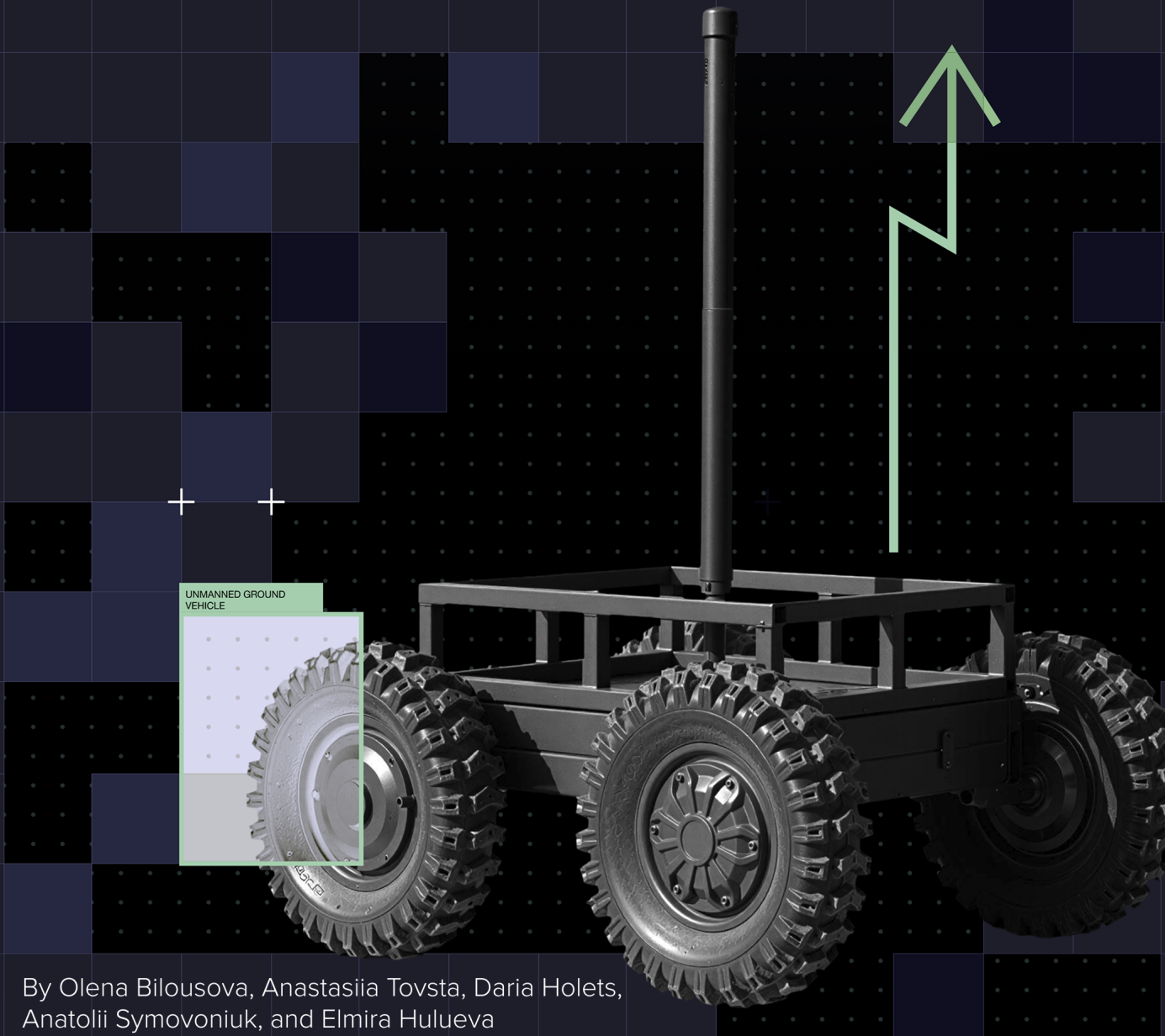
KSE | Institute

BRAVE1 UKRAINIAN DEFENSE INNOVATIONS

Defence Builder

MARCH 2026

THE UKRAINIAN DEFENSE TECHNOLOGY MARKET: OPPORTUNITIES FOR US INVESTORS



By Olena Bilousova, Anastasiia Tovsta, Daria Holets, Anatolii Symovoniuk, and Elmira Hulueva

Editors: Marta Bukhtiiarova, Nataliia Shapoval, Tymofiy Mylovanov, Anna Hvozdiar

ACKNOWLEDGEMENTS

We would like to thank the experts from **Brave 1, Defence Builder, Group 12** and **Altius Capital** who provided consultations and shared their views during the preparation of this report. Their contributions informed the analysis; however, the findings and conclusions presented herein remain solely those of the authors.

This report builds on KSE Institute's series on European defense and Ukraine's strategic defense partnerships with Western countries. Previous reports include:

- From the battlefield to the future of warfare: Harnessing Ukraine's drone innovations to advance US military capabilities (November 2025)
- Rethinking European security in the face of the Russian threat: Learning strategic lessons from Ukraine and relying upon Ukraine for the defense of Europe (June 2025)
- Ukraine's drones industry: Investments and product innovations (October 2024)

EXECUTIVE SUMMARY

Ukraine's defense-technology sector is rapidly evolving into one of the most dynamic and scalable components of the country's industrial economy. While total defense output in 2025 was constrained by the volume of domestic procurement financing, high-technology segments continued to expand at exceptional rates, confirming a structural shift from legacy platforms toward innovation-driven production. UAVs grew by 137%, UGVs by 488%, and electronic warfare by 215%, bringing the combined, conservatively estimated market to $6.8 billion. The real size is likely higher due to decentralized procurement, volunteer funding, and manufacturing by brigades that remain outside formal statistics.

High-technology growth is concentrated in three core segments, each with distinct maturity and risk/return profiles, but all supported by sustained battlefield-driven demand and fast iteration cycles:

- **Unmanned aerial vehicles (UAV)**—largest, scaled market: **$6.3 billion** output in 2025 and **+127%** YoY growth, with expansion across FPV, bomber, ISR, and deep-strike platforms. Deep-strike systems grew fastest (+169%), FPVs remain the mass segment (+110%) with intense competition and rapid cost/performance pressure, and fiber-optic control has scaled quickly in response to harsh EW conditions. The next growth pockets include interceptors (early scaling), domestically produced ISR multicopters to replace Chinese DJI/Autel dependence, and "middle strike" systems bridging tactical FPVs and deep-strike capabilities.
- **Unmanned ground vehicles (UGV)**—early-stage, scaling from a low base: **$252 million** output in 2025 with a **sixfold increase** year-on-year and a still-forming market structure. Growth is led by logistics and evacuation platforms (the adoption-heavy use case), while strike and kamikaze variants are expanding but remain less standardized—creating room for differentiated products that combine reliability, mobility, survivability, and simple operation. Demining and other dual-use pathways strengthen long-term demand and improve business resilience beyond pure wartime procurement cycles.
- **Electronic Warfare (EW)**—strategic enabler across all systems: **$220 million** output in 2025 and **3.1x** YoY growth, reflecting the centrality of spectrum dominance to both survivability and the effectiveness of drones and precision systems. The market is shifting from fragmented experimentation toward concentrated serial production around proven solutions, with rapid scaling in short-range protection, counter-UAV applications, and newer capabilities designed to counter high-precision weapons. Investor value increasingly concentrates in integrated, interoperable architectures rather than standalone devices.

The full-scale invasion has catalyzed a paradigm shift in military doctrine, centered on cost-effective, unmanned solutions that provide strategic parity against conventional forces. Technological progress is concentrated in four areas:

- **Communications –** EW-resilient, multi-layered connectivity (satellite, MANET, directional links) ensuring stable control in contested environments.
- **Navigation –** alternatives to GPS, including inertial and AI-based visual positioning for operations in denied conditions.
- **Autonomy** – a shift toward automatic target recognition, coordinated strikes, and early swarm capabilities that multiply combat effect while reducing operator workload.

- **Modularity & integration –** drones evolving into networked, configurable platforms that can rapidly adopt new payloads and act as force multipliers.

For investment decisions, it's critical to understand which technologies remain promising—and which have already proven ineffective on the battlefield. Below is where key technologies are heading across major defense segments:

- **UAVs (all types):** prioritize EW-resilient communications (including fiber-optic for FPVs), GPS-denied navigation (visual/inertial/terrain-aided), autonomy software (target recognition, retask-in-flight, swarm coordination, automated intercept), that scale across FPV, bombers, ISR, middle-strike, deep-strike, and interceptors.
- **UGVs (ground robots):** logistics/evacuation platforms with robust comms (multi-channel failover), higher autonomy for loading/unloading and routing, ruggedization for mines/shock/vibration, and modular mission kits (engineering, demining, remote turrets).
- **Maritime drones (USV/UUV):** modular multi-role USVs (ISR/EW/strike payloads, "mothership" concepts), and—highest upside but capital-intensive—underwater navigation, sensing (sonar), and communications enabling UUV/AUV scaling.
- **Electronic warfare (EW):** software-defined "smart EW" (detect–classify–targeted jam), integrated SIGINT + jamming loops, deconfliction tools that prevent friendly interference, and layered architectures combining mobile protection with stationary high-power systems.
- **Artificial intelligence:** prioritize computer-vision ATR modules (detection–classification–tracking), multi-source analytical AI / LLM-driven decision-support for fusing drone video, satellite, sensors, and intercepts into actionable situational awareness (e.g., DSS workflows), and GPS-denied autonomous navigation / terminal guidance modules that keep platforms effective under EW—while recognizing AI is still mainly human-in-the-loop and value concentrates in modular, interoperable integration (data pipelines, testing environments, and compatibility across hardware).

In 2025, Ukrainian defense tech companies attracted approximately **$129 million**, with the true figure likely higher given the share of undisclosed security-sensitive deals. The largest investments were concentrated in the AI/software segment, which investors view as lower risk than hardware or weapons production and less constrained by export and other restrictions. The financing landscape combined grants (notably through Brave1 and other donor-backed programs), equity from venture funds, accelerators, and strategic investors, and loans via the expanded "5-7-9" program for defense-critical enterprises (**$160 million**), alongside procurement-linked support from partner states. Case studies indicate that companies which received financing demonstrated strong results and grew significantly.

To reflect defense-specific risk dynamics, the **investment framework** uses Technology Readiness Levels (TRLs) as the organizing logic, since risk and valuation confidence shift sharply from prototype to fielded systems. It aligns financing instruments with maturity—TRL 1–5 (grants/R&D partnerships and SAFEs/convertibles), TRL 5–7 (equity and risk isolation via SPVs/JVs), and TRL 7–9 (growth equity and debt once revenue visibility improves)—and applies a checklist centered on TRL and operational validation, IP ownership, compliance, and certification/codification readiness.

Building on the financing and investment landscape outlined above, Ukraine's cooperation with the United States is underpinned by **a broader strategic partnership** shaped by shared security interests and long-term Euro-Atlantic alignment, which has expanded since 2022 into a more institutionalized

framework spanning defense, technology, energy, and investment. This architecture is anchored by baseline agreements (including the renewed U.S.–Ukraine Charter on Strategic Partnership and the bilateral ten-year security agreement under G7 commitments) and reinforced through multi-year U.S. funding mechanisms and joint coordination formats—providing a stable backdrop for deeper industrial cooperation and recovery-oriented investment initiatives. 10-year potential for recovery and defense after the end of the hostilities is estimated at **$690 billion**.

Recommendations for investors:

- **Prioritize TRL and operational proof.** Ukraine's strongest advantage is access to technologies that have combat validation; diligence should focus on field testing, end-user feedback, and mission logs.
- **Audit IP end-to-end.** Require a rigorous review of IP ownership and legal assignments, and confirm protection is maintained and enforceable in Ukraine, the U.S., or the EU.
- **Focus on technological priorities.** Consider developing technologies, which focus on advanced technologies: communication, navigation, autonomy, modularity & integration.
- **Invest in localization of critical components.** Reducing reliance on Asian supply chains—microelectronics, motors, sensors—supports resilience and longer-term export potential through a more vertically integrated base.
- **Adapt for Ukrainian war conditions.** Traditional investment models must be adapted to the realities of Ukraine's market.
- **Position for post-war exports.** Despite wartime export limits, invest in NATO-standardized/codified products with relevance for U.S. and allied militaries to capture future export upside.
- **Fund enabling infrastructure.** Consider direct investment not only in products but also in training schools, R&D centers, and testing grounds that strengthen the ecosystem and scaling capacity.

TABLE OF CONTENTS

DEFENSE INDUSTRY MARKET OVERVIEW

Ukraine's defense industry is rapidly transforming from a sector focused primarily on meeting security needs into one of the key drivers of national economic development. Alongside enterprises that inherited the Soviet-era specialization in conventional weapons and heavy platforms, a new ecosystem of defense-technology companies has emerged and is scaling at an unprecedented pace. These firms are not only strengthening battlefield capabilities but are also reshaping the structure of the defense-industrial base toward innovation-driven growth.

In 2025, overall defense production demonstrated only limited expansion compared to 2024, largely constrained by the available volume of domestic procurement financing. However, within this aggregate figure, **defense technologies continued to grow at a markedly faster rate**, significantly increasing their weight in the sector. Production of unmanned aerial vehicles (UAVs) expanded by 137%, unmanned ground vehicles (UGVs) by 488%, and electronic warfare (EW) systems by 215%**.** Together, these high-technology segments reached an estimated **market volume of $6.8 billion in 2025**, underscoring the structural shift toward modern, innovation-intensive capabilities.

At the same time, this figure should be regarded as **conservative**. A comprehensive assessment of the defense technology market remains methodologically challenging due to the **high level of data sensitivity** and the fragmentation of procurement channels: in addition to centralized state procurement—primarily conducted through the Defense Procurement Agency—a substantial share of acquisitions is financed through alternative mechanisms, including direct contracting by military units and large-scale purchases funded by thousands of charitable and volunteer foundations.

Moreover, a portion of production is carried out directly within **military brigades** and other units for their own operational use. These in-house manufacturing and assembly efforts—often focused on drones, electronic warfare components, and tactical adaptations—do not pass through formal market transactions and therefore remain statistically invisible. Despite being outside conventional accounting frameworks, this distributed production capacity forms an important part of Ukraine's wartime innovation model and further increases the real scale of deployed technologies.

As a result, the **actual market size is likely higher than current estimates suggest**. The combination of rapid technological scaling, diversified procurement mechanisms, and strong battlefield-driven demand positions Ukraine's defense-technology sector not only as a cornerstone of national security, but also as a growing pillar of the country's industrial output, innovation capacity, and long-term economic resilience.

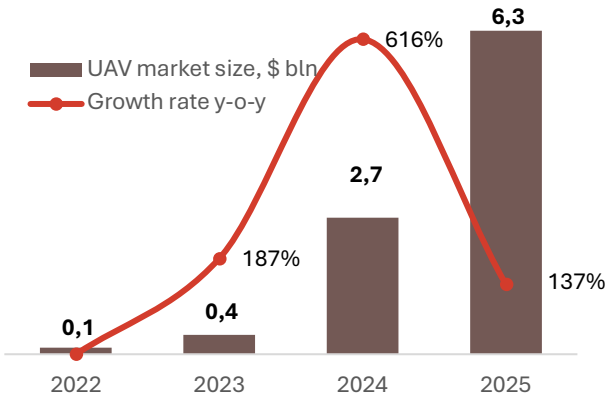
Unmanned Aerial Vehicles (UAVs)

Since 2020, Ukraine's UAV manufacturing sector has transformed from a niche, early-stage activity into the largest and most dynamic segment of the dual-use and defense technology industry. Its expansion has been driven by wartime demand, rapid technological adaptation, regulatory simplification, and strong state support combined with private-sector initiative.

The market has scaled at an exceptional pace, with production increasing by orders of magnitude and covering the full spectrum of platforms – from small FPV systems to deep-strike drones. This growth has been accompanied by the rapid entry of new firms, particularly small and micro enterprises, which now play a central role in innovation, flexibility, and the rapid deployment of new solutions. As a result, the sector is evolving from the earlier dominance of a few large manufacturers toward a more

diversified and competitive structure, while still retaining a high level of revenue concentration among leading producers.

FIGURE 1. UAV MARKET SIZE, $ BILLION



Source: KSE Institute assessment

In 2025, the Ukrainian unmanned aerial vehicle (UAV) sector generated an estimated **$6.3 billion** in output, with at least 150 companies active in the sector. The sector grew by 137% compared with the previous year.

Medium-sized companies form the backbone of industrial output, ensuring scalable production, whereas large firms provide volume, integration capacity, and program stability. At the same time, the proliferation of smaller producers strengthens resilience, shortens development cycles, and accelerates technological iteration.

The sector is overwhelmingly driven by private companies, while the role of state-owned enterprises has declined in relative terms, even though the remaining state player continues to hold strategic weight due to its scale.

Financially, rapid revenue growth has been accompanied by rising short-term liabilities, reflecting the fast expansion of production, procurement cycles specifics, and the limited availability of long-term capital. Investment in fixed assets has accelerated more recently, signaling a gradual transition from emergency scaling to more sustainable industrial development.

Dynamics of the Ukrainian UAV Market by Segment

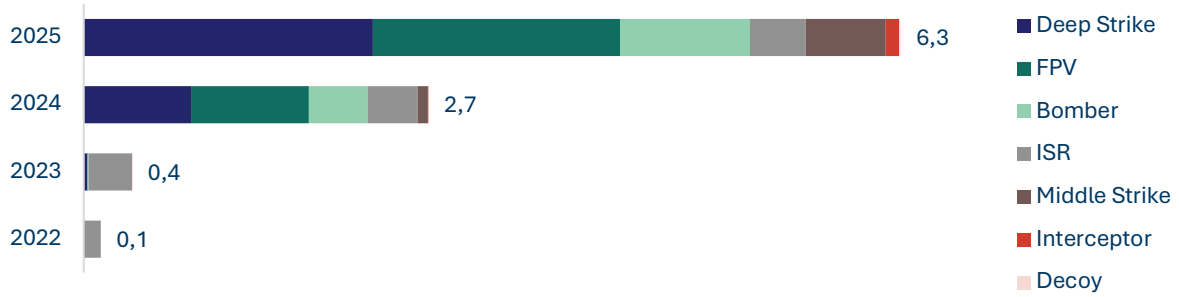
In 2025, all major segments of the Ukrainian unmanned aerial vehicle (UAV) market demonstrated continued expansion, reflecting both the intensification of combat operations and the rapid adaptation of domestic industry to evolving battlefield requirements. However, the pace of growth varied significantly across categories, highlighting shifts in operational priorities and technological maturity.

The **deep-strike** UAV segment recorded the fastest growth, expanding by **169%** year-on-year. This surge directly correlates with the increasing operational use of long-range systems against high-value military targets and energy infrastructure in the enemy's rear.

FPV drones continued to scale rapidly, growing by **110%**, and remain the backbone of daily tactical operations along the frontline. They are the most widely used strike asset for short-range engagements, enabling cost-effective and highly precise targeting. At the same time, this segment is

characterized by **intense competition**, with a large number of manufacturers with similar products and continuous pressure to improve performance while reducing unit costs. A defining market trend in 2025 was the rapid development and deployment of fiber-optic FPV drones, driven by the increasingly harsh electronic warfare (EW) environment.

FIGURE 2. UAV BY TYPE, $ BILLION



Source: KSE Institute assessment

The **bomber UAV** segment expanded by **121%**, although the market structure here is more concentrated. A limited number of proven models account for the majority of deployments, indicating a limited number of platforms that have demonstrated operational reliability and established production capacity.

Growth in the **ISR (intelligence, surveillance, and reconnaissance)** segment was more moderate at **11%**, reflecting its relative maturity. This is the oldest and most structurally stable UAV market in Ukraine, with a clear and consistent market leaders. The key forward-looking trend in this category is the development of domestically produced ISR multicopters intended to **replace Chinese DJI Mavic and Autel systems**, which remain widely used but pose supply-chain and security risks.

The **interceptor UAV** segment entered an active development phase only in 2025. Although several models have already achieved early dominance, the market is still in its formative stage and offers **substantial room for new entrants** and technological differentiation. Given the growing need to counter enemy reconnaissance and strike drones, this category is expected to demonstrate accelerated growth in the coming years as production scales and deployment becomes more systematic across the Defense Forces of Ukraine.

In addition to the core segments, several **smaller but high-potential categories** are emerging:

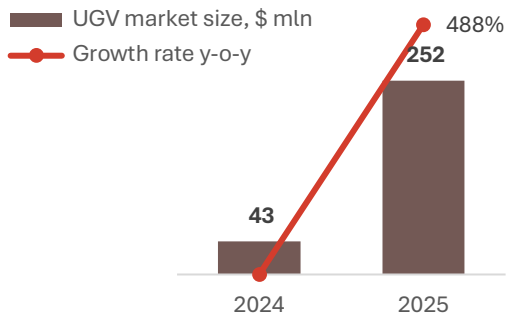
- **Middle strike UAVs** are likely to gain importance as the effective "kill zone" expands and engagement distances increase. Range is becoming a critical operational parameter, which will drive demand for systems that bridge the gap between tactical FPVs and deep-strike platforms.
- **Decoy UAVs** will grow in parallel with the expansion of long-range strike operations. As the scale of deep strikes increases, the use of decoys will be essential to saturate enemy air defenses and maintain a **lower average cost per successful attack**.

Overall, the Ukrainian UAV sector is moving from an emergency, demand-driven surge to a more structured industrial ecosystem. Despite continued concentration among leading firms, the increasing role of SMEs, diversification of production, and rapid technological adoption are creating a more competitive, adaptive, and resilient market with strong medium-term development potential.

Unmanned Ground Vehicles (UGVs)

The UGV market in Ukraine is still young, "fresh", and not yet fully formed. The years 2022–2023 were a "period of enthusiasts" for the UGV industry, and it developed more slowly than the UAV (aerial drone) segment. This was because aerial drones had a lower barrier to entry for development due to the availability of ready-made components, training courses, and software, as well as a higher demand and more predictable expected results. At the same time, the UGV market is highly diversified, with many manufacturers and developments, so a producer with a high-quality product can enter the market quickly and even become a leader.

FIGURE 3. UGV MARKET SIZE, $ MILLION



Source: KSE Institute assessment

In 2025, the Ukrainian unmanned ground vehicle (UGV) sector generated an estimated **$252 million** in output, with more than 50 companies active in the market. This represents a **sixfold** increase compared to the previous year.

Ukraine's unmanned ground vehicle (UGV) sector remains at an early stage of development but is expanding rapidly from a low base. The market is still relatively small within the broader defense ecosystem, yet production has grown sharply in recent years, driven by wartime demand, government support, regulatory simplification, and cooperation with international partners.

The industry is characterized by a limited number of players and a high level of revenue concentration among a few leading companies. At the same time, new entrants continue to appear, gradually diversifying the structure and signaling strong long-term scaling potential. Most firms are small or medium-sized, which supports flexibility and rapid experimentation, while the first signs of interest from larger industrial actors indicate a possible transition toward more sustainable, large-scale production models.

The ownership structure is dominated by private limited-liability companies, with no state-owned entities in the sector. Financially, sectoral growth has been accompanied by increasing reliance on debt financing, pointing to expansion under constrained access to long-term capital.

Dynamics of the Ukrainian UGV Market by Segment

UGV production now covers a wide range of applications — from logistics and evacuation platforms to combat and demining systems — with a growing level of autonomy and integration into broader battlefield networks. However, the market is still in the process of formation: investment in fixed assets remains limited, revenues are uneven across firms, and export potential is not yet explored.

FIGURE 4. UGV BY TYPE, $ BILLION

Source: KSE Institute assessment

Logistics platforms form the backbone of the UGV market, accounting for **61% of total sector** volume in 2025. This category was the primary driver of overall market expansion, increasing by **556%** compared to the previous year**.** The dominance of logistics solutions reflects their role in the most frequent UGV missions: ammunition delivery, evacuation of the wounded, transportation of equipment, and resupply under fire. These tasks address immediate operational needs while reducing risks for personnel, which explains both the rapid adoption and the continued scaling of production. Given the persistent demand for protected and automated supply chains on the frontline, this segment is expected to **maintain strong growth in the medium term**, with significant additional capacity still to be absorbed by the Defense Forces.

The **kamikaze UGV** segment recorded the highest relative growth rate, expanding by **967% year-on-year**. Despite this sharp increase, it **remains very small in absolute terms**, especially when compared to aerial kamikaze drones that perform similar strike functions. At the same time, the operational logic of ground-based and aerial kamikaze systems differs substantially in terms of mobility, survivability, terrain dependence, and tactical deployment. As a result, it is still unclear whether these two segments will evolve as complementary capabilities with distinct niches or remain in partial competition for resources and mission profiles.

The **strike UGV** segment grew by **19%** but continues to represent a relatively small share of the overall market. Although several successful combat uses have been publicly reported, these systems are not yet widely deployed at scale. Their limited adoption suggests that existing platforms have not fully matched the requirements of frontline units in terms of mobility, protection, ease of operation, and cost-effectiveness. At the same time, this creates a **window of opportunity for technological breakthroughs**—particularly for solutions that are simple to operate, rapidly scalable in production, and tailored to current frontline conditions.

In addition to the core categories, several **smaller but fast-growing segments** are emerging:

- **Demining** UGVs remain a relatively small portion of the market but demonstrate strong growth dynamics and **exceptionally high long-term potential**. The scale of mined territories in Ukraine creates sustained demand for automated and remotely operated clearance solutions, both for military and civilian applications.
- **Firefighting** UGVs also represent a niche segment, yet their development highlights the importance of dual-use technological pathways. Platforms that can be applied in both defense and civilian contexts improve business sustainability, diversify revenue streams, and strengthen the resilience of manufacturers in a highly volatile defense procurement environment.

For UGVs to become a mass-produced, effective weapon, several groups of factors must be balanced, each depending on different stakeholders — manufacturers, the state, commanders, instructors, and

the soldiers themselves.[1] The key factors include the general **technical capabilities** of the UGVs, such as reliability in aggressive environments, maneuverability, resistance to EW and fire, and payload capacity. Meanwhile, the market side of the issue includes the cost of UGV production and the need for sufficient manufacturing capacity to cover potential state contracts. As the co-founder of the NGO "Aerorozvidka" emphasizes, if you simply buy a UGV without training people to operate it or integrating it into combat processes, there will be no real benefit.[2] A constant, dynamic balance is required between new technologies and the military's adaptation.

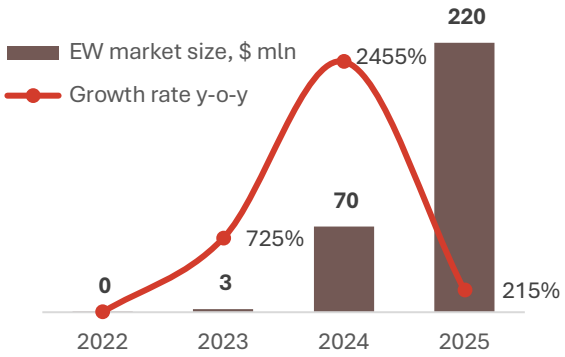
Overall, the UGV sector in 2025 is characterized by **logistics-driven growth, early-stage experimentation in combat roles, and the gradual emergence of dual-use applications**. The segments with the highest adoption rates are those that directly solve immediate operational challenges, while combat UGVs still require further technological adaptation to achieve mass deployment. In the longer term, sustained demand for automation in supply, evacuation, and demining operations will remain the key structural factor shaping the market. The segment is moving from a nascent, experimental phase toward a more structured industry. Continued entry of new companies, rising competition, and the gradual involvement of larger manufacturers are expected to drive the next stage of growth and industrial scaling.

Electronic Warfare

Ukraine's electronic warfare (EW) sector has expanded rapidly in recent years, moving from a relatively small and volatile segment to one of the key technology-driven components of the defense ecosystem. Although the core technologies were already in place, their large-scale deployment was triggered by the surge in battlefield demand. Growth has been fueled by wartime demand, the critical role of spectrum dominance on the battlefield, and the ability of domestic companies to deliver combat-proven solutions in a very short development cycle.

In 2025, the Ukrainian electronic warfare sector generated an estimated **$220 million** in output, with 3.4x market growth compared to the previous year.

FIGURE 5. EW MARKET SIZE



Source: KSE Institute assessment

Structurally, the sector combines a large number of small, specialized developers with a narrow group of medium and large manufacturers that generate most of the output. In the most recent period,

[1] See "More than 1,600 developments registered on Brave1 platform – Digital Transformation Ministry", Ukrinform
[2] See ""Soon the drone will make its own decisions": Ukrainian defense-tech trends", Liga Net [ua]

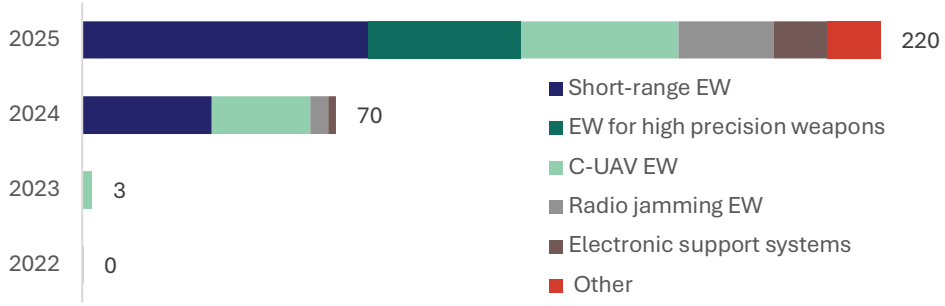
production has become significantly more concentrated among leading companies, reflecting the transition from experimental development to scaled manufacturing and the growing importance of system integration, serial production, and operational reliability.

The sector is primarily privately owned, with state-owned companies responsible for a number of critical systems. Financially, the sector has moved from a period of stress toward gradual stabilization, although expansion continues to rely heavily on short-term financing, pointing to the persistent shortage of long-term capital for industrial scaling.

Dynamics of the Ukrainian EW Market by Segment

Technologically, Ukrainian EW solutions now cover the full spectrum of functions — from electronic intelligence and suppression to protection of friendly systems and counter-UAV applications — and are deeply integrated into network-centric combat operations.

FIGURE 6. EW BY TYPE



Source: KSE Institute assessment

In 2025, all major electronic warfare (EW) categories demonstrated strong growth, reflecting the critical and continuously expanding role of electromagnetic spectrum dominance on the modern battlefield. The scaling of EW production and deployment has been driven by the need to counter increasingly sophisticated threats, protect personnel and equipment, and ensure the effectiveness of Ukraine's own unmanned and precision-strike capabilities.

Short-range EW systems constituted the largest segment of the market, accounting for **36% of total EW output**, and expanded by **122% year-on-year**. Their leading position is explained by their direct and constant use at the tactical level, where they provide immediate protection for units against enemy drones, communications, and other radio-controlled threats. These systems are now an integral element of frontline survivability and are being deployed at scale across a wide range of units.

The **counter-UAV (C-UAV) EW** segment also showed substantial growth, increasing by **195%** compared to the previous year. This reflects the continuing rise in the use of enemy unmanned systems and the corresponding need for layered defensive solutions capable of detection, disruption, and suppression across different ranges and frequencies. The expansion of this category is closely tied to the broader drone-centric nature of the war.

A notable development in 2025 was the emergence of **EW systems designed to counter high-precision weapons**, which formed a **new and rapidly scaling category**, reaching **19% of the total EW market** within a single year. The appearance of this segment highlights the growing importance of

electronic protection against guided munitions and advanced strike systems and signals a shift toward more complex and specialized EW capabilities.

Looking ahead, **continued growth is expected across all EW categories**, driven by the persistent escalation of electronic contestation on the battlefield. At the same time, it is methodologically difficult to isolate long-term trends for individual segments, as EW effectiveness is determined not by standalone systems but by their integration into a **coherent, multi-layered architecture**. The operational impact is achieved through the combined performance of detection, suppression, protection, and electronic support elements, which together create a cumulative effect. As a result, future development will be defined less by the dominance of a single category and more by the ability to build interoperable, system-of-systems EW solutions that enhance overall combat effectiveness.

Overall, the EW industry is transitioning from a fragmented innovation-driven environment toward a more structured and concentrated production model, with leading firms gaining strategic weight while smaller players continue to provide agility and niche technological breakthroughs.

Other Sectors

Several defense technology segments were not included as standalone market categories in this report due to the **limited availability of reliable and verifiable data**. In most cases, this constraint is driven by the high level of operational sensitivity, the early stage of market formation, or the absence of clear procurement and production benchmarks that would allow for consistent quantitative assessment. Nevertheless, these areas represent important components of the broader defense innovation ecosystem and demonstrate strong long-term potential.

One such segment is **maritime unmanned systems**. Within this domain, the **surface drone market** reached operational maturity earlier, with a small number of companies dominating production and deployment. At the current stage, the primary development trajectory is shifting from platform scaling to integration with other capabilities, including coordinated operations with aerial systems, intelligence assets, and long-range strike architectures. In contrast, **underwater and semi-submerged drones** remain a younger and less structurally defined market. Given their expanding range of missions, this segment is expected to **demonstrate faster growth in the coming years** as technological solutions mature and production capacity increases.

Another cross-cutting area that is not reflected as a separate market segment is **artificial intelligence (AI)**. Quantitative assessment is particularly challenging because AI is embedded across multiple product categories rather than procured as a standalone capability. However, the operational demand for AI-driven solutions is growing rapidly. The most prominent applications include **autonomous navigation** in electronic warfare–saturated environments and **machine vision** for target recognition**.** The increasing complexity of the battlefield and the need for reduced operator workload strongly suggest that AI adoption will continue to accelerate across all unmanned and electronic warfare systems, making it one of the key qualitative drivers of future capability development, even if its market size cannot yet be measured independently.

Taken together, these data gaps do not indicate limited relevance. On the contrary, they highlight segments that are either highly sensitive, structurally embedded in other markets, or at an early stage of rapid formation.

TECHNOLOGICAL PRIORITIES

Since 2022, Ukraine has moved from reliance on commercial off-the-shelf components to domestically developed military-grade solutions in communications, navigation, and autonomy—the three core enablers of drone effectiveness. The spread of enemy electronic warfare (EW) and the constantly shifting operational environment have accelerated the need for resilient technologies and local production.

Communications underpin all unmanned operations. Ukrainian companies have created EW-resistant architectures based on open-source software, multi-band modems, and hardened military systems. The combination of satellite connectivity (particularly Starlink), phased-array antennas, MANET networks, and directional data links ensures stable command and data transmission in contested environments.

Navigation has progressed beyond dependence on GPS. Inertial systems, ground-based triangulation, and AI-driven visual positioning—such as solutions developed by Bavovna.ai and Twist Robotics—allow drones to operate effectively in denied or degraded signal conditions.

Autonomy is transforming drones from remotely piloted assets into increasingly independent combat systems. What began as basic flight automation in 2022 has evolved into capabilities such as automatic target recognition, coordinated strikes, and early swarm intelligence, as demonstrated by companies like The Fourth Law and Swarmer. This reduces operator workload while multiplying battlefield impact.

At the same time, the **integration and modularity** of platforms is expanding operational roles. Different drone classes now function as interconnected systems and as force multipliers for conventional weapons—from FPVs paired with bombers to naval drones equipped with air-to-air missiles. Each platform is becoming a configurable base to which new payloads and functions can be rapidly added, creating virtually unlimited pathways for capability growth.[3]

Unmanned Aerial Vehicles (UAVs)

Russia's full-scale invasion has turned unmanned systems into the dominant strike capability on the battlefield. In 2025, UAVs accounted for 80–85% of engagements against frontline targets, including no fewer than 215,000 strikes over the summer period.

FPV drones are first-person-view loitering strike UAVs that provide low-cost, high-precision engagement through real-time operator control. First improvised in 2022 from commercial racing quadcopters, they rapidly became a core firepower tool as artillery shortages and enemy numerical superiority created demand for scalable precision strikes. Their use grew to around 30,000–45,000 engagements per month, enabling Ukrainian forces to destroy most targets within the 0–10 km frontline "kill zone" and high-priority objectives deeper in the rear with high accuracy against infantry, armor, and logistics. Over time they have evolved into a multi-purpose platform capable of supply delivery and communications relay, while current development focuses on localizing

[3] Note: This report is a continuation of our previous work on the drone innovations and expands the scope from a single domain to the entire innovative defense technology ecosystem. The core sectoral dynamics identified earlier remain valid and are therefore referenced here in a condensed form. For more information, please see "From the Battlefield to the Future of Warfare: Harnessing Ukraine's Drone Innovations to Advance U.S. Military Capabilities", KSE Institute

components, fiber-optic control to resist electronic warfare, and greater autonomy through automated targeting and swarm capabilities.

Multicopter bombers are heavy-lift UAVs designed for repeated precision strikes and aerial logistics through the sequential release of munitions while hovering over a target. Developed in Ukraine since 2014–2015 and scaled during the full-scale invasion, they compensate for artillery shortages by carrying up to 15 kg per sortie (and up to 100 kg per night through multiple flights) at typical ranges of 15–20 km, with special missions reaching 40–60 km. Operated mostly at night due to their size, they are used by every frontline brigade primarily to destroy shelters and buildings, mine supply routes and forest approaches, and deliver cargo to positions that ground vehicles can no longer reach; one UAV unit conducted over 1,600 deliveries in 2024 and emplaced about 11,000 mines in the first seven months of 2025. Their effectiveness comes from high strike accuracy with post-drop adjustment, unique performance in forested terrain, and growing resilience to electronic warfare through CRPA GPS, visual navigation, improved communications, and increasing mission autonomy.

Middle Strike UAVs are long-range loitering and bomber platforms designed to engage targets in the enemy's operational depth, typically from 20–40 km up to 150–200 km beyond the frontline. Emerging as a response to the declining effectiveness of satellite-guided munitions and the need to hit moving or recently relocated targets, they provide a dynamic pursuit-and-strike capability unavailable to most artillery and missile systems. This category—represented by systems such as the Switchblade 600 and RAM-2X and sometimes extended-range FPVs—destroys armor, artillery, air defense, radars, and logistics assets in rear areas, thereby disrupting force sustainment and battlefield cohesion. Their extended range is achieved through aerodynamic fixed-wing designs, larger energy capacity, and longer communication links, often with autonomous pre-programmed missions and terminal guidance. By mid-2025 more than ten models were in service, with further development focused on automated target detection, real-time mission control, and the ability to retask or abort strikes in flight.

Deep Strike UAVs are long-range one-way attack drones designed to deliver warheads at distances of roughly 300–2,000 km, providing Ukraine with a scalable strategic strike capability that was absent at the start of the full-scale invasion. Evolving from a few basic systems in 2022 to more than 11 manufacturers with annual production capacity exceeding 33,000 units, they enabled 3,776 successful target engagements in 2024 and can project force over about 25% of Russian-controlled territory. Their payload flexibility (8–250 kg) allows strikes against military depots, airfields, command posts, defense industry facilities, logistics hubs, and the oil sector, generating effects that go beyond physical destruction by forcing the adversary to disperse assets, invest in air defense, and shift resources from offense to protection and recovery. As a result, they reduce pressure on the frontline and have become a core element of Ukraine's deterrence strategy, with ongoing development focused on greater reliability, low-altitude penetration, electronic-warfare resistance, visual navigation, precision targeting, specialized warheads, and fast jet-powered "drone-missile" variants that combine the scalability and low cost of UAVs with the speed and kinetic energy of missiles.

Interceptor UAVs are unmanned aerial systems designed to destroy enemy reconnaissance and strike drones in the air, forming a low-cost, scalable alternative to traditional air defense. Developed rapidly in 2024–2025 in response to the widespread Russian use of ISR UAVs for artillery correction and precision strikes, this capability combines radar detection with high-speed multicopter and fixed-wing drones that can engage targets at altitudes up to 5 km and speeds around 120 km/h, with newer specialized platforms exceeding 300 km/h and operating more than 30 km from the launch point.

Their primary targets near the frontline are systems such as Orlan, Supercam, Zala and Lancet, and at the tactical level they deliver a cost-exchange ratio of roughly 1:10 because they rely on simple communications and inexpensive optical guidance to destroy UAVs equipped with costly payloads and navigation systems. The number of successful interceptions grew from a few hundred per month in late 2024 to over one thousand by summer 2025, significantly reducing the enemy's ability to detect Ukrainian positions and conduct effective strikes, while offering a far more economical solution than surface-to-air missiles. Current development focuses on fully specialized interceptor designs, automated guidance, reusable armed platforms, carrier-launched airborne interceptors, and coordinated multi-drone engagement, reinforcing the emerging principle that the most effective counter to UAVs is other UAVs.

Reconnaissance UAVs are unmanned platforms that provide continuous situational awareness by detecting enemy forces, directing fires, and conducting battle-damage assessment, and today they generate roughly 80–90% of frontline target identification while maintaining round-the-clock surveillance. Before 2022 Ukraine operated only a handful of domestic fixed-wing ISR systems and relied heavily on Chinese multicopters, but the full-scale invasion triggered mass procurement and rapid domestic development, resulting in more than 35 new Ukrainian models, including multiple local analogues of the DJI Mavic. Typical fixed-wing systems operate at 30–50 km combat radius with up to 2–3 hours endurance (with some exceeding 7–28 hours), while multicopters cover the close tactical zone; newer platforms also feature GPS-independent optical and AI navigation. Since mid-2025 the widespread use of enemy interceptor drones has increased losses and forced reconnaissance UAVs to fly higher and faster, reduce time over target, and adopt higher-resolution sensors, signature reduction, threat-detection systems, and automated evasive maneuvers, driving the next cycle of technological adaptation.

Unmanned Ground Vehicles (UGVs)

As of 2026, various Ukrainian Unmanned Ground Vehicles (UGVs) are increasingly being integrated into the Armed Forces of Ukraine's combat operations. They serve as a vital tool for **enhancing personnel safety and operational efficiency** within highly hazardous environments of minefields, dense enemy fire, pervasive drone activity, and active electronic warfare (EW). However, the current development of the UGV industry and the shifting dynamics of the battlefield do not allow these drones to fully replace humans, rather, they are transforming the methods of warfare. Military personnel are not being removed from the process, nor is their number decreasing. Instead, their roles and presence are evolving: rather than being physically exposed to fire, they now operate machinery from the safety of cover.[4] The **primary advantage of UGVs** lies in reducing the risk of casualties among personnel and increasing the overall effectiveness of combat operations, particularly in logistics.

Therefore, for successful combat missions, a UGV must possess high structural and electronic reliability, resistance to enemy EW interference, and the ability to operate even when damaged. High maneuverability is also essential, as the drone must navigate complex terrain while maintaining minimal dimensions to remain less conspicuous. Preference will also be given to highly autonomous

[4] See ""Vepr" took the fighter out of a hopeless situation: otherwise he would have died." Commander of the Robotic Systems Service "Da Vinci Wolves" Oleksandr Yabchanka – about ground drones that will soon fight instead of people", Novynarnia [ua]

designs that can minimize the time required for loading, unloading, and deployment. Last but not least, a UGV must be capable of maintaining a reliable communication link at a distance from high-risk zones (7–10 km from the front line).

Within the Ukrainian military UGV market, the following categories can be distinguished by their intended mission profile:

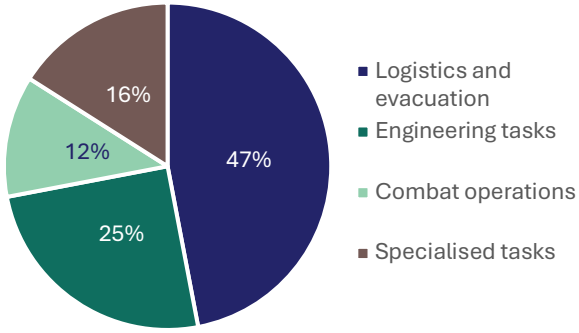
- **Logistics UGVs** are designed to deliver ammunition, water, food, medical supplies, and construction materials to infantry positions, as well as to evacuate equipment. In most cases, these UGVs are operated remotely from cover, with mandatory oversight provided by a reconnaissance copter. Currently, they are recognized as the most popular category because they are easier to master, missions are conducted within controlled territory where tracking progress is simpler, they do not require crossing the line of contact, and they do not necessitate specialized weaponry or complex balancing. An example of such a UGV is the multi-purpose Ratel H, which performs evacuation and the delivery of medical gear, ammunition, and cargo up to 400 kg, features a power reserve of 60 km, and is equipped with IR headlights, night vision cameras, and a launch platform for fiber-optic FPV drones.[5] Logistics platforms provide the most stable and scalable results and currently hold the best prospects for mass implementation.
- **Engineering platforms** are primarily designed for various tasks such as trench digging, deploying engineering support equipment, and clearing debris. They are frequently equipped with mine rollers (trawls), manipulators, and specialized engineering modules.
- **Evacuation UGVs** are required to transport the wounded from positions, though several barriers to wider adoption remain. These include a psychological barrier, as wounded soldiers often distrust the machine, and a tactical barrier, as medics cannot constantly walk alongside the drone due to the high risk of attack. Ukraine is the first country in the world to begin systematically replacing evacuation teams with UGVs. A prime example is Operation "Skittles" by the 1st Medical Battalion, during which two evacuation missions were conducted from different points, covering a total distance of 84 km in nearly 7 hours, with both soldiers surviving.[6] During the second mission, an FPV drone struck the armored capsule — while the hull was damaged, the wounded soldier inside was unharmed, and the robot completed the evacuation.
- **Reusable strike platforms** consist of either mobile combat robots equipped with weaponry, such as machine guns or grenade launchers, designed to return after a mission, or static turrets.[7] They are used for direct engagement, holding positions, supporting assaults, and countering enemy drones. An example of such a platform is the "Lyut" (Fury) robotic complex, developed with Brave1's support. It is armed with a 7.62 mm machine gun for delivering fire in combat conditions. "Lyut" was notably deployed by a Special Operations Forces (SOF) unit in the Kursk region, executing a coordinated attack involving the machine gun, FPV drones, and mortar fire against Russian positions.[8] As a result, it neutralized the enemy, survived hits from an FPV drone and an RPG, and successfully returned for repairs. Despite these successes, mobile combat robots remain less widespread due to the complexity of planning

[5] See "Ukrainian Ratel H UGV became the carrier of fiber optics FPV drones", Militarnyi [ua]
[6] See "Architecture of the Future Battlefield: How Ukrainian UGVs Rewrite the Limits of Human Risk", Army Inform, [ua]
[7] See "Unmanned Ground Vehicles (UGVs): when will robots replace humans?", VGI-9, [ua]
[8] See "Russians complain that the Armed Forces of Ukraine have more and more combat robots on the battlefield: how "Lyut" hits the enemy with a machine gun", Defense Express [ua]

and executing missions. A ground drone must navigate difficult terrain, avoid mines, and avoid getting stuck. There is also the risk of weapon malfunctions (jams), which are difficult for engineers to solve remotely and can lead to the failure of the entire mission.

- **Kamikaze (one-way mission) platforms** are single-use systems carrying a large explosive payload. While the "target market" for one-way missions is currently dominated by aerial drones, UGVs offer superior accuracy and significantly higher payload capacity.
- **Minelaying UGVs** are used for remote mine deployment. They offer significant advantages, including higher precision in mine placement, greater load-carrying capacity, and the ability to covertly plant mines in close proximity to enemy positions.
- **Demining UGVs** are designed for clearing minefields. A notable example is when the 8th SOF Regiment used a UGV equipped with a mine trawl to clear a corridor between flanks, allowing an assault group to advance without casualties.[9]

FIGURE 7. UGV MISSIONS



According to the Land Forces Command, Major Volodymyr Rovenskyi, approximately 47% of UGV missions are focused on logistics and evacuation. Around 25% are dedicated to engineering tasks, and 12% to combat operations, while the remainder consists of specialized tasks such as reconnaissance, special operations, and combined missions.[10]

Source: Defense Express

Trends, challenges, and features of UGV deployment on the battlefield

UGVs are already capable of competing with other unmanned systems, particularly UAVs, in terms of **functionality**. UGVs have a much higher payload capacity, with some logistical platforms transporting 4 to 5 times the total payload of several sorties by heavy UAV bombers. They also offer greater delivery precision for minelaying and strikes, allowing the operator to visually confirm the drone's exact position before detonation. There is a documented example of a real kamikaze UGV mission where a ground drone delivered 55 kg of explosives to successfully destroy an enemy logistical bridge.

However, ground drones also face **risks** compared to UAVs, with the latter being easier to operate due to a "cleaner" environment and the military's extensive experience with aerial systems. In contrast, UGVs can get stuck, hit a mine, lose communication, or be destroyed by enemy artillery and drones. Vibrations from movement and firing loosen bolts and damage electronics.[11] After every deployment, a technical inspection is required to check and tighten connections. Heavy modules, such as automatic grenade launchers (AGLs) or large-caliber machine guns, require powerful motors, stabilization, and dampers, otherwise, the platforms "shake" excessively during fire. Many UGVs are relatively slow (6–

[9] See "Architecture of the Future Battlefield: How Ukrainian UGVs Rewrite the Limits of Human Risk", Army Inform, [ua]
[10] See "What missions do UGVs perform most often on the battlefield and what is the difficulty of using this weapon?", Defense Express [ua]
[11] See "Robots instead of infantry. Could machine gun-UGVs replace humans on the front lines?", Oboronka [ua]

10 km/h)[12], meaning they remain in the strike zone of enemy FPV drones for extended periods over long distances. As one UAV operator correctly pointed out, a robot has to "hobble" its way to the front line, and the entire time it must be protected from enemy drones, EW, and artillery.

The tactics for employing UGVs remain more complex than those for UAVs due to the architecture of communication, deployment, and coordination with infantry. While battle planning follows standard "infantry" procedures, UGVs have technical limitations that headquarters may not always account for. Therefore, it is necessary to involve UGV specialists to adjust mission objectives. The systematization of experience is currently moving from the "bottom up", at the brigade and corps levels, the varying experiences of different units make rapid unification difficult, though. Not only the tactics but also the control of UGVs is more demanding than that of UAVs, which underscores the critical need for trained operators.

As of the beginning of 2025, the average **level of UGV automation** remained low. Drones were almost always under the direct control of an operator at all stages, with automation limited to specific auxiliary functions rather than full autonomous navigation. Increasing autonomy is critically important on the battlefield to minimize the time people spend at "ground zero" while unloading UGVs from vehicles or offloading cargo at positions. These moments are the most dangerous for personnel, as they are exposed in open areas and can become targets for drones or artillery. Over the past year, the situation has not changed radically. As of early 2026, fewer than 1% of systems in real combat operations are truly autonomous.[13] Most of what is labelled "autonomous" is, in reality, not.

However, **systems with partial autonomy are evolving.** For example, some UGVs now perform automatic sector patrolling, where the turret independently scans a sector and alerts the operator to potential targets.[14] Another critical priority for UGVs currently is increasing their operational range. Due to the expansion of the "kill zone" created by UAVs and the need to move operators further back from the front line, robots now require a range of 10–15 km or more.[15] Industry specialists also identify the development of turrets capable of shooting down FPV drones and Shahed-type loitering munitions as a top priority. These turrets must detect and track targets completely autonomously using machine vision, acoustics, and thermal imagers. An example of such development is the AI-powered, autonomous Sky Sentinel turret, designed to intercept Russian Shaheds and missiles.[16]

The **issue of communication and navigation** for UGVs remains acute. At the beginning of 2025, there were already demands for increased range and communication reliability due to the "kill zone" and the high activity of both Russian and Ukrainian EW near the front lines. As of early 2026, the situation has not changed significantly. For UGVs, a multi-channel communication system with automatic channel switching (LTE, Mesh, Starlink) is now critical for countering EW and jamming. For navigation, if GPS is jammed, platforms will need to switch to inertial navigation systems, other positioning tools, motion sensors, and terrain-based orientation.

[12] See “When will drones replace humans on the battlefield in Ukraine and will it happen at all?”, BBC Ukraine [ua]
[13] See “Nearly 20 UGV models and autonomous drone swarms: how Ark Robotics takes pilots away from the front lines”, Mind [ua]
[14] See “Robots instead of infantry. Could machine gun-UGVs replace humans on the front lines?”, Oboronka [ua]
[15] See “Why will there be more different UGVS on the front and what problem do they solve?”, Defense Express [ua]
[16] See “AI-Powered Turret That Hunts Russian Missiles and Drones? Meet Sky Sentinel, Ukraine’s New Air Defense”, United24 [ua]

As of the beginning of 2026, **the scale of UGV deployment within the units of the Armed Forces of Ukraine** has grown significantly. While at the beginning of 2025, there were only a few dozen units that had conducted at least one UGV mission and fewer than 10 units that had transitioned to a systematic, established process, now 22 units[17] have dedicated UGV subunits within their structure. In January alone, over 7 000 missions[18] were carried out using UGVs, the vast majority of which involved frontline logistics.

While in 2025 most UGV usage was driven by grassroots initiatives of small groups of soldiers, often even off the books, **by early 2026, a full infrastructure and organization for UGV implementation and corresponding training are forming**. Specialized companies and strike UGV companies have already been established, such as NS-13 within the 3rd Assault Brigade and the "Alter Ego" UGV company within the 93rd Mechanized Brigade "Kholodnyi Yar", featuring full staff positions for operators, engineers, IT specialists, and more. It is already known that the Ministry of Defense has certified the first 7 private UGV operator schools[19] and has launched state-led training[20] with 4 000 military personnel currently taking courses, and 1 500 have already received their certificates.

Ukrainian forces and manufacturers must maintain and expand their advantage in the development and deployment of UGVs, as **Russia is actively developing various types of ground drones**, including the "Uran-9", "Marker", "Robot", "Shturm", and others.[21] These systems possess expanded functionality but demonstrate mixed results — low autonomy, manual control, and poor "survivability" in real combat. Many Russian UGVs are destroyed by Ukrainian FPV drones before they can even complete their missions.

Ukraine is currently clearly **ahead of the adversary** in the UGV sector due to its focus on minimizing human casualties, rapid adaptation to frontline requirements, and a large number of codified models. Meanwhile, the enemy largely copies existing technology and rapidly scales it. The Armed Forces of Ukraine operate on a fundamentally different "compass": if a vehicle can take the hit, it must. The most striking example is **Operation "HVER",** where a severely wounded soldier remained at a position for 33 days.[22] UGVs were dispatched to him seven times. Six robots were lost to mines, FPV drones, and point-blank small arms fire. The seventh, despite a damaged wheel and hull, covered 64 km, reached the position, and evacuated the wounded man, resulting in his survival. The logic here is simple: **the loss of six machines is an acceptable price for one saved life**. In contrast, the Russian approach often involves an infantryman acting as a human shield in front, followed by the UGV, with the operator behind them. In the event of an explosion or strike, the soldier typically dies while the machine remains intact.

UGVs have already ceased to be "exotic" and have become a fundamental tool, much like artillery or aerial drones. The question is no longer "whether robots are needed at the front", but how quickly they can be mass-produced, how many operators can be trained, and how they can be integrated into all levels of tactics from the squad to the corps level. UGVs are already taking on the most dangerous tasks: logistics within the "kill zone", evacuation under FPV fire, demining, holding positions, and

[17] See “What missions do UGVs perform most often on the battlefield and what is the difficulty of using this weapon?”, Defense Express [ua]
[18] See “7,000+ combat missions of ground robotic complexes per month”, Fedorov [ua]
[19] See “Architecture of the Future Battlefield: How Ukrainian UGVs Rewrite the Limits of Human Risk”, Army Inform, [ua]
[20] See “Unmanned Ground Vehicles (UGVs): when will robots replace humans?”, VGI-9, [ua]
[21] See “Unmanned Ground Vehicles (UGVs): when will robots replace humans?”, VGI-9, [ua]
[22] See “Architecture of the Future Battlefield: How Ukrainian UGVs Rewrite the Limits of Human Risk”, Army Inform, [ua]

much more. Consequently, the UGV market in Ukraine has become one of the most dynamic in the world, featuring dozens of models, thousands of missions every month, rapid scaling, and close interaction between developers and the front line.

Maritime Drones

Ukrainian maritime drones have, to a certain extent, become a substitute for a national fleet in wartime conditions. A diverse force of unmanned surface vessels (USVs), unmanned underwater vehicles (UUVs/AUVs), and semi-submerged craft has largely replaced a conventional navy and pushed Russia's so-called "Black Sea Fleet" onto the defensive. Ukraine has managed to achieve, if not strategic superiority, then at least **strategic and operational parity** with the adversary, which has lost de facto control of parts of the Black Sea, suffered many ships damaged or destroyed, and was forced to partially withdraw the Black Sea Fleet to Novorossiysk. Maritime drones have become a "long naval spear" and a potent deterrent tool.[23] Russia has now clearly realized that the Kerch Bridge and its logistics are targeted, while its aviation, air defense, and radar systems are under constant pressure.[24]

That is, the Kerch Bridge attacks in the summer of 2023 and later disrupted the primary logistics route from Russia to Crimea. The adversary was forced to reroute via the Azov coast, relying on land routes and ferries, which carry higher risks and greater exposure to attacks. Furthermore, maritime drones helped secure a "grain corridor" without Russian "agreement", restoring merchant shipping to Ukrainian ports despite threats. These drones have also successfully engaged aerial targets, shooting down helicopters and jets (Mi-8, Su-30)[25], and attacking Pantsir-S1 air defense systems in the Kherson region[26], as well as strategic radar complexes in Crimea[27]. For Ukraine, this has generated a significant **asymmetric cost advantage**. While a Neptune R-360 missile costs approximately $1.5 million, USVs cost roughly $221,000 to $250,000 per unit.[28] In contrast, the value of the targeted assets, like warships, air defense systems, and aircraft, amounts to tens or even hundreds of millions of dollars per unit. Even with a loss-to-kill ratio of approximately 10:1, USVs remain exceptionally cost-effective.[29]

Currently, the Ukrainian maritime drone sector comprises various developments with different levels of modification, functionality, and capabilities. However, the field of naval unmanned vehicles in Ukraine remains relatively narrow and less publicized. This is because each development costs more than similar land-based or aerial drone projects, creating a high barrier to entry.

Currently, the most standardized classification of maritime drones is based on their operating environment and technology:

- **Surface vehicles/drones (USVs)** operate on the water's surface and include "kamikaze" boats, multi-purpose platforms, patrol/logistics craft, and drone "motherships". Key examples include the Magura series, Sea Baby, Sea Wolf, Katran series, Barracuda series, Stalker 5.0,

[23] See "From the battlefield to the future of warfare: Harnessing Ukraine's Drone Innovations to Advance U.S. Military Capabilities", KSE Institute
[24] See "How Ukraine's Unmanned Surface Vessels Have Reshaped Modern Naval Warfare in the Black Sea", RSDI
[25] See ""Storm of the Seas and Skies": Ukrainian reconnaissance naval drones have received new combat capabilities", Krym.Realii [ua]
[26] See "Ukraine's Marauding Sea Drones Bewilder Russia", CEPA
[27] See "How Ukraine's Unmanned Surface Vessels Have Reshaped Modern Naval Warfare in the Black Sea", RSDI
[28] See "Sea drones: What are they and how much do they cost?", BBC UK
[29] See "Uncrewed Platforms Have Been Critical to Ukraine's Success in the Black Sea", RUSI

Alligator, and Aquatechnik's Dzyga and Khoriv 2.0.[30] The "kamikaze" designs were highly effective in the early stages until Russian forces adapted, necessitating further evolution. Now, these vessels can be equipped with various types of anti-air weaponry, such as R-73 (AA-11 Archer) or AIM-9 missiles, as well as machine-gun turrets for engaging helicopters and aircraft. Furthermore, they are being developed as multi-role or modular platforms capable of carrying FPV drones, loitering munitions, sea mines, rocket pods, and EW/ISR modules. Their functional scope has also expanded to include logistics support (resupply and evacuation), dynamic minelaying, and riverine operations, as well as surveillance, patrolling, and target acquisition.

- **Underwater vehicles/drones (UUVs/AUVs)** operate fully submerged at various depths (typically 1-20 meters). They face significant navigation and communication challenges. Examples include the Toloka TLK-1000 and the Marichka AUV. The former features an advertised range of 2000 km and a maximum payload of 5000 kg, whereas the latter offers approximately 1000 km of range.
- **Submerged / semi-submerged / partially submerged drones** travel just beneath the surface, often with only masts protruding for communications and sensors. They conceptually combine the stealth and low acoustic/cavitation signatures of underwater craft with the easier communication and navigation characteristics of surface vessels. An example of this category is the Toloka TLK-150 semi-submersible/loitering torpedo, designed for anti-ship and anti-infrastructure attacks, with a warhead that strikes below the waterline, significantly increasing the probability of sinking the target. However, this design involves certain trade-offs, such as lower speed and range compared to surface craft, and the need to keep the mast above water for communications and visual navigation cues.

Overall, the Ukrainian maritime drone segment and its operational employment have evolved significantly. The initial solutions in 2022 were based on surface swarms of kamikaze boats, with the core concept being cheap, explosive-filled USVs attacking ships and ports (e.g., the October 2022 Sevastopol raid).[31] These missions demonstrated that small, disposable vessels, combined with a satellite link, could penetrate heavily defended bases and damage multiple ships. In contrast, the current **focus has shifted toward multi-functional universal platforms**, with each major manufacturer offering such solutions. Examples include the Magura V6P as a multi-functional platform, the Barracuda series, featuring multiple variants including kamikaze, FPV carriers, gunboats, logistics, and extended-range versions[32], and the Navy's USVs, which serve simultaneously as ramming weapons, mine-laying platforms, and FPV "motherships".

Trends and challenges

Indeed, the Ukrainian maritime drone campaign against Russian forces and their fleet has demonstrated that these products are **versatile, scalable, and adjustable** in their deployment, evolving alongside the dynamic nature of naval warfare as vessel roles continue to expand. Missions are conducted with high cost-effectiveness, as drones are far cheaper per sortie than missiles or crewed ships, yet they can threaten the same high-value targets. They enable the destruction of targets that Ukraine would otherwise be unable to reach, or that would entail prohibitive risks for

[30] See "Overview Of Ukrainian Maritime Drones (USVs) Of The Russo-Ukrainian War", H. I. Sutton
[31] See "How Ukraine's Unmanned Surface Vessels Have Reshaped Modern Naval Warfare in the Black Sea", RSDI
[32] See "9 new types of Barracuda naval drones have appeared in Ukraine, from ATGM carriers to kamikazes with 1-ton warheads", Defense Express [ua]

mission personnel.[33] Their operational reach provides Ukraine with significant advantages across the open sea, littorals, rivers, and inland waterways.[34] Furthermore, maritime drones have proven their stealth and resilience due to their small signature, as well as being exceptionally hard to detect on radar and difficult to engage with traditional anti-ship missiles or torpedoes.

However, maritime drones are not perfect products and possess **limitations** that could impact future operations. Currently, Ukrainian drones largely target ageing Soviet-era objects, ships, and platforms. Consequently, critics suggest that the results of attacks against modern fleets with better sensors and layered defenses might differ significantly. The majority of successful Ukrainian maritime drone strikes have indeed been carried out against Soviet-legacy Russian warships. Furthermore, alongside many successful missions, there are also those that failed or ended in drones being destroyed or washing ashore after a loss of contact. Russian forces are gradually adapting by improving early detection via helicopters and fast boats, deploying multi-layer defenses and barricades in ports, and implementing electronic warfare and interceptor drones. While maritime drones are relatively cheap compared to ships, for Ukraine, they remain finite and costly assets. Each USV still costs about $220,000 (excluding missile payloads), and funding, including crowdfunding, cannot expand infinitely.[35]

Ultimately, every technology and innovation eventually encounters **technical challenges** and obstacles within the operational environment. One such hurdle Ukrainian manufacturers have yet to overcome is underwater navigation and sensing, which is significantly more difficult than in the air due to currents, shifting seabeds, salinity, turbidity, and changing water properties. High-grade underwater navigation systems, particularly inertial navigation systems, are relatively expensive, sometimes costing hundreds of thousands of dollars per unit. Similarly, underwater detection systems, such as sonar and hydroacoustic networks, are incredibly important for effective naval warfare but are very costly and slow to develop. Underwater communication remains another critical challenge — it is essential both for controlling individual drones during missions and for swarm coordination between multiple maritime platforms. However, this technology is complex, expensive, and almost entirely dependent on imports.

Ukrainian experts stress that the war is "going deep underwater" and that **underwater technology must become a strategic investment priority**. Although Ukraine has achieved parity, or even superiority, over Russia in the surface vessel domain, the adversary retains a significant advantage in the underwater realm. This is due to their possession of submarines, fixed underwater detection infrastructure, underwater radar and acoustic surveillance systems, and a more integrated use of space-based assets. Although Ukraine already possesses certain innovations, such as the previously mentioned Toloka TLK-150/1000 and Marichka AUV semi-submersible/underwater attack drones, underwater technology remains exceptionally capital-intensive and time-consuming. Therefore, Ukraine's primary objective in the maritime drone sector remains clear: continued innovation is essential to maintain a long-term strategic advantage.

It is crucial to ensure sufficient R&D funding for manufacturers, especially considering that private investment tends to arrive in waves following headline-grabbing successful operations. Within the sector, a significant dependency on Asian, particularly Chinese, components persists, including

[33] See "Uncrewed Platforms Have Been Critical to Ukraine's Success in the Black Sea", RUSI
[34] See "After hammering Russian ships on the open ocean, Ukraine's drone boats appear to be taking the fight into new waters", Business Insider
[35] See "How Ukraine's Unmanned Surface Vessels Have Reshaped Modern Naval Warfare in the Black Sea", RSDI

microelectronics, cameras, lidars, radars, and electric motors. While a certain level of localization is already present in the Ukrainian defense market, it demands substantial up-front investment and pays off only at scale. At the same time, it is necessary to pursue further integration with other domains, as maritime drones increasingly operate as part of multi-domain complexes (e.g., USVs integrated with UAVs, or USVs acting as launch platforms for FPV drones against land targets). In the post-war era, these battle-proven maritime drones are expected to be in high demand, as Ukraine prepares to export both these systems and its unique operational know-how.

Electronic Warfare

The Ukrainian Electronic Warfare (EW) and frontline communications sector is the least discussed in the informational space compared to UAVs, UGVs, or missiles. However, it is precisely the EW and communication tools that enable the execution of combat missions and the preservation of human life.

When people refer to EW assets, they typically mean **electronic attack (jamming) systems**. However, such a generalization is misleading, as electronic warfare is an umbrella term. Beyond electronic attack, it also encompasses **electronic support (reconnaissance/SIGINT)** and **electronic protection systems**.

Overall, EW is a set of technologies and actions aimed at detecting, disrupting, degrading or deceiving enemy electronic systems (communications, navigation, control, radars, UAV links) by using electromagnetic energy. In simple terms, it is warfare with radio waves instead of bullets: you do not destroy the device physically, you make it "deaf", "blind", or misled so it cannot perform its mission.[36] Because current frontline dynamics critically depend on radios, drones, GPS and data networks, the side that better controls the electromagnetic spectrum often gets a decisive advantage in coordination, survivability and situational awareness.

Analyzing the sector, the core operational and tactical tasks of various Ukrainian EW systems include:

- **Suppression** to generate powerful interference so that receivers (drones, radios, GPS modules) cannot properly receive legitimate signals, as well as to cut off links "drone-operator", "drone-satellite", "unit-HQ", etc.
- **Deception** to transmit false information that looks like real: fake GPS coordinates, fake radar echoes, fake protocol packets. Along with that, to redirect munitions to false targets or make drones fly off-course or endlessly "search" those wrong targets.
- **Protection** to shield own command posts, columns, bases, depots and positions with "domes" or sectors of jamming so enemy drones and guided munitions lose effectiveness.
- **Masking and concealment** to suppress or spoof enemy reconnaissance and surveillance systems so they see a false or incomplete picture of the forces (false emissions, masking real ones, etc.).

Often, a single system can perform several of these roles simultaneously, especially when integrated with electronic support for reconnaissance and automated control.[37]

[36] See "What is EW: In simple words about electronic warfare", Drony.Ukraine [ua]
[37] See "How does electronic reconnaissance work?", Bezpeka.Club [ua]

Furthermore, EW systems are broadly classified by purpose, functionality, operational range, mobility, and other factors.

Foremost, EW systems differ in their **main functions:**

- **Radio-electronic suppression (jamming)** activates systems that generate interference and jam communications, navigation, and UAV control channels.
- **Radio-electronic reconnaissance** includes systems that detect, intercept and analyze enemy emissions to provide intelligence and targeting for suppression systems and fire assets.
- **Radio-electronic protection** is understood as measures and devices to harden own systems against enemy EW (resilient radios, anti-jam GPS, filtering, frequency agility, protected links).[38]

These three often exist in integrated complexes, where the same platform both listens (reconnaissance), decides and jams (suppression), while also protecting its own communications.

EW systems are also classified by their operational range, although experts often cite varying figures regarding these distances.

- **Sub-tactical or personal** systems to protect one soldier or a small team with a range roughly up to 50 meters. Those can be constructed as car-roof or "backpack" systems, personal anti-FPV "bubbles".[39] Kvertus company has developed the AD COUNTER FPV BACKPACK F2 M50, designed to protect small units on the move against FPV drones by creating a local "interference dome" around the unit.[40] Kvertus is highlighted as one of the Ukrainian leaders in EW suppression and reconnaissance systems, focusing on "smart EW" concepts. In their systems, the architecture consists of software logic, including signal analysis, modulation, suppression algorithms, and digital filtering.
- **Trench or close-range** systems with a range of 100-500 meters. Some sources generalize "close" as up to 10 km, but the actual effective radius for FPV is typically hundreds of meters to a few kilometers. Those are used to protect positions, vehicles, and local sectors, usually static or semi-static.[41] A prime example is the KRAKEN-M, a multi-band, combined-defense EW system that acts as a "fixed shield" against UAVs, disrupting control and telemetry channels before they reach the protected object.
- **Tactical** devices with a range up to about 50 km to protect frontline groupings, brigade-level areas, and suppress UAVs and communications in a larger sector.[42]
- **Operational-tactical or operational-strategic** systems with a range from tens to hundreds of kilometers (up to approximately 500 km for the most powerful). Those are usually mounted on large vehicles and can suppress aviation communication, satellite links, and regional networks.[43]

[38] See "Military electronic warfare and electronic reconnaissance systems: operating principles, classification and combat capabilities", Drongrif [ua]
[39] See ""Sometimes more is expected from electronic warfare than it can do." How electronic warfare works against FPV and Shaheds", DOU [ua]
[40] See "Electronic warfare in war: types, role and best systems of 2025", Bezpeka Veritas [ua]
[41] See "Electronic warfare: essence and principles of operation", Drongrif [ua]
[42] See "What are electronic warfare (EW) systems?", KOLO Ukraine [ua]
[43] See "What is an electronic warfare system and why are electronic warfare assets critically important for the Armed Forces of Ukraine?", Marketnet [ua]

- **Strategic** systems with the regional coverage and with emissions visible even from satellites, very powerful and rare though.[44]

Further classifications overlap with the previously mentioned types and can be found across various system classes. For instance, based on the **mobility factor**, EW assets are also divided into: **portable** (carried by a soldier as a "backpack EW" or a small personal jammer); **static** (installed at long-term positions such as trenches, checkpoints, or strongpoints); **vehicular/mobile** (mounted on pickups or armored vehicles); and **fixed/stationary** (large multi-antenna complexes for the protection of strategic infrastructure, often integrated with air defense).[45] The same systems also varied by **radiation pattern**, with **dome** EW systems creating a semi-spherical or circular protective field of 360° around themselves, usually with a radius of 500–1000 meters — it is Ideal for protecting static positions, vehicle parks, field HQs. Meanwhile, **directional** devices generate energy focused into a beam and are used for targeted jamming at longer distances (hundreds of meters to kilometers). Those include anti-drone rifles and directional vehicle antennas. Both systems have their **drawbacks**: the former are easy for the enemy to detect, since no cell or GPS works in the area, and can interfere with their own drones and communications. The latter have a narrow operational range, and it is harder for them to catch highly maneuverable drones without good cueing and aiming.[46] An example of a mobile dome EW system is the REB-OX developed by Rebel Group.[47] Their systems are mounted on vehicles to serve as the first echelon of protection for moving units and convoys. They create a protective zone around the vehicle, suppressing the control and navigation signals of enemy drones attempting to attack the convoy or accompanying troops. These systems are available in several versions with different operating frequency bands, allowing for adaptation to specific frontline sectors and varying threat sets.

Despite many variations, all EW devices follow a common logical process and **functional loop.**[48] Foremost, they conduct radio monitoring and detection of active signals, including drone control links, video links, GPS, LTE, Wi-Fi, radios, and radars. The next step is to analyze and classify a signal type, determining its parameters such as frequency, bandwidth, modulation, power, and others. Systems choose the jamming type based on the target and generate interference, transmitting powerful noise or structured signals to make the legitimate signal unusable. Finally, systems monitor how the target's signal behaves, whether its power drops, does the enemy changes frequency. As mentioned above, **smart complexes** tightly integrate EW reconnaissance and suppression systems, thereby fusing detection and jamming within a single software-defined architecture.

EW jamming and reconnaissance

"EW jamming without EW reconnaissance is profanation".[49] Since the enemy frequently changes frequencies and protocols, effective EW requires up-to-date knowledge of which signals to jam and where to jam them. Hence, the suppression devices are most efficient in the link with reconnaissance systems.

---

[44] See ""Sometimes more is expected from electronic warfare than it can do." How electronic warfare works against FPV and Shaheds", DOU [ua]
[45] See "What is EW?", BlueBird Tech [ua]
[46] See "What are electronic warfare (EW) systems and how do they work?", Drone State [ua]
[47] See "Conductor of the Invisible Battle: Rebel Group Brings Its Electronic Warfare Fighters Out of the Shadows", Defense Express [ua]
[48] See "What is an electronic warfare system and why are electronic warfare assets critically important for the Armed Forces of Ukraine?", Marketnet [ua]
[49] See ""Sometimes more is expected from electronic warfare than it can do." How electronic warfare works against FPV and Shaheds", DOU [ua]

When discussing electronic reconnaissance, specialists identify it as a set of methods and systems for the passive interception, analysis, and localization of enemy electromagnetic emissions. It is always "passive", because it does not emit, and it just listens, providing intelligence about enemy communications, drones, radars, navigation and control systems.[50]

The main tasks are:

- **Detecting** and identifying types of radios, radars, UAV control links, navigation and targeting systems.
- **Determining** precise positions of emitting objects like radio stations, command posts, UAV operators, radars.
- **Intercepting** and sometimes decrypting communications.
- **Monitoring** activity patterns to infer enemy plans and movements.
- **Providing** data to the EW suppression system, artillery, aviation, cyber units for further action.

Those systems can provide long-range information gathering without entering enemy territory and real-time threat detection, for instance, of FPV launches. They are difficult to detect because reconnaissance systems do not emit. However, it is still vulnerable to enemy EW, noise, and complex emission environments where many sources are close together. They are also high-cost and require highly skilled operators.[51]

Expert teams unanimously agree that electronic suppression and reconnaissance must work together as a "shield and sword". To ensure that defense and combat missions remain effective, they emphasize a **layered EW deployment** that extends from the forward line to the rear. For example, tactical and trench reconnaissance systems detect drones and communications, providing early warning. This data then feeds into EW systems, which select the appropriate jamming bands and intensities. Consequently, personnel on the front lines utilize personal or backpack EW ↣ trench dome jammers shield positions from FPVs ↣ while more powerful directional and vehicular EW systems are positioned further back to counter high-altitude or distant drones and communications. This layering can culminate in operational/strategic complexes that affect wider enemy infrastructure.[52]

Moreover, "one EW device is not a magic pill".[53] It is crucial to build **complexes** tailored to specific threats and tasks. This requires an understanding of several factors: from the core mission of the EW asset and the specific objects to be protected, to the types of drones and threats operating in the area and the specific frequencies they typically use.

The operation of EW must be meticulously **planned and coordinated**. If trench-level EW is left on permanently at full power, it can "blind" nearby reconnaissance systems, preventing them from detecting incoming drones. Moreover, uncoordinated dome EW can interfere with one's own UAV operations and communications. Therefore, to avoid "friendly fire" in the spectrum, reconnaissance systems must constantly update EW teams with real-time frequency data and threat intelligence.[54]

[50] See "Radio-electronic reconnaissance (RER): essence and principles of operation", Drongrif [ua]
[51] See "How does electronic reconnaissance work?", Bezpeka.Club [ua]
[52] See "Military electronic warfare and electronic reconnaissance systems: operating principles, classification and combat capabilities", Drongrif [ua]
[53] See "What are electronic warfare (EW) systems?", KOLO Ukraine [ua]
[54] See ""Sometimes more is expected from electronic warfare than it can do." How electronic warfare works against FPV and Shaheds", DOU [ua]

Rebel Group designs EW jamming and reconnaissance systems so they can function both as independent modules and as components of integrated multi-level defense systems. As mentioned above, the mobile REB-OX can be used as the first echelon, covering moving units, while stationary and high-power systems like FARA (possibly SDR SHTORA too) can protect objects and larger areas. At the same time, their SCAN-OX system provides continuous situational awareness and targeting.[55]

Challenges within the sector and obstacles on the battlefield

EW brings numerous advantages to the battlefield, including the capability to disorient Russian forces by jamming communications, suppressing UAV control links, and even knocking missiles off course. However, operational realities also reveal certain limitations of such systems.

Military personnel highlight both **technical limitations and challenges** in the employment of these systems by Ukrainian forces. High power consumption is a significant factor — it limits the duration of high-power operations in field conditions and necessitates additional energy resources, such as generators and high-capacity batteries.[56] Furthermore, the requirements for active cooling systems, high-quality antennas, and powerful transmitters increase the equipment's overall weight, size, and energy footprint. EW systems also face difficulties when operating in complex terrain or under the influence of external factors.[57] Forests, buildings, mountains, and other natural or man-made obstacles significantly reduce EW's operational range, thereby decreasing its effectiveness in urban or mountainous areas. Additionally, weather conditions, such as rain or fog, affect radio wave propagation, further decreasing the range and intensity of the jamming interference.

Proper utilization of EW systems and complexes remains a significant challenge. Without correct configuration or coordination, EW can suppress not only enemy assets but also friendly drones, air defense systems, and unit radio communications. In 2023, up to 50% of Ukrainian drones were lost due to "friendly fire". This highlights a further issue: interference between different modular EW systems. Since multiple EW assets (mobile, stationary, etc.) are often deployed simultaneously on the battlefield, their signals can overlap, leading to "clashing" and reduced effectiveness. Addressing this requires centralized control, synchronized frequency plans, and the use of software-defined radio (SDR) for dynamic coordination. Furthermore, **integrating EW reconnaissance and jamming** is inherently complex.[58] Without a constant data stream from reconnaissance systems, such as scanning, geolocation, and spectral analysis, EW operates "blind", reducing precision and increasing the risk of accidental jamming. The battlefield demands experienced operators capable of rapid spectral analysis and parameter setting. Operators must possess a background in radio engineering, understand protocols, and constantly update their skills, otherwise, the system will be utilized inefficiently.[59]

Ukrainian EW manufacturers face numerous challenges due to the ongoing **technical arms race with Russia.**[60] The adversary constantly introduces new drone types and communication protocols. To maintain an advantage, Ukrainian developers must design and deploy new solutions within a short time period. For instance, after drones were detected operating in the 500-600 MHz range, new jamming assets appeared at the front within 2-3 months. Furthermore, Russians not only experiment with different bands but can also hop between frequencies during a mission, complicating static

[55] See "Conductor of the Invisible Battle: Rebel Group Brings Its Electronic Warfare Fighters Out of the Shadows", Defense Express [ua]
[56] See "What is EW: In simple words about electronic warfare", Drony.Ukraine [ua]
[57] See "Electronic warfare: essence and principles of operation", Drongrif [ua]
[58] See "What are electronic warfare (EW) systems?", KOLO Ukraine [ua]
[59] See "What is EW: In simple words about electronic warfare", Drony.Ukraine [ua]
[60] See "EW: The shield of the modern battlefield — how electronic warfare works", Murder [ua]

jamming. This forces Ukrainian manufacturers to develop EW devices with new modulations, specialized antennas, wider suppression ranges, and dynamic adaptation algorithms. Enemy innovations in the UAV sector present a separate set of problems.[61] Like Ukrainian units, the Russians employ drones equipped with machine vision, capable of autonomously detecting targets at a range of 300–500 meters. This leaves an extremely narrow window for jamming. Moreover, approximately 15% of enemy drones now utilize fiber-optic video links, which are immune to radio-frequency jamming and cannot even be detected by electronic reconnaissance. Currently, the only practical solution is the physical destruction of such drones (e.g., using shotguns or net guns). EW systems are also limited in their defense against Shahed-type drones and other long-range UAVs. Long-range drones with multi-layered navigation systems require a comprehensive approach involving EW, air defense, interceptor drones, and other kinetic systems. In Shaheds, 16 simultaneous navigation channels are used, rendering traditional GPS spoofing ineffective. Consequently, EW often only reduces accuracy rather than neutralizing the target. Additionally, Russian units are testing mesh networks, which allow real-time command relay between drones, creating a swarm effect. As a result, Ukrainian EW must be adaptive and "smart", significantly complicating both development and operation.

