AB3TECH — SNAKE ISLAND INSTITUTE

Defense TECH MONTHLY

Edition 8.0

IN THIS EDITION:

SATELLITE WAR

Starlink Terminals on Russian Drones — implications for Ukraine

January 2026

TABLE OF CONTENTS

NORTHEAST (SUMY–VOVCHANSK–KUPIANSK–LYMAN):

Fighting continued along the **Vovchansk** axis, where Russian forces attempted to outflank the city from Starytsia and Hrafske, advancing near Synelnykove and Tsehelne toward Symynivka and Lyman (Kharkiv Oblast), while assault groups also pushed into Vilcha. Russian units also attempted advances toward Dehtiarne and Kruhle. Building on the December counterattack, Ukrainian forces continued clearing remaining enemy personnel in **Kupiansk**. South of the city, Russian forces secured Lozova and attempted to advance toward Nova Kruhliakivka. North of **Lyman** (Donetsk Oblast), Russian units advanced near Shandryholove toward Novoselivka and Drobysheve, while pressure continued along the Yampil–Dibrova axis, with probing attacks toward **Lyman**. Further Russian advances were reported near Hrabovske (Sumy Oblast).

EAST (SIVERSK–KRAMATORSK–CHASIV YAR–KOSTIANTYNIVKA–DOBROPILLIA–POKROVSK):

Russian forces continued advancing near **Siversk**, with fighting reported around Sviato-Pokrovske, Pereizne, Fedorivka, and Vasiukivka, alongside pressure toward Rizhnykivka. In the **Kramatorsk–Sloviansk** direction, Russian units advanced near Vasiukivka, Minkivka, Markove, Maiske, and nearby settlements toward Nykyforivka and Pryvillia. Pressure on **Chasiv Yar** intensified, with Russian forces moving toward Viroluibivka and Mykolaivka. Russian activity continued against **Kostiantynivka** and surrounding settlements, with probing actions reported near Predtechyne, Oleksandro-Shultyne, Ivanopillia, Kleban-Byk, and Rusyn Yar, toward Berestok and Stepanivka. Russian forces also continued efforts to develop an offensive toward **Dobropillia**, advancing toward Sofiivka, Shakhove, Nove Shakhove, Ivanivka, and Fedorivka. Heavy fighting persisted across the **Pokrovsk–Myrnohrad** agglomeration, where Russian forces expanded control across much of the urban area and advanced near Novoekonomichne, Svitle, Rivne, Rodynske, and Novopavlivka, with a focus on disrupting logistics routes from Hryshyne.

SOUTH (HULIAIPOLE–STEPNOHIRSK):

Intense fighting continued in the western part of **Huliaipole**, where Russian forces pushed Ukrainian units out of parts of the central area and advanced toward Zelene, Sviatopetrivka, Staroukrainka, and Zaliznychne. Further advances were reported near Danylivka, Yehorivka, