthrough in cost-exchange ratios, they are not a silver bullet. Ukrainian systems like the Sting and Bullet provided a sustainable economic response, however these interceptors functioned effectively only because they worked in an overarching command and control architecture with human intervention. They rely on radar networks filtered through automated AI analysis to predict flight paths and guide collisions. NATO cannot simply procure interceptors but must build a full ecosystem where expensive surface-to-air missiles are used only against high end threats (cruise missiles, ballistic and air-launched hypersonic missiles). This ecosystem requires the integration of AI prediction algorithms, sensor fusion, and automated launch authorities to manage the volume of targets involved in modern aerial warfare.
- **The limits of electronic warfare and the return to physical engagement**: The rapid adaptation of offensive drone technology, including optic-fiber drones, has challenged traditional EW jamming and spoofing. Future force protection planning must assume that the electromagnetic spectrum will be a contested or denied environment and invest in physical countermeasures that function independently of signal manipulation.
- **Decentralized innovation outpaces institutional procurement**: The war revealed that tactical innovation often occurs faster at the unit level than through centralized acquisition cycles ("cope cages" for armor protection, mobile fire groups in response to the Shahed threat) and is later integrated into the national command network. The lesson for NATO is the need for flexible management and procurement mechanisms that can validate and scale frontline innovations rapidly.

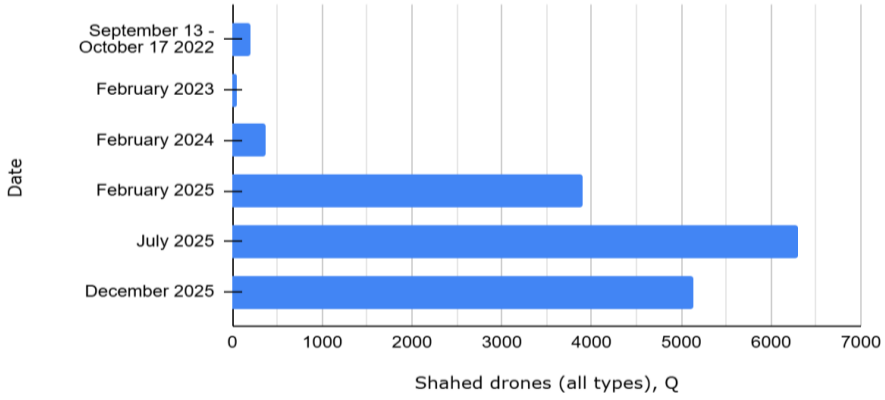
The Ukrainian Ministry of Defense initially failed to prioritize commercial drones, leaving units to rely on volunteer supplies until late 2022. To maintain a technologically advanced NATO, nations must create pathways to identify soldier-led adaptations and industrialize them quickly rather than waiting for formal requirements processes to catch up with battlefield realities.[127]

The Salvo competition: an economic approach to air defense

The massive use of combined aerial attacks in Ukraine, reaching the scale of hundreds of drones and scores of missiles and guided bombs per night, triggered the need to reevaluate the approach to air defense. Numerous drone incursions in Europe throughout 2025 made clear what has been evident in Ukraine in the first year of war: the industrial capacity to mass-produce cheap and disposable air strike capabilities gives an important military advantage in a war of attrition. Russia has demonstrated its capacity to overwhelm Ukrainian air defense capabilities with the number of Shahed-type drones it can produce and fire daily, the effect of layered combined attacks on classical air defense systems, and the adaptation capability of drone and missile technology to the evolving air defense strategies.

Given the growing menace of drone attacks on critical infrastructure in Ukraine and NATO, and the disruptive effect of these attacks for civilian life and defense industry production (in Ukraine at present, in Europe potentially in the future), it is important to understand the key elements of air defense evolution in Ukraine and how they can be integrated into NATO air defense strategy.

Chart 4: Growth in Russian use of Shahed drones against Ukraine



Source: B.Kostiuk, "Strategic Adaptation and the Rise of Sustainable Air Defense", Eastern Circles, January 12, 2025, available at: www.easterncircles.com.

127. B. Kostiuk, "Strategic Adaptation and the Rise of Sustainable Air Defense", Eastern Circles, January 12, 2025, available at: www.easterncircles.com.

Among many differences, one is essential in the confrontation between Shahed drones and classical means of air defense in a war: cost. An average Shahed-136 type drone, produced in Russia as Geran' drone, is estimated to cost between 30,000 and 80,000 dollars per unit.[128] From 970 OWA drones of all types on Ukraine in 2024, that number rose to 44,228 in the first 10 months of 2025.[129]

The strategy of countering the high quantity of cheap, easy, and fast-to-produce drones with the power, big, expensive, and slow-to-produce missiles falls short. The disadvantage of cost on the defending side risks depletion of missile stockpiles and an unsustainable strain on state budgets to fund new production. Furthermore, in a multilayer attack, Russia uses Shahed-type drones to detect the location of the launch systems in order to target them with the following round of missile strikes. This drives the cost of air defense even further.

How layered combined attacks altered the air defense calculation in Ukraine

Ukraine has reacted to the multilayer air attacks with a multilayer air defense system, which combines different air defense systems for different purposes. The first is kinetic interception systems:

- Against missile attacks, Ukraine has been using expensive Patriot missiles. Their effectiveness has gone from 85% in early 2025 for cruise missiles and 25% for ballistic missiles to near zero, when Russia introduced maneuverable Iskander missiles in late summer of 2025.[130] An effective means of defense could be a hyper-sonic plane, but there the problem of cost and availability are on the surface.
- Against Shahed-type Geran drones before the summer 2025, Ukraine used a combined response of artillery and automatic gunfire by mobile groups on pick-ups.
- Against the turbojet-powered Shahed-type drones Russia started producing since the summer 2025, flying at 250 km/hour to 500 km/hour speed, conventional anti-aircraft artillery (AAA) has grown ineffective. Ukraine has been adapting with counter-drone systems produced by Wild Hornets, General Cherry, Vyriy, of which the French equivalent Alta Ares is also being tested in Ukraine. These C-UAV relying on AI for navigation and targeting can develop a speed between 250 and 400 km/hour and target to reach the Russian drone

128. T. Safronov, "Shooting Down Russian Drones in Poland Cost NATO Millions", Militarnyi, 11 September 2025, available at: militarnyi.com.
129. M. Oleksandr, "Victory Drones", Lecture on air defense in Ukraine at the EUDHI Hackathon, Saint-Germain-en-Laye, France, November 8, 2025.
130. A. Fratsyvir, "Russia Upgrades Iskander Ballistic Missiles, More Difficult for Ukraine's Patriots to Intercept, Air Force Says", *The Kyiv Independent*, May 24, 2025, available at: https://kyivindependent.com.

from the rear, without being seen. Their effectiveness was countered by Russia in the fall of 2025 by installing rear-view cameras on Shahed-type drones and increasing the latter's maneuverability, which renders the last-mile effort more difficult.[131]

While C-UAV drones have proven to be effective against Shahed-type drones, operating them, in addition to the EW equipment, to defend towns and villages creates an HR pressure on the Ukrainian army, which needs to prioritize the frontline.

One solution has been a civilian-military C-UAV operator model, introduced by a leading drone-training civil society actor in Ukraine, Dignitas. This approach proposes to train teams of C-UAV operators with a civil-military ratio of 3:1 to allow civilians become the actors of their own defense, while lowering the burden for the military. To reconcile solving the HR pressure with the need of the military to maintain the monopoly on the legal use of force, the responsibilities of such a unit remain clear-cut, with the military retaining control over the key equipment (EW, payload-equipped C-UAV), while civilians are given supporting roles.[132]

The second form of defense, EW is now challenged with the latest developments on the Russian side, including low-altitude flight and multi-branch antennas, which have resulted in successful impairment of EW counteraction. The race of changing the frequencies is ongoing, but the latest developments in speed, altitude change capacity and non-EMS drones can make the use of EW less effective.[133]

Cyber war: the integration of Starlinks directly into Russian strike drones for navigation, as well as the use of SIM-cards, allowing the use of ground objects for mapping the drone flight route, have increased the importance of cyber counter-attack tools as an integral part of air defense.

In addition to Shahed-type Geran drones, Ukraine has been attacked by tens of thousands of guided missiles (KAB or FAB in Ukrainian), against which the traditional air defense listed above have very limited effectiveness. To make KABs, the Russians have been equipping unguided or "dumb" bombs, found in abundance as a post-Soviet legacy in military warehouses, with precision guidance systems, which turn them into "smart" bombs. This recycling approach allows to keep the cost of KABs at a minimum, while maximizing the damage. The 500 to 1,500 kg of explosive power of one KAB, combined with the undetected approach and consequent surprise at the explosion, renders this weapon devastating in the force of destruction and psychological damage on the morale of the targeted troops. The independence of the KAB from a radio signal makes it hard to detect

131. Eastern Circles interview with air defense system operator, Kyiv, December 2025.
132. Dignitas presentation and subsequent interview by Eastern Circles at the EU DefTech Hackathon at Ixcampus, Paris region, November 7, 2025.
133. Eastern Circles interview with EW expert at Medovyk bureau, Kyiv, December 2025.

and immune to EW, thus hard to intercept.[134] Besides the devastating psychological effect on the frontline, making people "lose their mind" and thus incapacitating soldiers, the KAB's physical destructive force obliterates frontline positions and multi-story buildings in the "deep rear".

Key lessons learned - Air defense

Multilayered defense requires trained personnel who can master the skills to manage different means of air defense, to make them interoperable, and include maintenance skills. The training time is non-compressible, and requires ahead planning by military command, if NATO is to prepare the type of air defense needed in modern war.[135]

- A shortage of military personnel is unavoidable. To prepare for it, NATO must anticipate and prepare military-civil cooperation formats for air defense.[136]
- AI-based navigation and strike-decision systems hold the key to counter modern Russian drones and missiles, including maneuverable high-speed weapons. AI military systems developed in Ukraine are more effective than those developed in Europe in the current conditions. Therefore, industrial partnerships development between Ukrainian and European developers is key.[137]
- Another key element of air defense is increasing European production capacity of smaller and cheaper missiles, which can counter Shahed-type drones.
- To ensure sustainable military production in the worst-case scenario of an attack on Europe, given the Russian ability to inflict hundreds of Shahed-type drone strikes and dozens of precision (including ballistic) missile strikes daily, as Ukraine's experience shows, requires integrating the option for underground defense industry production facilities into European contingency plans.
- Guided glide bombs (KAB, FAB), which devastate Ukrainian military positions and civilian infrastructure, also remain a blind spot of NATO air defense.[138]

134. Eastern Circles Newsletter 31, October 2025, available at: www.easterncircles.com.
135. Interview by Eastern Circles with a member of Ukrainian Armed Forces, Kyiv, December 2025.
136. D. Shmyhal, "Підприємства критичної інфраструктури можуть долучатися до державної системи ППО під керівництвом військового командування" [Critical infrastructure enterprises can join the state air defense system under the leadership of the military command], Telegram, November 19, 2025, available at: https://t.me.
137. Interview by Eastern Circles with Arnaud Valli, Comand AI battle management systems, Paris, December 17, 2025.
138. Interview by Eastern Circles with the faculty of the French War School (École de Guerre), January 7, 2025.

Deep strike capabilities

Deep strike capabilities have become a central instrument of Ukraine's operational and strategic posture, allowing Kyiv to impose costs on a larger adversary by contesting depth, logistics, and force generation rather than seeking decisive battlefield breakthroughs. Constrained by limited access to Western long-range systems and by political restrictions, Ukraine progressively built a layered deep-strike approach combining asymmetric UAV campaigns with a narrower set of conventional precision-strike options. Technologically, these capabilities evolved from sporadic, opportunistic attacks into sustained campaigns enabled by improved navigation, targeting, and production scale, while remaining constrained by persistent shortfalls in payload, survivability, and stockpiles. This section, therefore, distinguishes between asymmetric deep strikes conducted with low-cost systems and conventional deep strikes relying on Western-supplied and indigenous missile programs before assessing their respective trade-offs and strategic effects.

Asymmetric deep strikes: from occasional to sustained campaign

As early as 2022, Ukraine tried to regain the initiative by launching deep strikes inside Russia. These strikes were overwhelmingly asymmetric in character, reflecting the absence of both indigenous capacity for conventional long-range precision strike and lack of political authorization to do so with donated systems. These early operations relied on low-cost, low-payload UAVs, often combined with covert action, aimed less at decisive destruction than at psychological, economic, and operational disruption.

The targets—oil storage sites, rail infrastructure, lightly defended airbases and very occasionally political sites with heavy symbolic value—were typically fixed, visible, and OSINT-identifiable, enabling Ukraine to leverage commercially available satellite imagery and social media geolocation rather than classified ISR (from Ukraine's partner intelligence sharing). This phase represented a form of "asymmetric signaling": demonstrating reach, imposing friction, and forcing Russia to allocate resources to rear-area defense well beyond the frontline. Technologically, the strike weapons systems used in these early strikes were constrained by very limited payloads, GNSS-dependent navigation, and low survivability as Russian rear-area air defense improved. As a result, the Ukrainian asymmetric strikes in 2022 were episodic and opportunistic, effective primarily through cumulative disruption rather than through the destruction of high-value military assets.

The Ukrainian military modified civilian light aircraft like the Aeroprakt A-22 to overcome the range limits of early drones and strike targets over 1,200 km away in Tatarstan. By late 2024, these missions evolved with more advanced platforms like the E-300 Enterprise, which allowed for precise strikes against naval and military targets in distant regions such as Dagestan and Chechnya.[139]

Over time, Ukraine's asymmetric deep-strike posture has undergone a qualitative and quantitative transformation, crystallized most clearly in Operation Spiderweb against the Diaghilev and Ivanovo airbases, that may have destroyed or damaged more than 40 Russian aircraft, including the strategic assets such as A-50, Tu-95 and Tu-22M3, used in missile attacks on Ukraine.[140] Spiderweb illustrates a shift from difficult long-range attacks to a logic built on covert access, proximity launch, and operational surprise.[141] Indeed, as launch platforms were covertly positioned inside Russian territory, the UAVs could be released at short range, reducing navigation error and EW exposure. This approach enabled the use of simpler autopilot systems and commercially derived components, since the hardest part of the strike (long-distance navigation under a GNSS-denied environment) had been transferred to the human domain (covert infiltration or local asset recruitment).[142]

By 2025, asymmetric deep strikes were no longer isolated events but interlinked campaigns: the refinery and energy campaign, aimed at degrading refining capacity, export flows, and fuel availability; the airfield campaign, focused on aircraft on the ground, support infrastructure, and sortie-generation capacity. Across both campaigns, asymmetric systems retained payload limitations. Most systems delivered light warheads, insufficient to destroy hardened military infrastructure outright. However, when combined with repetition, surprise, and OSINT-enabled targeting, they achieved operationally meaningful effects: fires, downtime, repair cycles, aircraft relocation, and defensive overextension.

Key lessons learned – Asymmetric deep strikes

- Ukraine's asymmetric deep strike evolved from episodic disruption (2022) to campaign-level warfare (2025), especially against energy and airpower enablers.

139. Harbuz (Dnipro OSINT), "Дістати до Алабуги та Грозного. Як Україна нарощує дронові удари на 1000+ кілометрів" [Reaching Alabuga and Grozny: How Ukraine is scaling up drone strikes at 1000+ kilometers], Oboronka, January 7, 2026, available at: https://oboronka.mezha.ua.
140. J. Dempsey, "Operation Spiderweb: an Assessment of Russian Aerospace Forces Losses", International Institute for Strategic Studies, 6 June 2025.
141. K. Bondar, "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare", CSIS, 2025, available at: www.csis.org.
142. O. Kryzhanivska, "Drone warfare in Ukraine: operation Spiderweb Semi-autonomous capabilities and AI-enhanced support", *Ukraine's Arms Monitor*, June 2025, https://ukrainesarmsmonitor.substack.com.

- Operation Spiderweb demonstrates that clandestine access and proximity launch can occasionally produce effects similar to advanced missile technology, neutralizing EW and air-defense advantages.
- OSINT and commercial ISR are sufficient for deep-strike target development against fixed infrastructure, lowering barriers to strategic reach.
- Payload limitations remain structural: while repetition, surprise, and strategic target selection can offer leverage, the inherent characteristics of asymmetric strike systems make them harmless against a variety of targets for the moment.
- Asymmetric deep strike redefines success metrics: cumulative economic and operational pressure can matter more than single-strike lethality.
- For modern warfare, asymmetric deep strike is not a stopgap—but a durable complement to conventional precision strike, particularly under political and industrial constraints.

Conventional deep strikes: Ukraine's missile options, constraints, and strategic trade-offs

Ukraine's conventional deep-strike posture combines a narrow set of high-end Western-supplied missiles with a broader, but less mature, array of domestically developed strike systems, both heavy, medium and light.[143] The critical analytical distinction is not between "missiles" and "drones" (whose difference in the light section is hard to substantiate), but in the range, precision and payload equation. As of now, Ukraine's options fall into four capability categories, each presenting a different balance of operational advantages and structural limitations.[144]

Western-supplied deep strike systems

Western-supplied air-launched cruise missiles, notably MBDA's Storm Shadow/SCALP-EG, remain Ukraine's most decisive conventional deep-strike capability. Their principal advantage lies in their ability to combine range, accuracy, and destructive effect in a single mature system. Operational range of 550 km (approximately 340 miles), multi-mode guidance architectures (GNSS, Terrain Contour Matching or TERCOM, Inertial Guidance INS, and terminal EO scene matching) enable high precision even in electronically degraded environments, while heavy

143. F. Hoffman, "From Flamingo to Neptune: Ukraine's Conventional Deep Strike Options", Missile Matters, 2024.
144. D. E. Sanger et al., "Why Ukraine Is Betting on Strikes Deep Inside Russia", *The New York Times*, 2024.

warheads (450 kg) allow effective engagement of hardened targets such as airbases, command facilities, and ammunition depots.[145]

The first limit is the very small number of missiles produced and therefore donated to Ukraine, precluding high-tempo use. From a technical perspective, while guidance systems are more resilient than those of improvised or domestic platforms, GNSS jamming remains a challenge, especially when combined with degraded terrain-reference data or suboptimal mission planning. Air-launched cruise missiles, by definition, require a capable combat aircraft fleet to operate them, and this remains a rare asset in the Ukrainian Air Force and a risky engagement. Moreover, StormShadow/SCALP-EG are subsonic weapons, which inherently increase exposure to modern, layered air-defense networks. As Russian short- and medium-range integrated air-defense systems (IADS) have expanded and adapted, the survivability of subsonic cruise missiles has become increasingly dependent on careful routing, suppression of enemy air defenses, and limited saturation. These factors do not negate the military value of donated cruise missiles, but they constrain their scalability and underline their role as campaign-shaping assets rather than a sustainable strike backbone.

Surface-to-surface ballistic missiles such as ATACMS provide a different set of advantages. Their high speed, steep terminal trajectories, and short time-to-target reduce exposure to traditional air-defense interceptors and complicate defensive reaction. This makes them particularly effective against area targets such as airfields, logistics hubs, and rear-area infrastructure, where rapid disruption is operationally valuable.

However, these advantages are offset by even sharper limitations. ATACMS availability is extremely restricted, employment is politically sensitive, and there is no prospect of domestic production or meaningful stockpile expansion. Also, in the version donated to Ukraine, the ATACMS is range-limited, and DPS exposes the launcher to front-line interdiction from Russian loitering munitions, SS-26, and FPVs.[146] In addition, ballistic missiles offer limited flexibility in flight path and targeting compared to cruise missiles, reducing adaptability against evolving defenses. As a result, while ATACMS can deliver important operational effects, it cannot support a sustained or autonomous Ukrainian conventional deep-strike doctrine.

145. F. Hoffmann, "Ukraine's Conventional Long-Range Strike Forces at the End of 2025", Missile Matters, 2025, available at: https://missilematters.substack.com.

146. Y. Taradiuk, "Ukraine Confirms Use of US-made ATACMS on Russia after Months of Pentagon Restrictions", *The Kyiv Independent*, November 18, 2025.

Ukraine's domestic designs

Ukraine's most consequential indigenous missile line is the Neptune (R-360) family, which now spans three conceptually distinct variants. The original R-360 anti-ship *Neptune* (derived from the Soviet designed Kh-35 *Kayak*) proved combat effective early in the war and validated Ukraine's ability to integrate propulsion, guidance, and warhead at missile scale. Building on this baseline, a land-attack "Bulged" Neptune adapts the airframe and mission profile for fixed terrestrial targets, trading maritime seekers for navigation optimized for overland routes. The most ambitious evolution, often referred to as "Long Neptune" (R-360L), reportedly aims at ranges approaching 1,000 km, positioning it as Ukraine's closest analogue to a Western cruise missile. The principal advantage of the Neptune line is payload (150-260 kg) relative to drones, enabling effects against military infrastructure rather than mere disruption. The constraints are guidance robustness and industrial scalability: open sources do not confirm a mature, Western-grade TERCOM/DSMAC stack, leaving GNSS vulnerability under heavy jamming as a residual risk; production scale is further bound by energetics, engines, guidance electronics, and wartime quality control.[147]

Flamingo occupies the upper end of the drone–missile continuum. It extends reach and sortie density at lower cost and faster iteration than heavy cruise missiles, which makes it attractive for sustained pressure campaigns. Its advantages lie in availability, flexibility, and operational learning speed. However, Flamingo remains constrained by lighter payloads and simpler navigation, typically relying on GNSS-centric guidance without confirmed terrain or image matching. These characteristics limit its effectiveness against hardened or well-defended targets and expose it to EW over long distances. As a result, Flamingo is best understood as a medium strike system that complements heavier missiles by widening the attack envelope and imposing cumulative costs, rather than replacing them for decisive effects.

Another Ukrainian-designed Sapsan/Hrim-2 represents an aspiration toward short-range ballistic missile (SRBM) capability. In theory, SRBMs offer high speed, penetration, and reduced exposure to traditional air defenses. In practice, they impose higher technological and industrial demands on Ukraine than cruise missiles: precision guidance under EW, solid-fuel quality and consistency, survivable basing, and rigorous systems integration. These demands are magnified by wartime constraints. Consequently, while ballistic options carry signaling value and long-term

147. *Ukraine Air War Monitor*, Vol. 11, 2025; F. Hoffman, "Ukraine's Conventional Long-Range Strike", op. cit.

appeal, they remain aspirational in the near term and do not presently offer a shortcut to reliable, scalable deep-strike cruise missile capabilities.[148]

Beyond those three high-profile systems, Ukraine has publicized additional designs such as Ruta, which reflect experimentation across propulsion, airframe, and mission concepts[149]. Their shared advantages are rapid development cycles and adaptability to available components; their shared limitations mirror those of medium systems—payload mass, guidance systems resilience, and production depth. These projects broaden the portfolio and hedge risk but, absent confirmation of hardened guidance and heavier warheads, are best assessed as adjuncts that expand reach and tempo rather than deliver single-strike decisiveness against protected targets.

Finally, Ukraine has developed a wide array of strike platforms combining medium to long range (100-1,000 km) and lighter payload (less than 100 kg), with various airframes and propulsion (propeller, jet, rocket), sometimes presented as "One-way attack vehicles" or "drones" but increasingly inseparable from missiles. This segment remains central to Ukraine's campaign design despite their limited lethality per round. Their advantages are cost, producibility, and saturation potential: they can be fielded in numbers, adapted quickly, and employed persistently against a wide target set. While their payloads are insufficient for hardened destruction, they excel at disruption, forcing dispersal, triggering air-defense expenditure, and imposing repair and protection costs across Russia's rear.

Their dependence on GNSS and modest terminal accuracy make them vulnerable to EW, but volume and repetition compensate for individual limitations. The enduring importance of light systems lies in campaign economics and system stress, not single-event lethality. By expanding the frequency and geographic spread of attacks, they dilute defender attention, increase the strain on the Russian IADS, and create windows for heavier systems when available. In Ukraine's layered strike posture, light platforms thus function as the pressure layer—a necessary complement to scarce heavy missiles and an effective means of sustaining strategic pressure under industrial and political constraints.[150]

Key lessons learned – Conventional deep strikes

- **Deep strike is a scarce, campaign-shaping capability, not a decisive tool in isolation**. High-end conventional missiles deliver unique effects but cannot be employed at scale or sustained tempo; their

148. Ibid.
149. "Ukraine's RUTA Missile-Drone Will Get an EW-Immune Navigation System", *Defence-UA*, May 17, 2025, available at: https://en.defence-ua.com; J. Marinero, "Ruta: Ukraine's Long Range, Low Cost Precision Loitering Missile", The Dock on the Bay, November 3, 2025, available at: https://medium.com.
150. F. Hoffman, "Ukraine's Conventional Long-Range Strike", op. cit.

value lies in shaping operations rather than achieving strategic decisions alone.

- **Economic sustainability now conditions deep-strike effectiveness**. Limited stockpiles and slow production mean that deep strike must be planned with cost-exchange ratios and industrial resilience in mind, not solely on range or precision.
- **Effectiveness depends on integration, not missile performance alone**. Conventional deep strikes achieve greater impact when embedded in layered campaigns combining asymmetric systems, ISR, deception, EW, and saturation to stress adversary defenses.
- **Adaptive air defenses reduce the payoff of single or limited salvos**. Penetration can no longer be assumed; deep strike increasingly delivers cumulative disruption rather than decisive destruction and must be synchronized with follow-on actions.
- **Deep strikes have a strategic and political impact that needs to be anticipated by planners**. Targeting, employment, and tempo are shaped by escalation management, intra-war deterrence and alliance cohesion, making political usability as important as technical capability.

Conclusion

The Russo-Ukrainian war has become a real-life laboratory for contemporary military technology and operations, not by design but by necessity. Fought under conditions of extreme resource asymmetry, constant adaptation, and sustained high-intensity combat, it has generated an unprecedented volume of empirical evidence on how modern war is fought when mass, precision, connectivity, and attrition intersect. Unlike exercises, simulations, or short campaigns, Ukraine offers a prolonged confrontation against a peer adversary willing to commit the bulk of its conventional power, adapt tactically, strategically and technologically, and absorb losses over time. For NATO, this makes Ukraine not a marginal or idiosyncratic case, but the single most relevant contemporary source for understanding how future conflict is likely to unfold.

A recurring debate in Western military and policy circles questions the relevance of Ukraine's experience for NATO. Critics point to differences in force structure, often noting that Ukraine lacks the depth of air and naval power available to the Alliance, and that the nuclear dimension plays a fundamentally different role for a non-nuclear state than for a nuclear alliance. These arguments may be valid, but they largely miss the strategic point. The Russian conventional military threat to NATO that will emerge from this war is being reshaped, at scale, by Ukrainian battlefield experience acquired against a determined, adaptive opponent. If Russia seeks to confront (openly or covertly) the Alliance in the years ahead, it will do so using tactics and technologies refined in Ukraine – it already does, as demonstrate drone overflights against the NATO territories. Learning from the Ukrainian battlefield is therefore not about preparing to fight like Ukraine; it is about understanding how Russia now fights, adapts, and innovates after having confronted the full spectrum of modern warfare. In that sense, Ukraine represents a unique and time-sensitive opportunity for NATO to learn from the only country that has absorbed and resisted the weight of Russian military power in the field.[151]

One of the central findings of this report is that few of the technologies observed in Ukraine are truly new in isolation. Drones, satellite communications, electronic warfare, precision strikes, and data fusion all predate the war. What is new and consequential is the way these technologies have been combined, scaled, integrated and employed through

151. M. Engqvist (ed.), *The Future of Warfare in Russian Military Thinking*, Stockholm: FOI, R-5806-SE, January 2026; O. Jonsson, "A New Face of War: Russian Military Strategy Post-Ukraine", *Strategy Series*, No. 2, NATO Defence College, February 2026.

a fundamentally digital-native mindset. Ukraine's armed forces have relied extensively on civilian-grade, state-of-the-art technologies, repurposed and adapted at speed for military use. Commercial drones, cloud-based software, private satellite constellations, open-source intelligence, and AI-enabled processing tools have been woven into a dense, adaptive operational fabric. The result is not a collection of novel gadgets, but the emergence of a lethal kill web in which sensors, shooters, communications, and decision-support tools are tightly coupled, continuously updated, and increasingly automated. This accelerated integration has profoundly altered the character of war, compressing decision cycles, eroding traditional distinctions between tactical and operational levels, and placing a premium on connectivity, data processing, and rapid coordination rather than on platform-centric excellence alone.

The Ukrainian case also highlights the return of economics as a central determinant of military effectiveness. The war has exposed, with unusual clarity, the importance of cost-exchange ratios, production capacity, and sustainability over time. Russia's ability to mass-produce relatively cheap one-way attack drones, repurpose legacy munitions, and exploit salvo dynamics has repeatedly strained Ukraine's air-defense resources, forcing constant adaptation. Ukraine's response, layering high-end systems with low-cost kinetic solutions, interceptor drones, and distributed sensor networks, illustrates how operational effectiveness increasingly depends on economic logic as much as on technological sophistication. For NATO, this has direct implications. High-intensity conflict against a peer – or even locally superior – adversary cannot be won, or even sustained, on the basis of exquisite, scarce capabilities alone. The economics of firepower, attrition, and replenishment must be treated as one of the core elements of operational planning and force development, not as secondary industrial concerns.

Furthermore, Ukraine has revealed the criticality of supply chain autonomy, especially in the face of China controlling key elements of the supply chain for a wide variety of conventional weapons (magnets, batteries, electronics). NATO must rethink its production strategy to ensure the sustainability weapons production capacity and of scaling. Other important side of economics – to secure the supply chain with trustable partners that won't disrupt production cycle based on geopolitical interests (China is systematically delaying supply of critical components for drones).

Perhaps the most consequential lesson emerging from Ukraine is institutional. Ukraine's advantage has rested less on possessing superior systems than on its ability to learn, adapt, and iterate faster than its adversary. This capacity to "learn while fighting" has been enabled by unusually tight feedback loops between frontline units, engineers, software developers, and commanders, and by an ecosystem that tolerates experimentation, failure, and rapid modification. In contrast, many

Western defense institutions remain structured around slow acquisition cycles, rigid requirements, and peacetime assumptions about stability and predictability. The gap that matters most for NATO is therefore not a specific capability shortfall, but a learning gap.

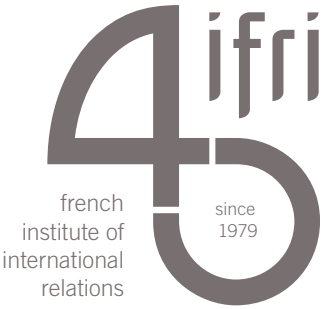
The way forward for NATO follows logically from this observation. Learning from Ukraine cannot be reduced to extracting lessons learned reports or selectively adopting individual technologies. It requires learning how to learn under conditions of rapid change and uncertainty. Continued and intensified support to Ukraine is central to this process. The more NATO will assist Ukraine through sustained military aid, joint ventures, industrial cooperation, training, and on-the-ground engagement, the closer and more integrated the Alliance becomes with the operational realities of this war. That proximity is not only a moral or strategic necessity; it is also a learning mechanism. It allows NATO to observe adaptation in real time, to test assumptions against battlefield evidence, and to grasp how the character of war is evolving under pressure.

For NATO, more important than supporting Ukraine is to start seeing Ukraine not as a temporary receiver of military aid or a testing ground for modern weapons, but as a long-term strategic ally, an essential part of the European security architecture. In this sense, assisting Ukraine and preparing NATO's future are not competing priorities but mutually reinforcing ones. Ukraine is demonstrating, at immense cost, how modern war is fought, how militaries adapt, and how technology, economics, and organization can perform under extreme conditions. For NATO commanders, the central imperative is clear: to treat Ukraine not as an exception to be explained away, but as a warning and an opportunity, accepting it not as a soldier to train from a NATO manual, but as a military instructor who will challenge the manual and rewrite it.

The Alliance's ability to deter, and if necessary fight, in the years ahead will depend less on whether it copies Ukrainian solutions than on whether it internalizes the deeper lesson Ukraine offers—that military advantage in the 21st century belongs to those who can integrate and adapt faster, learn better than their adversaries, and do it as part of a team.

Latest publications from *Focus stratégiques*

- Guillaume Furgolle, "L'autonomisation dans le milieu sous-marin : une révolution sans limite ?", *Focus stratégique*, No. 131, Ifri, January 2026.
- Léo Peria-Peigné, "Char de combat : obsolescence ou renaissance ?", *Focus stratégique*, No. 130, Ifri, November 2025.
- Élie Tenenbaum, with Jean-Baptiste Guyot et Guillaume Furgolle, "Quelle autonomie capacitaire pour l'Europe ? Une analyse multi-domaine", *Focus stratégique*, No. 129, October 2025.
- Amélie Férey and Pierre Néron Bancel, "'Glaives de fer', une analyse militaire de la guerre d'Israël à Gaza", *Focus stratégique*, No. 128, Ifri, October 2025.
- Rachid Chaker, "La guerre au commerce au XXIe siècle. Enjeux et défis pour la Marine française", *Focus stratégique,* No. 127, Ifri, August 2025.
- Guillaume Furgolle, "Repenser la fonction "Protection – Résilience". Un nécessaire changement de paradigme face à un environnement qui se durcit", *Focus stratégique*, No. 126, Ifri, July 2025.
- Amélie Férey, "Sous le feu des normes. Comment encadrer sans désarmer la défense européenne ?", *Focus stratégique*, No. 125, Ifri, April 2025.
- Jonathan Caverley, Ethan Kapstein, Léo Péria-Peigné and Élie Tenenbaum, "Une base industrielle de défense transatlantique ? Deux analyses contrastées", *Focus stratégique*, No. 124, Ifri, March 2025.
- Léo Péria-Peigné and Amélie Zima, "Pologne, première armée d'Europe en 2035 ? Perspectives et limites d'un réarmement", *Focus stratégique*, No. 123, Ifri, February 2025.
- Adrien Gorremans, with Jean-Christophe Noël, "L'avenir de la supériorité aérienne. Maîtriser le ciel en haute intensité", *Focus stratégique*, No. 122, Ifri, January 2025.
- Héloïse Fayet and Léo Péria-Peigné, "La frappe dans la profondeur : un nouvel outil pour la compétition stratégique ?", *Focus stratégique*, No. 121, Ifri, November 2024.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org