The EW market in Ukraine faces issues of **low quality and the proliferation of "cheap" systems**. Some suppliers sell equipment assembled with inexpensive Chinese electronics that fail to meet declared technical specifications and do not perform in field conditions. Testing grounds have shown that such systems are unable to suppress even basic FPV drones, and their use results in wasted time on repairs and modifications. On the other hand, complex systems, particularly strategic and operational-tactical complexes, carry a high price tag, which limits their large-scale deployment. These systems require regular technical maintenance and the replacement of components that are often imported. Consequently, this reliance on imported parts, combined with supply chain delays and high costs, complicates the task of mass equipping military units.[62]

Innovations

Some EW manufacturers are shifting from simple broadband noise jammers to **software-defined, algorithm-heavy systems**. In many current systems, 60–80% of the capability is software logic: signal analysis, modulation, suppression algorithms, frequency databases, and digital filtering. IT engineers now design algorithms that recognize signal types and protocols, filter out noise, analyze the spectrum in real time, and detect drones earlier than a human operator could. This is what companies call "smart EW": instead of blindly jamming, the system detects, classifies, and then applies the most effective suppression mode for that specific signal.[63]

Another interesting innovation is the **"Mirage" technology**, which operates over a radius of about 800 meters and combines detection and suppression into a single system. Drones appear on EW operators' displays ↠ the operator can select a drone and press a button to focus jamming on that specific threat ↠ "Mirage" effectively manages a network of EW nodes, coordinating them against multiple targets. This is a move away from "always-on noise" and toward selective, operator-controlled EW fire, almost like air defense, but with radio waves.[64]

[61] See ""Sometimes more is expected from electronic warfare than it can do." How electronic warfare works against FPV and Shaheds", DOU [ua]
[62] See "What are electronic warfare (EW) systems and how do they work?", Drone State [ua]
[63] See ""Sometimes more is expected from electronic warfare than it can do." How electronic warfare works against FPV and Shaheds", DOU [ua]
[64] See "What are electronic warfare (EW) systems and how do they work?", Drone State [ua]

Artificial intelligence is being actively explored, but in a limited, safety-conscious way. It is used to detect and classify signals, determine drone frequency, protocol, polarization, and the optimal jamming method, thereby reducing false alarms in drone detection and spectrum monitoring. Experts stress that AI should prepare EW (choose modes, propose actions), but not make the final decision to jam, as the operator must authorize suppression to avoid jamming friendly drones and comms.

Ukraine's EW sector is featuring **organizational innovations** that directly impact how fast the technology evolves. The state cannot fully cover the demand, so dozens of private startups and volunteer teams are building jammers, drone detectors, and signal-analysis systems. These small teams can quickly change designs, test in combat, and ship small batches, reacting faster than big defense plants.

Artificial Intelligence

Since the start of the full-scale invasion, Ukraine has been actively integrating artificial intelligence (AI) into its defense complex and military strategy. In a broad sense, AI is a technology designed to emulate human intelligence, capable of learning, adapting, and making decisions.[65] Various types of AI are built upon neural networks, computer vision, machine learning, natural language processing, and automated decision-making. Consequently, this enables AI to process, analyze, and evaluate vast volumes of data, identify patterns, and generate forecasts.

In the Ukrainian AI-driven defense sector, the main efforts are focused on **operational and mission-support AI**[66] solutions that improve command and control during active combat operations and enhance autonomous weapon capabilities. AI-driven investments are directed toward the development of fire control systems, autonomous drones and other combat platforms, reconnaissance and surveillance systems, and predictive analytics. As of March 2024, **more than 10% of venture capital** invested in the defense sector was channeled toward AI companies.[67]

However, it is vital not to fall into the trap of delusion that current battlefield dynamics and experience are primarily driven by AI technologies. Ukrainian forces are rapidly integrating such solutions to preserve human resources, enhance operational efficiency, and mitigate cognitive load. Yet fully autonomous AI systems capable of operating in unpredictable environments with minimal or no human intervention have not yet been fully developed or integrated. Consequently, confusion often arises between unmanned and autonomous technologies, where the latter is understood as pre-programmed automation rather than complex, independent decision-making.[68] Thus, AI currently operates within a human-in-the-loop decision-making process — not replacing humans, but rather augmenting them to boost efficiency, accuracy, and speed.

The primary AI tasks in the Ukrainian defense sector can be categorized as follows, though this list is not exhaustive:

- **enhancing** situational awareness and command and control on the battlefield, aiding in decision-making

[65] See "Smarter Wars: Ukraine's Use of AI and Drones in the Fight for Survival", VGI-9
[66] See ""Technology will win the war." How will artificial intelligence help win the war with Russia?", Ukrainska Pravda [ua]
[67] See "Mapping the use of artificial intelligence in priority sectors and the competitiveness of Ukraine", UNIDO
[68] See "Military AI: Lessons from Ukraine", Tech Policy Press

- **increasing** the accuracy of target identification and strike precision[69]
- **supporting** autonomous navigation and counteracting Russian EW systems.
- **enabling** the analysis of massive datasets, such as processing thousands of satellite images, photos, and drone video feeds
- **helping** to predict potential enemy movements
- **assisting** with logistics and operational planning[70]
- **minimizing** personnel losses, including through the evacuation of wounded soldiers under fire[71]
- **detecting** attacks not only on the battlefield but also in cyberspace
- **helping** to protect infrastructure facilities in real-time
- **improving** demining capabilities
- **creating** opportunities for military personnel to train using realistic combat scenarios.

Currently, within the Ukrainian defense landscape, there is a visible effort to institutionalize innovative military developments, specifically those involving AI. Key roles are played by actors such as the Ministry of Defense and the Ministry of Digital Transformation, as well as initiatives such as Brave1, the Army of Drones and others. These entities facilitate AI research and solutions, serving as a platform for a collaborative chain between military end-users and defense startups or firms. The government's primary legislative strategy[72] is the deregulation of AI products within the defense sector, aimed at streamlining bureaucratic processes and promoting rapid innovation.[73] This, in turn, fosters an environment for prompt response, testing, and modification of developments based on frontline needs. However, observers note that the defense AI solutions sector remains largely **reactive and ad hoc**, underscoring the need for a more long-term strategic vision to build a sustainable AI ecosystem, collaborating with allies. Still, the AI domain, like many other sectors of Ukraine's defense market, remains decentralized, with bottom-up or even networked development rather than a top-down framework.

Ukraine's defense AI-powered solutions

Ukraine's AI-powered solutions are located at the intersection of other innovative technologies, including autonomous, situational awareness, and intelligence systems. Hence, it is challenging to pinpoint particular, solely AI-focused actors and institutions within its ecosystem that transcend other sectors, raising the issue of horizontal integration and compatibility between hardware and software. Therefore, many hardware producers strive to develop their own software solutions for their systems. Given such a tangled environment, the following sections aim to break down AI solutions by functionality.

Autonomous combat systems and automatic target recognition (ATR)

Modern combat is being reshaped by autonomous systems, including a diverse array of AI-powered drones, naval surface vessels, unmanned ground vehicles (UGVs), and advanced combat modules.[74] By

[69] See "Smarter Wars: Ukraine's Use of AI and Drones in the Fight for Survival", VGI-9
[70] See "Artificial Intelligence on the Battlefield. Smart Weapons Review: Ukraine, Israel, USA, Australia", BBC Ukraine [ua]
[71] See "Artificial Intelligence (AI) Drones in Russia's War Against Ukraine. Is Europe Falling Behind?", Radio Liberty Ukraine [ua]
[72] See "Strategy for the development of artificial intelligence in Ukraine for 2022-2030 (working version)", Institute of Artificial Intelligence Problems of the Ministry of Education and Science [ua]
[73] See "White Paper on AI Regulation in Ukraine: Vision of the Ministry of Digital Transformation", Ministry of Digital Transformation [ua]
[74] See "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare", CSIS

integrating these technologies, military forces can significantly reduce the necessity for direct human involvement during high-risk surveillance, reconnaissance, and strike missions.

At the heart of these autonomous platforms are **Automatic Target Recognition (ATR)** systems powered by computer vision. Designed to minimize human error and enhance precision, ATR onboard various systems improves target locking and enables the identification of sophisticated enemy camouflage and decoys. By filtering out deceptions, these AI-powered tools substantially increase the probability of mission success.

The operational core of AI-powered technology follows a three-step process:

- **Detection:** scanning a designated area to locate potential points of interest.
- **Classification:** categorizing the detected object, such as distinguishing between a person, a vehicle, or hardware.
- **Tracking:** maintaining a lock on the identified target and providing real-time updates on its position.

Furthermore, these systems are able to prioritize and lock onto multiple targets simultaneously, adjusting their focus based on the specific threat level or mission objectives.

Beyond direct engagement, this technology is particularly efficient for reconnaissance drones.[75] These assets can now generate real-time 3D terrain maps, which serve as a foundation for broader operations. These maps are used to guide FPV and strike drones, providing personnel with detailed intelligence on enemy fortifications, concealed positions, minefields, and battlefield changes. Together, these capabilities form an ongoing loop of intelligence and action. The implementation of this practice is the **SAKER technology**, which combines the SAKER SCOUT drone with software built on AI algorithms.[76] Utilizing advanced optics, the system independently recognizes and records the coordinates of enemy equipment, even when camouflaged, immediately transmitting this data to the command post for appropriate decision-making.

At the same time, the market for ATR modules has matured, and a transition toward more sophisticated solutions is already underway. The new priority is ATR with classification, where the system can identify and prioritize a specific target rather than simply homing in on a "point". The **"Agent 001" module** from the startup Sky Spy can detect, classify, and localize radio emitters in real time, providing immediate visual confirmation via its onboard camera.[77] At the same time, first-generation modules often lose a target (such as a vehicle) if it moves behind an obstacle, treating it as a new object upon reappearance. In contrast, more intelligent systems can maintain object persistence, identifying it as the same target even after temporary occlusion.

However, it is worth noting that most automated or unmanned vehicles currently rely on algorithmic logic. This trend highlights the **primary complexity of AI integration:** while AI excels at focused, precision tasks, it often falters when managing complex, end-to-end processes. To address this, workflows are implemented algorithmically, with AI integrated as a "sandwich" between these algorithmic steps. In this architecture, AI handles specific, high-intent tasks (such as target recognition or optical navigation), while the algorithmic layers "validate" and verify the AI model's

[75] See "Smarter Wars: Ukraine's Use of AI and Drones in the Fight for Survival", VGI-9
[76] See "The Ministry of Defense has approved the SAKER SCOUT drone with artificial intelligence for operation in the Armed Forces of Ukraine", Ministry of Defense of Ukraine [ua]
[77] See "Top 10 Ukrainian miltech startups that attracted the most investments in 2025", Dev [ua]

output before passing it further for processing or execution. Still, while the use of neural networks for direct control remains less explored, it holds significant transformative potential.

LLMs and Analytical system AI

The integration of Large Language Models (LLMs) and analytical AI systems has expanded **the processing of multi-source intelligence**. These systems are capable of simultaneous multi-source data analysis, ingested from satellite imagery, reconnaissance drone footage, stationary cameras, acoustic sensors, radar intelligence, and intercepted communications.[78] By processing vast amounts of adversary publications, including intercepted text messages and videos, this AI can identify likely enemy objects and pinpoint the potential locations of adversary weapon systems and troop concentrations.[79] The Ukrainian defense innovation market offers a wide range of such systems: from the **Avengers platform**, which identifies and classifies 70% of enemy vehicles and equipment in drone and surveillance video[80], and **Satim AI**, which identifies ship classes in radar satellite imagery unaffected by camouflage[81], to the **Primer system**, which uses AI to analyze intercepted enemy communications.[82]

Beyond identification, these analytical models provide advanced threat identification and predictive analytics, offering actionable recommendations. This functionality is centralized within **Decision Support Systems (DSS)**, which enhance battlefield situational awareness by providing a reliable, up-to-date picture of the entire theatre of operations as well as specific localized engagements.[83] The most prominent example is the **Delta** combat digital situational awareness ecosystem, which enables real-time battlefield visualization, operational planning, and seamless information sharing.[84] Furthermore, the system enables automated detection of enemy equipment in an online environment.

In the context of intelligence and surveillance, these AI models address several challenges simultaneously:[85]

- **Optimization**: they streamline the processing of massive data sets, augmenting limited human cognitive capacity and significantly reducing the risk of analytical error.
- **Velocity**: they exponentially increase the speed of data processing and information transfer, enabling the rapid response times essential for swift mission execution.
- **Integration**: these systems process and integrate multimodal data from diverse sources in real-time, synthesizing fragmented information into a single, comprehensive operational picture.

AI is rapidly evolving in the field of open-source intelligence (OSINT), where the vast majority of data from social media and other public platforms is essentially "noise". Therefore, the primary task of AI is to extract the signal from the noise, systematize the relevant information, and present it to the commander to facilitate informed decision-making.

[78] See "Use of artificial intelligence in the defense sphere", Vernadskyi TNU, [ua]
[79] See "How Ukraine is using AI to fight Russia", The Economist
[80] See "Ukraine's Defence Tech Ecosystem: Real-Time Coordination and AI Targeting in Action", Digital State
[81] See "New Technology Sees Through Russian Attempt to Hide Ships from Ukraine", Naval News
[82] See "As Russia Plots Its Next Move, an AI Listens to the Chatter", Wired
[83] See "How artificial intelligence is being integrated into the military sphere: models, prospects, challenges", Espreso [ua]
[84] See "Technological advantage on the battlefield: Ukraine officially introduces DELTA system with AI elements", Army Inform [ua]
[85] See "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare", CSIS

One of the most acute limitations is that leading LLMs and analytical AI struggle significantly with geospatial data. Since a commander's primary tool is the map, LLMs currently lack the capability to "think" in geospatial terms. Due to their non-deterministic (probabilistic) nature, if asked, for instance, to "show all tanks within a 10km radius", an AI might yield inconsistent results rather than precise, reliable coordinates.

Autonomous navigation

Autonomous navigation and **terminal guidance** (often referred to as "last-mile navigation") serve as the critical mechanisms that direct a drone during its final approach to a target, functioning entirely independent of the operator.[86] Once a target has been identified, either by a human operator or an ATR system, autonomous navigation takes over the guidance and trajectory-planning phase. For the final strike or landing, the system relies on onboard sensors and visual odometry. These mechanisms are currently available as modular systems, enabling integration with a wide variety of platforms.

The primary advantage of autonomous navigation is its ability to enable **accurate positioning without GPS**, which is vital in environments dominated by Electronic Warfare (EW). AI-powered technologies like **Bavovna AI**[87], **Skynode**[88], **Vermeer**[89], **VGI-9**[90] and other systems can identify and make real-time flight-path decisions without operator involvement, avoiding obstacles — the drone with these systems onboard remains effective even when satellite signals are jammed.

Furthermore, this technology is crucial for maintaining flight stability. It allows the drone to constantly assess its position and maintain a steady course even if the command link degrades or is lost entirely. Ultimately, these advancements in onboard intelligence and independent positioning serve as the foundational technology that **enables drone swarming techniques,** where multiple units must coordinate their movements autonomously in a shared battlespace.

Currently, much of the focus has shifted toward **autonomous systems for air defense.** Significant development is underway in AI-powered terminal guidance for intercepting aerial targets, such as Shahed-type and other enemy drones. The ultimate goal is to achieve a fully autonomous mode for interceptors, covering everything from takeoff to the successful engagement and neutralization of the aerial target. The most prominent initiative currently is the **Brave1 Dataroom**, supported by the Ministry of Defense, the Armed Forces of Ukraine, the Research Institute of Military Intelligence, and the US company Palantir.[91] The Dataroom will provide a secure environment for testing and training AI models specifically designed to detect and intercept hostile UAVs. It already features extensive visual and thermal datasets of aerial targets, including Shahed-type drones, with plans to further expand the scope of available data.

As mentioned before, there are significant challenges in the **hardware-software and horizontal technological integration**. A sophisticated terminal guidance system (software) may be designed for a specific camera or compute module, while the drone manufacturer (hardware) utilizes different components. This integration process is far from "plug-and-play". It often requires reassembling and re-integrating components, which substantially increases development time. One of the main

[86] See "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare", CSIS
[87] See "Hybrid AI-Powered Navigation for Uncrewed Vehicles", Bavovna AI
[88] See "How Ukraine Is Using AI Drones to Outsmart Russia on the Battlefield", United24
[89] See "Vermeer, the US-Ukrainian Startup Making Drones Immune to Russian EW, Lands $10M from Draper Associates", Tech Ukraine
[90] See "Optical Terminal Guidance System", VGI-9 [ua]
[91] See "Launching Brave1 Dataroom", Brave1 [ua]

developers' solutions is to manufacture the system with AI software already integrated. One example is Buntar, whose publicly described architecture combines the airframe with proprietary mission-planning and control software and an AI-based navigation module tailored to the platform, illustrating that in practice such solutions are often developed as integrated systems rather than simple plug-and-play software add-ons.[92]

Other domains

Beyond direct combat and reconnaissance, AI is significantly transforming logistics and cybersecurity.

In **logistics**, predictive AI assists with the entire supply chain: modelling complex delivery logistics, optimizing supply routes. These systems also enable maintenance planning and the precise management of fuel and ammunition stocks. The ability of AI to provide accurate demand forecasting ensures that resources are positioned where they are needed most, reducing waste and increasing the sustainability of long-term operations.[93]

Simultaneously, AI has become indispensable in **cybersecurity**, serving as a shield for critical infrastructure. AI-driven systems are designed to detect, analyze, and neutralize not only established threats but also emerging ones. By providing this automated, real-time response capability, AI adds an additional layer of protection to command and control (C2) systems and defense communication channels.[94]

Trends

The AI industry operates within a **rapid development-to-deployment cycle**, linking government and military efforts to engage developers and create leading-edge solutions.[95] This allows the sector to leverage civilian expertise for military applications, as seen in the notable operational shift from the civilian to the defense sector. A pivotal element of this ecosystem is the real-time combat testing of technologies rather than in controlled environments, enabling immediate feedback for continuous improvement.

It is evident that the AI ecosystem is still an emerging sector within the Ukrainian defense industry — it is in the early stages of development and is actively engaging in establishing international cooperation and **financing infrastructure**. Based on the number of venture capital funding rounds, patents, and publications, the Ukrainian defense sector combines high global competitiveness with a deep level of AI penetration.[96] Consequently, Ukraine holds some of the strongest prospects for leadership, offering broad economic opportunities featuring high profitability and low risk. Moreover, **sector-wide trends** indicate that foreign investors, particularly from the EU, prefer joint ventures and minority stakes to full acquisitions. For them, this represents a lower-risk profile, provides access to combat-proven innovations, and offers a more streamlined investment pathway into this rapidly advancing field.

[92] See "How Ukraine Is Using AI Drones to Outsmart Russia on the Battlefield", United24
[93] See "How artificial intelligence is being integrated into the military sphere: models, prospects, challenges", Espreso [ua]
[94] See "Artificial Intelligence in Defence of Ukraine", ICDS
[95] See "Survival of the Smartest? Defense AI in Ukraine", The Very Long Game
[96] See "Mapping the use of artificial intelligence in priority sectors and the competitiveness of Ukraine", UNIDO

A key technical trend driving the growth is **modularity and cross-platform integration.**[97] This involves developing autonomous software as standalone modules (such as camera-equipped chips) that can be integrated into any platform — from FPV drones to unmanned ground turrets. However, it is important to note that the **transition** from automated systems that merely execute algorithms to truly autonomous systems capable of making decisions has not yet fully occurred. While AI is already replacing 99% of human labor in video analysis and reconnaissance, it still primarily enhances certain functions and addresses operational challenges rather than enabling full system autonomy. Observers emphasize that throughout this evolution, the principle of **"human-in-the-loop"** has to remain central — despite increasing automation, the final engagement decision remains with a human, ensuring ethical and strategic oversight.

Furthermore, the shift toward **network-centric warfare** is becoming critical. To ensure comprehensive real-time operational awareness, drones and other battlefield systems must increasingly be able to integrate with situational awareness and fire-correction platforms. These include "Delta" situational awareness system, "Zvook" acoustic reconnaissance system, "Griselda" text analysis system, "GIS Arta" artillery coordination system and others.

Currently, the majority of AI solutions are concentrated in the UAV sector, whereas **expanding these technologies** to ground, subsea, and maritime platforms requires further technical refinement for multi-domain operations. Even within the aerial domain, innovations such as drone swarms require better coordination among individual UAVs, achievable only through advances in AI algorithms and other supporting capabilities.

To support these advancements, there is a clear move toward **institutionalization, coordination and ecosystem building**.[98] Efforts are underway to address the rather chaotic trends by creating a unified, though largely unregulated, ecosystem involving the state, the private sector, and volunteers, while introducing grants for long-term projects.

Challenges

The Ukrainian defense AI sector faces a critical need **to stay a step (if not several steps) ahead of Russia**, especially given the enemy's significant investments in the field. To remain competitive, Ukraine must match Russia's investment volumes. While it is debatable whether Russia will be able to develop a fully AI-controlled kill chain, its financial capabilities are undoubtedly more extensive. Current developer efforts are focused on leveraging AI to establish a competitive advantage over Russia, which is also actively refining its military AI.[99] The primary challenge remains: **how to secure this advantage?** For Ukraine, the solution is straightforward yet demanding — the accumulation of knowledge and expertise, coupled with robust experience-sharing with international partners, while also accounting for the influential **"China factor"**.[100]

As was already mentioned, Ukraine's AI defense ecosystem is expanding rapidly. However, this network is becoming increasingly complex and necessitates synchronization. **Systemic integration remains a challenge** due to the diversity of projects, which can hinder efficiency and speed of implementation. On a more discursive note, there are warnings that enthusiasm for certain AI applications may divert resources, suggesting that some market solutions are currently

[97] See "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare", CSIS
[98] See "Artificial Intelligence in Defence of Ukraine", ICDS
[99] See "Survival of the Smartest? Defense AI in Ukraine", The Very Long Game
[100] See "The AI Frontier: Ukraine's role in the future of warfare", Friends of Europe

overestimated. Consequently, observers emphasize a need for an optimization and integration strategy alongside potential standardized protocol solutions. Currently, Ukraine has developed a roadmap that excludes defense AI from regulatory practices[101], largely but not exclusively due to **rapidly shifting battlefield dynamics, a complex and ever-changing operational environment and legal challenges**. The most appropriate solution in such circumstances is to balance domestic deregulation with a more constructive policy framework, leaving room for the sector's natural development while reducing the risks of the ecosystem becoming unmanageable.

Investment remains another significant hurdle. **Broader sectoral challenges** include the fact that many startups and SMEs lack proper accounting practices, reliable financial information, and standardized financial records. This hampers investors' ability to assess profitability and project future performance. Issues with intellectual property (IP) registration and the absence of formalized decision-making processes also create legal uncertainty.

An additional barrier has been the wartime ban on **arms exports**, which constrained production scalability and international revenue potential, thereby weakening the clear growth story investors typically seek. At the same time, recent policy changes suggest that Ukraine is beginning to replace a de facto export ban with a **controlled export model**, including new institutional steps, simplified procedures for some transfers, and the first approvals for wartime defense exports[102]. If implemented carefully, this could improve the sector's investment case by allowing selected companies to access foreign markets while preserving strict state oversight, protection of sensitive technologies, and priority supply for Ukraine's military needs. While this may appear less directly relevant to AI than to conventional arms production, it still matters because many defense AI solutions are embedded in export-controlled drones, interception systems, ISR platforms, and autonomy modules, so restrictions on international transfers also limit their ability to scale, reach foreign markets, and present a clearer growth case to investors.

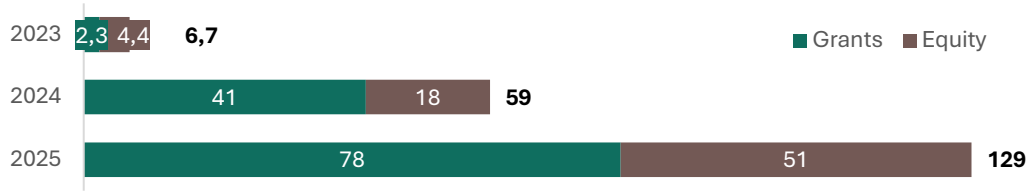
Beyond industry-specific limitations, significant concerns arise in **the ethical and governance domains**, especially regarding the limits of human control, accountability, and compliance with international law.[103] The Ukrainian defense AI sector has become a testing ground for determining whether a "human-in-the-loop" approach stifles innovation and where liability lies when humans are removed from the process. While Ukraine and its allies deliberate on these issues, the adversary continues to scale its capabilities without pausing for ethical dilemmas. Experts emphasize that human presence remains essential for ensuring accountability, judgment, and context, while simultaneously underscoring the need to facilitate innovation.[104] Likewise, while establishing a regulatory framework is challenging, implementing adaptive, flexible regulation could provide the necessary oversight without hindering innovation.

[101] See "Regulation of artificial intelligence in Ukraine: presenting a roadmap", Ministry of Digital Transformation [ua]
[102] See "Ukrainian arms producers receive first wartime export licences, Kyiv says", Reuters
[103] See "Military AI: Lessons from Ukraine", Tech Policy Press
[104] See "Autonomy is not intelligence: why the future of unmanned systems must remain human", Independent

IMPACT OF FINANCING ON COMPANY DEVELOPMENT

In 2025 Ukrainian tech companies received $498 million of financing (investments and grants). An estimated 26% of all investments and grants were directed to defense companies and startups. The total amount of financing (investments and grants) reached **$129 million**.[105] The real figure may be higher, as part of the defense tech funding remains undisclosed due to security considerations.

FIGURE 8. EQUITY INVESTMENTS AND GRANTS FOR DEFENSE COMPANIES AND STARTUPS, $ MILLION



Source: AVentures Capital, KSE Institute

The majority of significant investments targeted the AI/software segment, seen as lower risk compared to hardware or weapons production. Software avoids restrictions such as export prohibitions and circumvents investors' general reluctance to fund arms manufacturing.

The current financing structure reflects the early stage of Ukraine's defense and dual-use industry: a large number of immature startups, often with weak business development skills and a need for structured support.

Investors' Perspective: Defence Builder

Over the past four years, Ukraine's defense tech ecosystem has shown that a new industry can be built from near-zero to global relevance in a very short time.

This is no longer only a wartime story about urgent battlefield demand. It is a venture story with companies moving from prototype to scaled production in months, and some already show trajectories toward billion-dollar valuations, IPO paths, and strategic joint ventures.

This report confirms that the financing mix has changed over the years (grants, state support mechanisms, accelerators, equity, loans, etc.). In 2025, it estimates total financing (grants + investments) for Ukrainian defense companies and startups at $129 million, with the actual figure likely higher due to undisclosed defense-related funding. At the same time, grants remain essential at the earliest stages with Brave1 grant financing exceeding $60 million in 2025 and supporting 600+ companies. But grants alone do not build durable companies, production capacity, or long-term category leaders. The next phase requires venture capital, follow-on financing, and capital matched to company maturity.

From our perspective, the issue is not a lack of opportunities, but lack of targeted, risk-matched capital, especially capital combined with sector expertise and hands-on support. For investors entering the sector for the first time, it is also important to understand that diligence in Ukrainian

[105] See "Dealbook of Ukraine", AVentures Capital

defense tech is different not only because of risk, but because the core advantage is live battlefield learning, and that advantage changes fast. Wartime data and operational feedback are strategic assets. As a result, investors should expect partial visibility into some technical details, deployment data, or restricted components, especially where security, export-control, and technology-transfer constraints apply. At the same time, Ukraine is moving toward exports and joint ventures, which makes cross-border structuring and compliance readiness part of the investment thesis, not just legal paperwork.

In practice, two things are true at once: battlefield proof is a strong signal of product relevance, but it is not, by itself, proof of venture scalability. The investors best positioned to select winners are those with local market access and the ability to verify real performance, assess whether it could scale, and manage compliance requirements on the ground.

Across our accelerator + fund combined, we have built one of the larger private portfolios in Ukrainian defense tech (20+ companies), giving us a cross-stage view of company quality, capital use, and execution patterns. Some Defender Fund's earliest 2025 investments already show a combined potential uplift of more than ~7.5x based on expected 2026 follow-on rounds. This market is no longer just "high risk / high uncertainty." It is a market of asymmetric upside for investors with access and real sector expertise. Entry paths are becoming clearer, but outcomes will depend on strong local presence or trusted partners with ability to select the best opportunities early.

Daria Yaniieva
Chairman of the Board @ Defence Builder (accelerator, fund)

Investments and Grants

Grants

Prior to 2022, funding for Ukrainian defense startups was extremely limited, and no dedicated state investment mechanisms existed. This began to change in 2023 with the launch of the Brave1 defense tech cluster, a government coordination platform operating within the Innovation Development Fund under the Ministry of Digital Transformation in cooperation with the Ministry of Defense, General Staff, NSDC, and Ministry of Economy. Legally, Brave1 is not a separate entity but a state program and marketplace that issues grants, provides military-led expertise, and runs hackathons and acceleration activities. Applicants must be Ukrainian-registered legal entities with no links to Russia, Belarus or other sanctioned jurisdictions; foreign shareholders are allowed in practice as long as the company is incorporated in Ukraine and complies with sanctions, although Ukrainian producers are prioritized. In 2025, grant financing increased to over **$60 million**, up from roughly $40 million in 2024, allowing the program to support more than **600 companies**.

In parallel, the Ukrainian Startup Fund (USF) – also integrated into the Innovation Development Fund – pivoted toward wartime priorities and launched the Dual-Use Grant Support Programme in June 2022, offering up to $35,000 per project (including accelerator support) for technologies applicable to both civilian and defense needs. During 2022–2023 this program distributed about $1.2 million and supported UAV developers, training software, sensing systems and other solutions, combining funding with mentoring. Additional initiatives broadened the ecosystem: the EU-backed €20 million Seeds of Bravery program (137 projects funded in 2024), a USF–UMAEF $2.5 million early-stage grant

scheme, the Ministry of Economy's 2025 Made for Victory program providing up to ₴8 million in co-financed equipment grants (up to 80% for frontline regions and UAV producers), and the Google for Startups Ukraine Support Fund, which has delivered more than $15 million in $100,000 grants, cloud credits and mentorship to around 82 teams since 2022.

Equity

Private capital has rapidly become a second pillar of financing for Ukraine's defense tech sector, complementing state grants with equity, accelerator funding and strategic partnerships. The largest dedicated pool is the $30 million D3 Venture Fund (backed by Eric Schmidt), whose early investments in companies such as Swarmer, Buntar Aerospace, Airlogix and Frontline Robotics helped legitimize the market for foreign investors. DEFENDER Fund, investment arm of the Defence Builder ecosystem, adds an integrated accelerator-to-equity pathway to Ukraine's defense-tech financing landscape. Working in tandem with the accelerator, it backs pre-seed to selected Series A companies with tickets of up to $300,000. Portfolio includes companies as Sine Engineering, Falcons, MaxOn, Huless, and more. The MITS International Defence Accelerator (target size $50 million) is scaling from $200k seed tickets to multi-million rounds, including the $3.74 million Series A for the ground-robotics company Tencore and investments in Teletactica and UADamage. Early-stage and bridge capital is provided by funds such as Green Flag Ventures, Nezlamni (≈$2 million), Darkstar, Freedom Fund VC ($1–5 million tickets) and the Angel One angel syndicate, while WNISEF/u.ventures plays a quasi-DFI role, co-investing alongside European partners and signaling due-diligence quality to the market.

Venture Capital case: Ukrainian developer of UGVs

Ukraine-based developer and supplier of unmanned ground vehicles has become one of the country's fastest-growing defense-tech companies. Its flagship platform is a NATO-standardized, modular, tracked robot designed for a range of battlefield roles.

This product is battle-tested on the front lines, supporting logistics, casualty evacuation, engineering tasks, mine clearance, and fire support (mounting heavy machine guns or grenade launchers). A couple of dozen Ukrainian brigades use the platform, ordering units directly from the developer and receiving training and after-sales support. The company's rapid deployment has helped address frontline manpower shortages by allowing personnel to stay back from high-risk logistics and evacuation missions.

The investment was carried out through Ukraine's Diia.City legal regime, which provides a special framework for tech companies, including defense tech, allowing convertible loan agreements with international arbitration and foreign law protection. Thus, in 2025, this UGV developer secured a couple of million dollars in investment from an international defense VC and accelerator. They began their collaboration with the investor within an accelerator framework not as a fledgling startup but as an already structured, established company, which served as the catalyst for negotiations regarding a potential investment.

The investment was secured to drive **institutional growth and product enhancement** across several key areas:

- **Scaling production**, procuring robotic equipment to automate and increase output.

- **Expanding infrastructure**, increasing production capacity through the leasing or acquisition of new warehouse and manufacturing facilities.
- **Team expansion**, specifically growing the R&D department to accelerate the development of new technologies.
- **Market development**, promoting the UGV market, and ensuring that military end users' needs are fully met.

FIGURE 9. REVENUE GROWTH

Source: KSE Institute

Consequently, the developer can now improve their leading product based on end-user feedback. In addition, the manufacturer recently developed an enhanced version of this platform, while another R&D team is working on additional modules for the UGV and on entirely new products. Currently, the team is seeing **production volumes increased approximately fourfold** compared to 2024.

Notably, in making the decision to commit capital, the investor relied primarily not on financial indicators — as the company was scaling rapidly and could not yet provide stable financial reporting — but rather on the quality of the product, feedback from the military, the strength of the team, and personal impressions from trials at the testing range. At the same time, large state contracts had already been signed by the time of the investment, which added significant confidence to the deal.

However, the company notes that **foreign investors must be prepared for the specific features of the Ukrainian defense tech market**. First, the market is extremely dynamic, making long-term forecasting inherently risky. Furthermore, there are numerous circumstances beyond a manufacturer's control due to the war conditions. Interested investors must also be prepared for the fact that, during the due diligence process, companies may be restricted in sharing confidential information to prevent the disclosure of manufacturing locations and other sensitive data. Second, a potential investor must have a deep understanding of the end user, the military, and the structure of communication and feedback loops, as the company must adapt rapidly to consumer needs. As this developer's experience has shown, the ambition and proactivity of the owners and key managers play a major role, as they personally visit the front lines and communicate directly with combat units.

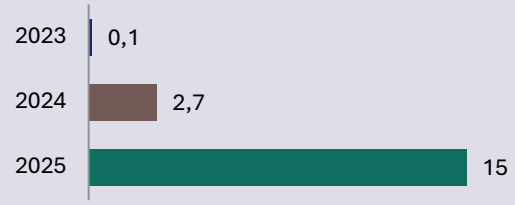
Strategic and individual investors are increasingly important for larger scaling rounds and international integration. Western defense companies are entering through equity stakes and joint R&D – for example Quantum Systems' share in Frontline and Terma's partnership with Odd Systems – bringing supply-chain access and export pathways in addition to capital. High-net-worth investors such as Brooks Newmark (who committed $5 million to build the Trypillian group) and Ukrainian tech founders reinvesting their own funds add flexible risk capital, while grassroots vehicles like Resist.ua finance very early FPV and EW teams at the prototype stage. Major domestic funds such as Horizon Capital and TA Ventures are beginning to explore the sector, indicating future capacity for larger growth rounds. Together, this creates a multi-layered investment stack – from angels and accelerators to venture funds, DFIs and corporate strategics – that did not exist before 2022 and is now capable of financing Ukrainian defense technologies across the full development cycle.

Grant + Venture Capital + IPO case: Swarmer

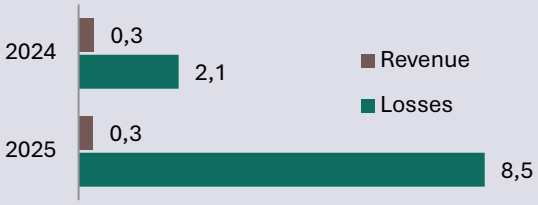
Swarmer is a Ukrainian startup specializing in developing a software platform that enables unmanned aerial vehicles (UAVs) to operate autonomously in coordinated swarms. In 2025, it reached the point where swarms of up to 25 drones are operating autonomously in GNSS-denied environments. The company's developed swarm-management platform, consisting of Swarmer UI, Swarmer AI, and Swarmer OS, handles independent coordination and data sharing of dozens of drones. Currently, the team plans to expand capabilities to include hundreds of drones in combined-arms operations, integrating aerial, surface, ground vehicles. At the same time, Swarmer Platform requires humans to make all life-or-death decisions while allowing AI to handle rapid data processing and tactical response.

As of now, the team has raised about $20 million in capital. In 2023, Swarmer raised $125 000 in private investment during a pre-seed round. By 2024, this figure increased to $2.7 million in the seed round. In 2025, as part of a Series A round, the company secured $15 million. This investment is the largest publicly disclosed funding round for a Ukrainian defense tech company to date. Additionally, the startup previously received $50 000 and $200 000 grants from Brave1. Swarmer's current portfolio includes a diverse range of investors, including Broadband Capital Investments, R-GAI, Radius Capital, Green Flag Ventures, and Network VC.

FIGURE 10. INVESTMENTS, $ MLN



REVENUE AND LOSSES, $ MLN



Source: United24

The investments received were primarily directed toward the **accelerated growth of the company**:

- **Product development** – continuous refinement and engineering of the core product.
- **Team expansion**, focusing on scaling human capital.
- **Market penetration and end-user engagement**, prioritizing the fastest possible interaction with end users.

The investment has also enabled testing, which is more expensive for drone swarms, as 5-10 times more drones are lost at a time.

Swarmer's experience is common among other companies raising venture capital. In the early stages, investors primarily invest in the founder and the idea, specifically its viability, and only later shift their focus to the management team's ability to navigate the market and maintain a balance between rapid growth and staying focused on the product. At this stage of development, the focus is on the absorption and efficient utilization of allocated funding rather than on immediate profitability or revenue growth.

On 2 February 2026 Swarmer has filed for a Nasdaq IPO, becoming the first Ukrainian defense tech company to start the public listing process.

Loans

In Ukraine, the government introduced the “5-7-9” affordable loan program in 2020 to support small and medium-sized businesses with concessional credit. Initially it was open to a wide range of sectors, with no specific exemptions for dual-use goods, but the defense industry was formally included only in 2024. CMU Resolution № 1288 (05.11.2024) “Some issues of providing state financial support to enterprises designated as critical for the functioning of the economy during a special period in the defense-industrial sector" applies to enterprises recognized as critical by Ministry of Defense (earlier – Ministry of Strategic Industries).

Form of support: partial compensation of loan servicing costs. Support is provided via the Business Development Fund (under Ministry of Finance).

Eligible loans: for development, production, repair, modernization, and disposal of arms, military and special equipment, ammunition, and components to meet the needs of the Armed Forces and other military formations.

- Purpose: both investments and working capital.
- Loan amounts: up to UAH 500 million for 5 years (investments), up to UAH 100 million for 3 years (working capital).
- Maximum interest rate: UIRD(3m) + 5%.
- Reduced to 5% annual effective rate.

Financing scheme: The recipient obtains critical status, concludes a loan agreement with an authorized bank under set terms, the Fund opens an escrow account at the bank, and the bank receives repayment of interest from the Fund.

Assessment: The simplest, most transparent, and tested mechanism. It applies not only to defense but other sectors too. However, given the specific risks of the defense sector (supply chains, procurement, force majeure), it is advisable to establish a **separate sub-program** for the defense industry.

As of February 2026, **108 loans granted worth ~UAH 6.7 billion (~$160 million) and 103 enterprises applied**. An additional 13 loans have already been approved for disbursement, and 68 applications are currently under review.

To obtain an affordable loan, manufacturers must apply to a bank participating in the program. Currently, there are **five banks** that meet defined security criteria: **Ukreximbank**, **Oschadbank**, **MTB Bank, PUMB**, and **Bank Credit Dnipro**.

Loans + **Venture Capital case: Infozahyst**

The company Infozahyst supplies the Ukrainian defense market with signals intelligence, electronic warfare systems, and high-frequency technical defense systems. The team has experience with **various types of funding**: prior to 2022, they received private-equity capital from a single private individual. Later, they managed to secure a loan under the state program "Affordable Loans 5-7-9%" as well as specialized loans for the defense industry. Over the years of

the full-scale war, the company's **team has doubled in size**, now numbering 400 employees, including developers of various profiles, design engineers and cybersecurity specialists.[106]

Infozahyst is currently partnering with a **Danish holding company**, which significantly strengthens their ability to supply products to the Ukrainian military. Furthermore, this partnership is strategically vital as it helps to:

- Strengthen the company's branding.
- Receive philanthropic support for corporatization.
- Facilitate access to EU markets.
- Scale and attract investments larger than those acquired through other channels.
- Expand the pool of funds available for OPEX projects and specific R&D developments.

The company has noted plans to expand its presence not only into the Nordic region but across all of Europe.

The company is also in the process of **applying for two additional loans** to expand its production and repair capabilities, as well as to purchase equipment and complex technical facilities. However, Infozahyst is one of many companies in the Ukrainian defense market highlighting the difficulty of obtaining financing and loans for R&D, particularly from banking institutions. This forces the company to outsource studies to state institutes, underscoring the need for investments specifically targeting R&D expenditures. Moreover, Ukrainian banks' credit-risk committees lack experience with software-related costs, making it difficult to secure financing for specialized tools.

Despite having an expanded team, the company still faces an **outflow and shortage of specialized personnel** in several high-technology domains, particularly in:

- Materials science, metamaterials, and nanotechnology.
- Electrodynamics and radio engineering.
- Modelling and quantum computing.

To address this, Infozahyst has opened **a back-office in Poland** to bring in Ukrainian expatriates and serve as a hub for future R&D collaborations. The company stresses the need to start talent development by investing in vocational schools, technical colleges, and university programs.

The company emphasizes that various financial instruments, while imperfect, represent an efficient and unprecedented opportunity for Ukrainian businesses to attract capital. Therefore, investment and exports are the keys to ensuring the defense industry once again becomes a unique achievement for Ukraine.

Loans case: Ukrainian manufacturer of ammunition for drones

A Ukrainian company has been manufacturing munitions of various functions and calibers for drones since 2022, operating on a closed-cycle production basis. By delivering a finished munition and producing several thousand units per month, they ensure a complete end-to-end manufacturing process.

[106] See "Defense pays more than IT." Infozahyst CEO on the shortage of engineers, exports without illusions, and deftech problems", DOU [ua]

The company secured funding through the state program "Affordable Loans 5-7-9%", which is designed to support Ukrainian manufacturers — including defense tech developers — and stimulate business by reducing the cost of credit through state subsidies or guarantees. The enterprise successfully utilized a loan at an annual rate of 5%, whereas the standard bank rate is approximately five times higher, a factor that would have significantly impacted the final cost of the product.

Thanks to this loan, the company was able to purchase equipment and acquire a new facility. As a result, production volume increased approximately **fourfold**. Additionally, since its founding, the enterprise has **doubled** its number of design engineers, although recruiting engineering and technical staff remains a persistent challenge.

Partner States Funding

Partner states funding (often referred as Danish model) has emerged as one of the most practical and scalable frameworks for accelerating the growth of defense and dual-use technology companies in Ukraine. At its core, it is not merely a funding instrument but a demand-driven industrial development mechanism that links financing with real procurement, shortens the path from innovation to deployment, and provides companies with predictable revenue streams. In 2025, foreign funding for Ukraine's defense industry totaled **$6.1 billion**. By comparison, the figure for 2024 was approximately **$600 million**.[107]

By allocating funds for the direct purchase of Ukrainian-produced capabilities for the needs of the Armed Forces of Ukraine, the model addresses the most critical constraint faced by high-growth technology firms in wartime: the gap between technological potential and bankable demand. Confirmed contracts enable companies to move beyond prototype production, invest in serial manufacturing, hire and retain skilled personnel, and build resilient supply chains. This, in turn, unlocks access to additional private capital, as revenue visibility and validated battlefield performance significantly reduce investor risk.

Equally important, the partner states funding creates a powerful signaling effect. It demonstrates trust in domestic producers, validates their products through operational use, and integrates them into international defense procurement and cooperation frameworks. For companies, this means not only immediate scaling opportunities but also a pathway to export markets, partnerships with global primes, and long-term participation in European defense value chains.

Partner states funding case: Ukrainian manufacturer of Deep Strike drones

The company has a long production track record and had been operating well before the full-scale invasion. However, its revenues remained relatively low and volatile for many years. A major contract secured in 2024 became a turning point: it led to a multiple increase in revenue and enabled rapid scaling of operations. As a result, the company expanded its workforce threefold, reflecting a

[107] See "The Ministry of Defence secured over $6 billion for Ukraine's defense industry in 2025", Ministry of Defence of Ukraine

transition from a small, unstable producer to a significantly larger and more sustainable industrial player.

FIGURE 11. REVENUE GROWTH

Source: KSE Institute

The company's rapid expansion was largely enabled by financing provided by one of the partner states. At a time when the growth of Ukrainian defense manufacturers is constrained by the limited purchasing capacity of the state, this mechanism creates an alternative and predictable source of demand, allowing companies to scale production, invest in their workforce, and plan longer-term development.

In an ecosystem where many firms are technology-rich but capital-constrained, the partner states funding transforms procurement into a catalyst for industrial growth. It allows companies to shift from survival to strategic development — investing in R&D, improving product quality, expanding production capacity, and professionalizing corporate governance. Ultimately, it is a model that converts public funding into sustainable private sector expansion, strengthening both national defense capabilities and the future competitiveness of the industry.

INVESTMENT INSTRUMENTS

Traditional venture capital metrics often fail in defense contexts because risk profiles shift dramatically between a lab prototype (TRL 4) and a fielded system (TRL 7). This framework uses Technology Readiness Level (TRL) as the organizing logic for evaluating Ukrainian defense tech investments.

Unlike commercial software where beta products can generate revenue, defense hardware requires strict validation before adoption. TRL measures technology maturity from conceptualization to deployment. As companies progress through TRL stages, risk evolves from technical ("will it work?") to execution ("can we scale manufacturing?").

By aligning investment instruments—grants, equity, and venture debt—with specific TRL stages, investors can match capital structures to the technical and operational realities of defense technology development.

Defense Tech Maturity Stages

TRL 1-2

Concept and Basic Research

Theoretical validation through paper studies of basic properties. Scientific research begins translating into applied R&D. Highest technical risk and highest potential upside.

TRL 3-4

Proof of Concept and Lab Proto

Lab prototypes and bench tests demonstrate technical feasibility. Active R&D with analytical and experimental proof of concept in laboratory environment. Operational utility not yet proven.

TRL 5-6

Prototype in Environment

System tested in relevant simulated environment. Risk transitions from pure engineering to product-market fit. Component/breadboard validation and subsystem prototype demonstration.

TRL 7

Operational Demonstration

System prototype demonstration in operational environment with field tests and end-users. Critical inflection point for defense valuation.

TRL 8–9

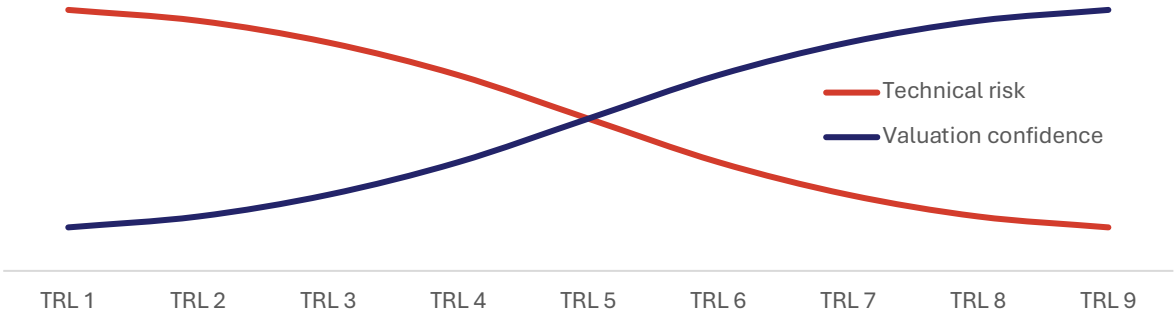
Deployment & Scaling

Actual system completed, qualified, and proven through successful mission operations. Focus shifts to scaling manufacturing, logistics, and supply chain.

Risk and Capital Dynamics

The evolution of a defense technology company across Technology Readiness Levels (TRLs) is not only a technical process but also a fundamental shift in its risk profile and access to capital. Each successive stage reduces uncertainty, increases the reliability of valuation, and unlocks new financing instruments, thereby reshaping the optimal funding structure.

FIGURE 12. RISK AND CAPITAL DYNAMICS

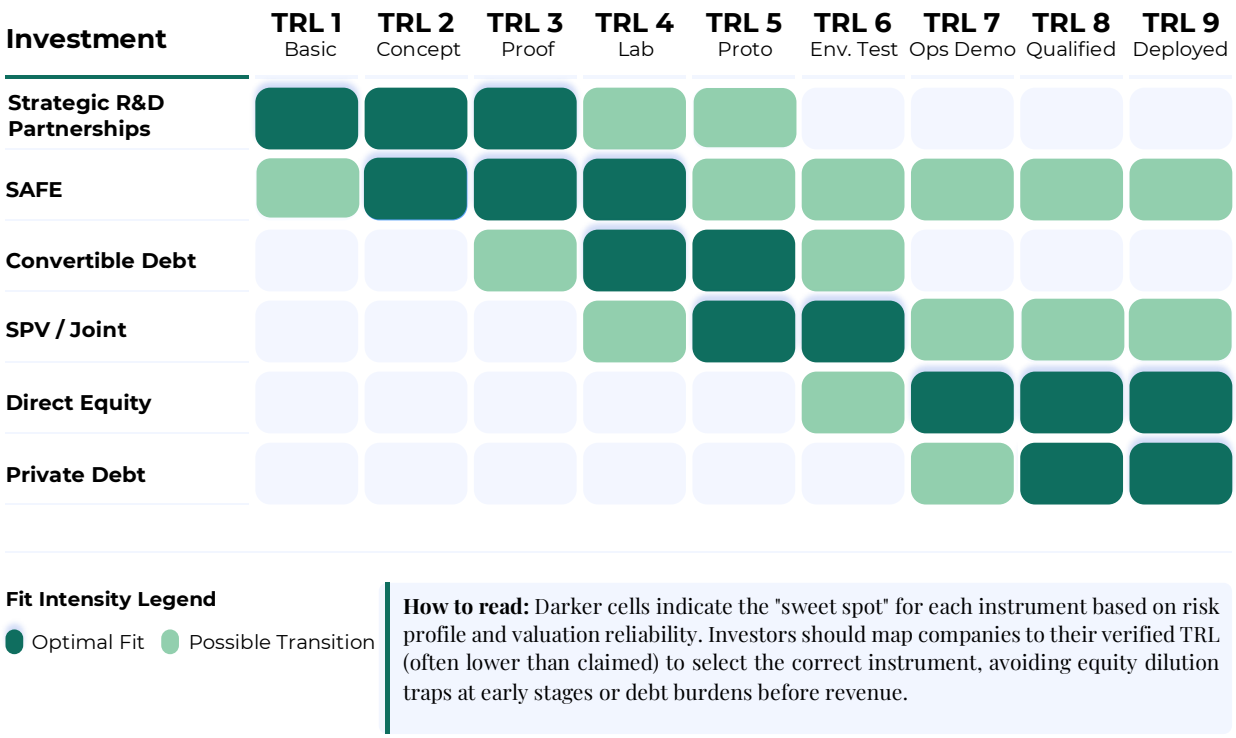


As TRL increases (1 to 9):

- **Technical Risk (↓):** Falls because the "unknowns" are engineered out through prototyping and real-world deployment.
- **Valuation Confidence (↑):** Rises because data replaces assumptions, making the project a safer bet for institutional capital.
- **Capital Needs (↑):** Scale-up requires significantly more hardware and infrastructure than R&D.
- **Debt Capacity (↑):** Lower risk allows the transition from expensive equity to cheaper debt financing.

Instrument Fit Snapshot

FIGURE 13. TRL VS. INSTRUMENT FIT HEATMAP



How to read: Darker cells indicate the "sweet spot" for each instrument based on risk profile and valuation reliability. Investors should map companies to their verified TRL (often lower than claimed) to select the correct instrument, avoiding equity dilution traps at early stages or debt burdens before revenue.

TRL 1-5: R&D Partnerships + Option Capital (SAFE)

At this stage, the primary objective is proving the scientific concept and moving from the lab to a functional prototype. Because technical risk is at its peak and revenue is non-existent, traditional valuation is nearly impossible. Funding relies on R&D grants and SAFE (Simple Agreement for Future Equity) agreements, which allow investors to provide capital now while deferring valuation until a later, more predictable priced round.

TRL 5-7: Equity-Anchored + SPVs

As the technology moves into field testing and pilot programs, the focus shifts to scaling the solution for real-world environments. Special Purpose Vehicles (SPVs) are frequently used here to isolate the specific risks of a pilot project from the main company. This stage is "equity-anchored" because while risk has decreased, it is still too high for banks; investors provide growth capital in exchange for direct ownership as they witness the transition from prototype to product.

TRL 7-9: Growth Equity + Debt

Once the technology is fully operational and integrated into the market, the business model becomes the primary focus. With technical failure largely off the table, the company can access Growth Equity to dominate the market share. More importantly, the high valuation confidence and predictable cash flows finally unlock Debt Financing. This allows the company to scale production or infrastructure using cheaper, non-dilutive capital while preparing for an exit or IPO.

Possible Financial Instruments

Different financing instruments correspond to different stages of technological maturity. As a defense technology progresses across TRLs, declining technical risk, improving revenue visibility, and growing capital intensity reshape both investor appetite and the optimal capital structure. The following toolkit illustrates which instruments are structurally best suited for each phase of the lifecycle.

1. Strategic R&D Partnerships (TRL 1–5)

Description & Structure: Under this framework, an investor provides specialized R&D capital in exchange for a royalty on future sales or a first-right-of-refusal for licensing deals. The partnership is structured around gaining technology access rather than traditional equity ownership, appealing to strategic investors who seek to bridge funding from concept through prototype testing.

- **Advantage (+):** This approach provides the investor with direct access to emerging technology while maintaining a lower capital commitment than equity, often resulting in a predictable return structure tied directly to sales.
- **Disadvantage (-):** The primary drawback is the limited upside potential compared to full equity ownership, and the timeline for revenue realization may be significantly extended due to the early stage of development.

2. SAFE — Simple Agreement for Future Equity (TRL 1–9)

Description and Structure: The SAFE serves as a streamlined agreement where capital converts to shares at the next priced funding round, typically incorporating a valuation cap or discount. It

functions as option-like capital that is particularly useful for high-growth potential when a formal valuation is currently unreliable.

- **Advantage (+):** This instrument allows for very fast execution and defers the valuation process while providing the investor with a built-in discount hedge to gain upside from the valuation cap.
- **Disadvantage (-):** Investors face a lack of downside protection or liquidation preferences, and the timing of the conversion remains uncertain as there is no fixed maturity date.

3. Convertible Note (TRL 3–6)

Description and Structure: This is a debt instrument designed to convert into equity upon specific triggers, such as future financing or liquidity events. It balances early-stage uncertainty by including features like a maturity date, interest rate, and conversion caps to protect the investor's initial outlay.

- **Advantage (+):** It successfully defers valuation to a later stage while offering faster execution than priced equity and providing partial downside protection through its status as debt.
- **Disadvantage (-):** The investor lacks control or governance rights prior to conversion, and the accrual of interest may ultimately reduce the equity upside during the final conversion process.

4. SPV / Joint Venture (TRL 4–7)

Description and Structure: This involves the creation of a separate legal entity dedicated to a specific product or technology, characterized by defined IP contributions and clear governance. It is the ideal structure when a specific technology's maturity outperforms the parent company or possesses a distinct risk profile.

- **Advantage (+):** The structure allows for the effective isolation of risks and the deferral of valuation, providing a clear mechanism for exit or independent capitalization.
- **Disadvantage (-):** Like other pre-equity tools, it offers no control before conversion and relies heavily on the success of future financing rounds to realize value.

5. Direct Equity (TRL 6–9)

Description and Structure: This involves an ownership stake, typically a minority interest of 10–30%, governed by a formal Shareholders' Agreement. Equity capital is best utilized once feasibility and demand are validated, as it allows the investor to absorb scale, production, and procurement risks.

- **Advantage (+):** Investors benefit from full upside participation and significant governance influence, ensuring that incentives remain aligned between the founders and the investors.
- **Disadvantage (-):** There is a substantial valuation risk at the point of entry, and the stake is generally illiquid with exposure to the risks of the entire company rather than a specific project.

6. Private Debt (TRL 7–9)

Description and Structure: Private debt is a fixed-income financing model that is either secured or revenue-linked and sits senior to equity in the capital stack. Once revenues and order books are established, leveraging debt can materially improve risk-adjusted returns without further diluting ownership.

- **Advantage (+):** It provides capital seniority and a predictable yield, offering strong downside protection through fixed or flexible repayment covenants.
- **Disadvantage (-):** The upside is strictly limited to the interest and principal, and the requirement for consistent cash flow to service the debt can strain operations; furthermore, it offers no governance or control rights.

Investor Decision Framework

In Ukraine's rapidly evolving, battlefield-driven innovation environment, the speed of technological development often outpaces traditional investment processes. A clear decision framework allows investors to distinguish between demonstrable capability and unverified claims while structuring transactions in a bankable way.

Before investing:

- **TRL Validation:** Is technical maturity proven or just claimed?
- **Operational Proof:** Is there battlefield validation by end-users?
- **IP Ownership:** Who owns the IP and where is it registered?

Instrument selection:

- **Valuation:** Is it reliable enough for equity, or defer via SAFE?
- **Protection:** Is downside protection (debt/notes) required?
- **Scope:** Investing in the company platform or a specific product?

Ukraine specifics:

- **Compliance:** Check export controls and end-use restrictions.
- **Certification:** Preparedness for Ukrainian MoD certification and NATO codification to unlock procurement and export markets
- **IP Protection:** File IP registration in parallel with Ukrpatent and foreign jurisdictions (US/EU) to ensure comprehensive protection.

Actionable Investor Next Steps

The following actions define the minimum execution requirements for translating investment intent into risk-adjusted capital deployment.

Validate TRL and Market Traction

Investors must go beyond pitch-deck claims to demand concrete evidence of field testing and pilot deployments. It is essential to verify end-user feedback from these early implementations to ensure that the technology's performance in real-world conditions aligns with its theoretical potential.

Confirm IP Ownership and Protection

A rigorous audit of the Intellectual Property portfolio is mandatory to ensure all assets are cleanly held by the company with proper legal assignments. Furthermore, one should verify that protection is actively maintained and enforceable in all key strategic jurisdictions, specifically including Ukraine, the US, and the EU.

Isolate Product-Specific Risk

In scenarios where a single technology's maturity or risk profile differs significantly from the parent company's overall operations, strategic isolation is recommended. Utilizing Special Purpose Vehicles (SPVs) or Joint Ventures (JVs) allows for targeted investment and protects the broader organization from specific technical or project-related liabilities.

Deploy Debt Strategically

Debt should only be introduced into the capital stack once there is high revenue visibility or long-term contracts in place. This ensures clear serviceability and provides essential downside protection, allowing for non-dilutive scaling only when the project's cash flows are stable enough to support traditional financing.

Investment Rule of Thumb

1. Early Stage: Discovery and Proof (TRL ≤ 4)

Focus: R&D Partnerships and Option Capital

At this entry point, the primary challenge is High Technical Risk. Traditional valuation is unreliable because the product hasn't left the lab. Funding strategy focuses on R&D Partnerships, grants, and Option Capital like SAFEs or Convertible Debt. These instruments allow early believers to provide seed funding without forcing a premature valuation, effectively "buying an option" on the technology's future success.

2. Mid-Stage: Validation and Transition (TRL 5–7)

Focus: Equity-Anchored and Risk Isolation

As you move into the Validation Phase, the risk profile shifts from "Will it work?" to "Can it scale?". This is a critical Risk Transition period. Capital becomes Equity-Anchored, involving direct equity rounds or Special Purpose Vehicles (SPVs) and Joint Ventures (JVs). These structures are designed to isolate project-specific risks and bring in strategic partners who provide more than just cash—they provide the testing grounds for prototypes and field validation.

3. Scale: Commercial Deployment (TRL ≥ 8)

Focus: Growth Capital and Asset-Backed Debt

At TRL 8 and beyond, the technology is Deployment Ready and increasingly Revenue Generating. The "Technical Risk" has been largely eliminated, replaced by market execution risk. This maturity allows the company to tap into Growth Equity and, crucially, Senior Debt. Because the asset is now bankable and predictable, you can use debt to finance large-scale production and deployment, which is significantly less dilutive for founders and early investors than equity alone.

US-UKRAINE STRATEGIC PARTNERSHIP

The United States and Ukraine are strategic partners bound by shared security interests, democratic values, and a common vision for a stable and prosperous Euro-Atlantic area. Over the past decade—and especially since 2022 — this partnership has evolved from traditional security assistance into a comprehensive, institutionalized framework that spans defense, technology, energy, and investment. A network of bilateral agreements, multi-year funding mechanisms, and joint industrial initiatives demonstrates a clear mutual commitment not only to Ukraine's immediate resilience, but to long-term cooperation that will endure beyond the current phase of the war.

Baseline Strategic Agreements

At the core of this relationship is the renewed **U.S.–Ukraine Charter on Strategic Partnership**[108], which defines cooperation across security, economic, and governance dimensions and anchors Ukraine's Euro-Atlantic trajectory. This political foundation has been reinforced by the **bilateral ten-year security agreement**[109] concluded as part of the G7 commitments, stating structured, capability-based planning, long-term training, intelligence sharing, and defense industrial integration. In parallel, multi-year funding instruments authorized by the U.S. Congress—particularly through the **Ukraine Security Assistance Initiative**[110] and Foreign Military Financing—create predictable demand, enable long-term procurement contracts, and connect Ukrainian capabilities to the U.S. and allied defense industrial base.

This institutional architecture is complemented by practical cooperation in joint production, battlefield technology development, and regular high-level coordination formats such as the Ukraine Defense Contact Group. Together, these mechanisms signal that the U.S.–Ukraine partnership is not a temporary response to crisis, but a strategic, future-oriented alignment. For the private sector and international investors, this provides a durable policy framework, reduces political risk, and confirms that Ukraine will remain a central element of the United States' security and industrial strategy in Europe for years to come.

The architecture of cooperation is currently being formed on the basis of the following institutions (initiatives).

The Ukraine Recovery and Infrastructure Fund (URIF) was created as a partnership that finances and coordinates investment projects for the recovery and development of Ukraine. It was established through an intergovernmental agreement between Ukraine and the United States. The Fund's initial capital has been formed from equal contributions – $75 million from the United States via DFC and $75 million from Ukraine, totaling $150 million in seed capital. The Fund's activities are focused on the following key areas: natural resources, energy, information and communication technology, development of logistics infrastructure, and strategic and emerging technologies. At present, the Fund has already received more than 60 project proposals across all declared sectors. The authorized partners are the U.S. International Development Finance Corporation (DFC) from the United States and the Public–Private Partnership Agency (PPP Agency) from Ukraine. The interaction procedure is

[108] See "U.S.-Ukraine Charter on Strategic Partnership", US Department of State
[109] See "Bilateral security agreement between Ukraine and the United States of America", President of Ukraine
[110] See "Operation Atlantic Resolve (OAR)", Special Inspector General report to Congress

structured as follows: an online portal[111], has been created through which potential participants submit applications describing their projects. The Fund then conducts a due diligence review and makes a decision on financing. Further monitoring of project implementation is envisaged. The integration of already existing international cooperation projects into the Fund's framework is possible.

Furthermore, a **Prosperity Plan**[112] aiming to attract $800 billion of public and private funds to help rebuild Ukraine is discussed. The leaked draft document describes a **long-term joint EU–U.S. economic strategy for Ukraine after the war.** The main lines of this initiative are EU integration and security guarantees, mobilization of private capital, and the restoration of human capital in Ukraine. The indicative targets on which the participants in the discussion rely (and which will also guide future recovery projects) are the return of 2.1 million citizens within two years after the war, an increase in labor productivity from 1.3% to 5% annual growth, and the attraction of USD 400 billion in private capital.

Thus, if these two initiatives are combined, and taking into account the political discussions on Ukraine's further development, it can be assumed that the potential of Ukraine's post-war recovery is being formed and will be expanded in the following promising areas: ensuring security, restoration of human capital, restoration of industry, and restoration of agriculture.

Market Potential

- **Security:** USD 140 billion for the formation of a sustainable security structure and USD 20 billion annually, with export potential from USD 10 to 100 billion per year.
- **Restoration of human capital:** the housing market potential from USD 2.5 billion per year (rental), the services market from USD 1.5 billion per year only for creating living conditions for those who return.
- **Industrial recovery:** according to RDNA4, the need for funds to restore production and infrastructure amounts to about USD 300 billion over 10 years. This is essentially a sales market for tool manufacturing, construction, and related services.
- **Agricultural recovery:** the cost of demining agricultural land exceeds USD 10 billion (USD 1,500 per hectare, 50% of the mined 140,000 sq. km).

Promising investment projects

Security. Investment priorities are as follows:

- development of joint production of weapons and military equipment (Radionix and others)
- construction of a service network for Western-produced weapons; ammunition production
- development of a secure communications network to control the line of demarcation
- development of early warning systems for air threats from the east (radars, AWACS)
- training centers for mastering modern weapons by the military of partner countries
- development of production in the dual-use segment, primarily UGVs and UAVs; production of weapons and military

[111] See "Mobilizing Investments for the Reconstruction and Prosperity of Ukraine", URIF
[112] See "Document reveals EU-US pitch for $800B postwar Ukraine 'prosperity' plan", Politico

- development of infrastructure for hosting the “Coalition of the Willing” forces.

Restoration of human capital. Key factors are security, availability of jobs, provision of housing, and social infrastructure. Investment priorities are as follows:

- construction of housing in new industrial clusters to receive citizens returning from abroad on the basis of subsequent rental
- development of the service sector for citizens returning from abroad
- construction of social infrastructure in conjunction with local employers (possible launch of financing programs through the insurance system and others)
- construction of new vocational and technical educational institutions for training specialists on the basis of secondary education.

Industrial recovery. The foundation will be recovery in the energy sector. On the basis of restored energy supply capacities, new industrial clusters will be formed. Investment priorities are as follows:

- construction of decentralized power generation facilities (wind, solar energy, small hydropower)
- restoration of HPPs and NPPs
- production of equipment for distribution networks
- restoration of distribution systems (electricity transmission lines)
- tool manufacturing
- machine-tool building for the needs of the energy sector, the defense-industrial complex, the mining industry, and mechanical engineering
- production of electronic components for industrial equipment; metallurgy – construction of new and modernization of existing metallurgical plants to new environmental safety standards
- advanced technologies – investment in the development of R&D on the basis of existing military production with the aim of their conversion
- recycling of secondary raw materials, as the clearing of territories after hostilities will generate enormous volumes of secondary raw materials for processing.

Agriculture

- USD 25 billion is the real potential for investment in land, and the same amount for investment in equipment and machinery.
- USD 25 billion invested in the land market will immediately be converted into a consumer market in rural areas.
- The humanitarian demining market for agricultural land alone amounts to USD 10 billion.

In total, over a 10-year horizon after the end of hostilities, the market related only to recovery and defense amounts to $690 billion.

LEGAL FRAMEWORK FOR INVESTMENTS

Current Regulations on Investments

Foreign investment drives Ukraine's growth via capital, technology, and job creation. Key laws—"On Foreign Investment," "On Investment Activity," and the "Investment Nanny" act—guarantee protection, profit repatriation, and incentives for large-scale projects. This framework integrates the Tax Code, double taxation treaties, and war-risk insurance through the ECA. Corporate forms are further shielded by BITs and international arbitration.

How Does Investing in Ukraine Differ from Investing in the U.S. or the EU?

Ukraine offers an open investment regime in defense, R&D, and high-tech, guaranteeing national treatment, expropriation protection, and profit repatriation. **Unlike the established U.S. (CFIUS) or EU screening models, Ukraine is currently institutionalizing its own FDI framework.** Key unique features include **martial law and NBU currency restrictions on dividends.** While the defense sector is open via joint ventures and R&D, it remains sensitive, requiring specific licensing. Risks are mitigated by the ECA, BITs, and international support. Post-war, Ukraine aims for full currency liberalization and alignment with EU regulatory standards.

- **Law of Ukraine on Protection of Foreign Investments in Ukraine –** guarantees investment security, prohibits uncompensated expropriation, and ensures rights to profit repatriation, reinvestment, and defense-sector licensing.[113]
- **Law of Ukraine on Foreign Investment** defines the specifics of foreign investment in Ukraine, establishes national treatment, a 10-year stability clause, protection against nationalization, and rights to international arbitration and IP protection. [114]
- **Law of Ukraine on Investment Activity** defines the general legal, economic, and social conditions for investment activity in Ukraine, grants investors full autonomy over project goals and partner selection while prohibiting state interference in private contracts. [115]
- **Law of Ukraine on State Support for Investment Projects with Significant Investments in Ukraine** provides 30% investment compensation and tax exemptions for 15-year projects exceeding €12M that create 10–50 new jobs.[116]
- **Law of Ukraine "On Amendments to the Law of Ukraine" On Financial Mechanisms for Stimulating Export Activities"** empowers the Export Credit Agency (ECA) to insure and reinsure investments and infrastructure against military and political risks.[117]
- **Agreement between Ukraine and the United States of America on the Promotion and Reciprocal Protection of Investments** guarantees American investors national treatment, protection against uncompensated expropriation, and the right to international arbitration (ICSID/UNCITRAL)[118]
- **Convention between the Government of Ukraine and the Government of the United States of America for the avoidance of double taxation and the prevention of fiscal evasion with**

[113] See "Law of Ukraine On Protection of Foreign Investments in Ukraine", Verkhovna Rada of Ukraine, Vidomosti Verkhovnoyi Rady Ukrainy (VVR) [ua]
[114] See "Law of Ukraine on Foreign Investment", VVR [ua]
[115] See "Law of Ukraine on Investment Activity", VVR [ua]
[116] See "Law of Ukraine on State Support for Investment Projects with Significant Investments in Ukraine", VVR [ua]
[117] See "Law of Ukraine "On Amendments to the Law of Ukraine", VVR [ua]
[118] See "Agreement between Ukraine and the United States of America", VVR [ua]

respect to taxes on income and capital reduces Ukrainian withholding tax on dividends to 5% (for major stakes) and royalties to 10%, while exempting interest in most cases. [119]

- **The Law of Ukraine on International Commercial Arbitration** allows parties to bypass local courts by choosing foreign seats, languages, and flexible rules for resolving international economic disputes.[120]
- **Resolution of the National Bank of Ukraine "On the operation of the banking system during the period of martial law"** restricts martial law currency transfers but permits payments for imports, debt service to international lenders, and dividend repatriation (up to €1M/month for profits earned after Jan 2023).[121]
- **Law of Ukraine on Currency and Currency Transactions** establishes the principle of currency freedom for non-residents while authorizing the NBU to impose temporary protective measures during crises. [122]
- **Law of Ukraine on Banks and Banking Activities** regulates the licensing and operation of banks, ensuring foreign investors can open accounts and acquire equity in the Ukrainian banking sector.[123]
- **Law of Ukraine on State Registration of Legal Entities, Individual Entrepreneurs, and Public Organizations** mandates that all corporate entities and changes to ownership (UBOs) be registered in the Unified State Register to achieve legal validity.[124]
- **Tax Code of Ukraine** sets a 18% base corporate tax, reduced to 9% for Diia.City residents (tech/R&D), and a 15% withholding tax on non-resident income. [125]
- **Law of Ukraine on Limited Liability Companies and Additional Liability Companies[126] and Law of Ukraine on Joint Stock Companies[127]** define the corporate governance, capital formation, and shareholder rights for the most common investment vehicles in Ukraine.

Intellectual property regulation and its conditions in defense sector

Intellectual property in Ukraine is a protected proprietary right regulated through a hierarchy of the Constitution, Civil Code, and specialized laws covering inventions, trademarks, and copyrights, supported by international standards like WIPO and TRIPS. While the system aligns with global norms, full integration with EU standards remains a work in progress, facing challenges such as fragmented regulations, undefined legal terms, and inconsistent enforcement. Despite these hurdles, **ongoing legislative reforms aim to increase regulatory predictability and strengthen the practical protection of IP assets.** In late 2025, new amendments addressed IP rights for military-related developments, establishing that the state may claim ownership or restrict the export and licensing of technologies created under government contracts or with military involvement. While rights to inventions created outside official duties remain with the author, vague criteria for proving this status necessitate precise contractual records to avoid ownership disputes. Furthermore, "secret inventions" involving state secrets are subject to confidential filing and strict export controls, which protects critical technology but can limit immediate commercialization. To balance these restrictions, the

[119] See "Ukraine-US Double Taxation Convention", VVR [ua]
[120] See "The Law of Ukraine on International Commercial Arbitration", VVR [ua]
[121] See "Resolution of the National Bank of Ukraine", VVR [ua]
[122] See "Law of Ukraine on Currency and Transactions", VVR [ua]
[123] See "Law of Ukraine on Banks and Banking Activities", VVR [ua]
[124] See "Law on State Registration", VVR [ua]
[125] See "Tax Code of Ukraine", VVR [ua]
[126]See "Law of Ukraine on Limited Liability Companies and Additional Liability Companies", VVR [ua]
[127] See "Law of Ukraine on Joint Stock Companies", VVR [ua]

Defense City regime offers tax incentives and simplified export mechanisms specifically for defense IP assets. However, because defense products often involve a complex mix of IP components, the failure to protect even one element can lead to a loss of product control or competitive blocking. Consequently, while the environment is becoming more investment-friendly, defense-tech projects still require rigorous legal review to navigate the overlap of state security interests and private commercial rights.

Draft Law on Screening of Foreign Direct Investment

In late 2025, Ukraine introduced Draft Laws No. 14062 and No. 14062-1 to establish its first systematic **Foreign Direct Investment (FDI) screening mechanism**. Driven by the need to protect strategic sectors like the defense-industrial complex, energy, and critical infrastructure during the war, these initiatives aim to prevent hostile influence while aligning national legislation with EU standards. The absence of such oversight had previously created a regulatory gap as Ukraine integrated further into the European single market. The two proposals offer different frameworks: Draft Law No. 14062 favors a rigid list of sectors managed by the Ministry of Economy, while Draft Law No. 14062-1 provides a flexible approach delegated to the Cabinet of Ministers with a larger role for the Antimonopoly Committee of Ukraine. While the final legislative architecture remains under parliamentary review in early 2026, the government has already signaled tighter oversight by establishing the **Interagency Commission on the Screening of Foreign Direct Investment** on January 29, 2026, to ensure transparency and analyze high-stakes transactions. Still, the absence of such a mechanism in Ukraine had created a regulatory gap, particularly in the context of integration into the European single market.

At the same time, the two registered draft laws reflect different conceptual approaches:

- **Draft Law No. 14062** establishes a clearly defined and narrow list of sectors (critical infrastructure, strategic resources, defense and security), sets strict threshold triggers for screening, and assigns the primary role to the Ministry of Economy, supported by an advisory commission involving security and intelligence authorities. Non-compliance or illegal investment actions trigger severe penalties.[128]
- **Draft Law No. 14062-1** adopts a more flexible approach. It does not fix the list of sectors in the law itself but delegates their determination to the Cabinet of Ministers (with periodic review). It also proposes a strengthened role for the Antimonopoly Committee of Ukraine and introduces elements of "silent consent," potentially creating a more flexible but less formalized model. The draft focuses on assessing the specific risks that a particular investment may pose to national security, economic stability, and critical infrastructure, taking into account the characteristics of the investor, the target entity, and the structure of the transaction.[129]

The choice of the specific model will have a direct impact on transaction structuring, approval timelines, and the overall investment climate in Ukraine.

Key takeaways

[128] See "Draft law "On Screening of Foreign Direct Investments" dated September 22, 2025, No. 14062", Liga [ua]
[129] See "Draft law "On Screening of Foreign Direct Investments" dated October 7, 2025, No. 14062-1", Liga [ua]

Ukraine's current investment regulations formally provide foreign investors with a wide range of rights, guarantees and dispute resolution tools. For a long-term presence, it may be effective to obtain resident status in the special Defense City zone, which provides tax and institutional incentives. In the case of large-scale production projects, it is advisable to consider the "significant investment" regime, which provides additional guarantees and support.

Due to the state of war investments may be accompanied by licensing requirements, export control regime, special permits to work with technologies or state secrets. Transactions involving the acquisition of control or a significant stake in a company require special attention to the ownership structure and the origin of capital. In the field of export control and defense cooperation, the state is strengthening coordination at the level of interdepartmental bodies while export control policy has been updated. Ukraine is transitioning to an active export model of defense industry development, planning to launch a network of export centers in European countries and scale up the production of Ukrainian technologies abroad (in particular, unmanned systems in Germany and the UK). A defense hub called Defense City is being formed with the involvement of international companies, which provides for various models of cooperation, from localization of production to joint R&D projects.

Ukraine is implementing a systematic mechanism for screening foreign direct investments, which means that the approval of agreements may take longer, an expanded set of documents will need to be submitted, and conditions or restrictions may be imposed.

During martial law, temporary restrictions of currency transactions imposed by the National Bank of Ukraine apply. Repatriation of dividends, repayment of loans, and payment for imports are currently permitted but are subject to established conditions and limits.

In the field of defense technologies, rights to objects created under government contracts or with the participation of the military may be subject to special treatment. Without proper contractual structuring, there is a risk of limiting control over the results of development. Additional specificity is created by the regime of secret inventions, which may restrict the commercialization and export of technologies.

CONCLUSIONS AND RECOMMENDATIONS

Ukraine's defense technology sector has undergone a revolutionary transformation since 2022, evolving from a nascent industry of enthusiasts into one of the world's most **dynamic and battle-hardened innovation ecosystems**. Driven by the urgent need to counter a conventionally advanced adversary and the imperative to minimize human casualties, the market has seen explosive growth in the quantity of both designs and manufacturers across multiple domains, including unmanned ground, aerial, and maritime systems, as well as electronic warfare and artificial intelligence. This rapid, bottom-up innovation cycle, featured by direct feedback from the front lines, allows for **swift adaptation and iteration, a key strategic advantage**.

The core strength of this ecosystem lies in its agility and the **symbiotic relationship between developers, the military, and the state**, facilitated by actors like Brave1. Technological advancements have moved beyond reliance on commercial off-the-shelf components to domestically developed, EW-resistant solutions with increasing levels of autonomy. The principle of using technology to replace human risk is a fundamental driver, starkly contrasting with the adversary's methods and cementing unmanned systems as an indispensable tool of modern warfare.

The sector is now maturing, supported by a **growing infrastructure of state-led grant programs, private venture capital, and accessible government-backed loans**. Furthermore, a strong strategic alignment between the United States and Ukraine, solidified by a ten-year bilateral security agreement and multi-year funding initiatives, provides a durable policy framework that **significantly mitigates political risk for investors.**

While challenges related to scalability, regulatory hurdles, and technological gaps persist, they represent clear **opportunities for targeted investment**. Capital deployed to solve bottlenecks in autonomy, resilient communications, and domestic component manufacturing will not only generate significant returns but also contribute directly to a strategic U.S. interest: fostering a resilient and innovative partner capable of producing battle-proven defense solutions for the entire Euro-Atlantic community.

Recommendations:

1. The primary advantage of Ukraine's market is access to technologies that have moved beyond the prototype stage (TRL 4-6) and have been proven in combat (TRL 7-9). The potential investor should **center due diligence on operational proof**—field testing, end-user feedback from military units, and successful mission logs.
2. A prospective investor should **require a rigorous audit of the Intellectual Property portfolio** to ensure all assets are cleanly held by the company with proper legal assignments. Furthermore, one should verify that protection is actively maintained and enforceable in all key strategic jurisdictions, specifically including Ukraine, the US, and the EU.
3. **Focus on platforms that are now technological priorities**, acting as force multipliers by removing humans from the most dangerous tasks. UGVs for logistics within the "kill zone", drone-hunting AI turrets, and unmanned maritime systems are proven solutions with immediate and scalable demand. Less than 1% of fielded systems are truly autonomous, creating a massive opportunity for **investment in companies developing AI-driven navigation, automatic target recognition, and more autonomous decision-making**

software. These software modules are often platform-agnostic, allowing for integration across UGV, UAV, and USV domains. Along with that, the constant battle against adversary EW has spurred the development of hardened, multi-channel communication systems. Companies specializing in **EW-resistant hardware and "smart EW" software** that can detect and selectively jam threats are critical enablers for all unmanned systems and represent a highly defensible investment.

4. The sector's reliance on Asian components is a recognized vulnerability. **Investing in the localization of critical hardware** — such as microelectronics, electric motors, and sensors — offers a long-term strategic plan to build a resilient and vertically integrated supply chain, with the potential for both domestic and future export revenue.
5. Traditional venture capital models must be adapted to the realities of Ukraine's market. By **aligning investment instruments — grants, equity, and venture debt — with specific TRL stages**, investors can match capital structures to the technical and operational realities of defense technology development. Moreover, standard processes may differ in Ukraine due to data sensitivity in ongoing war conditions.
6. While a wartime ban on arms exports currently limits revenue, the post-war export potential for these battle-proven systems is enormous. Therefore, it is prospective to **invest in companies with NATO codifications and standards** whose products have applications for U.S. and allied militaries. Early investment now is a ground-floor opportunity to capture the upside when Ukraine becomes a major global defense exporter.
7. **Direct investment not only into hardware but also into enabling infrastructure**, such as specialized training schools, R&D centers, and testing grounds. Supporting the entire ecosystem is crucial for sustainable growth and long-term success.

In summary, Ukraine has successfully created a cauldron for defense innovation, proving its ability to develop and deploy cutting-edge, battle-proven technologies at remarkable speed. The challenge now is to transition from this reactive, crisis-driven model to a sustainable, scalable, and fully integrated defense industrial base capable of securing a long-term strategic advantage.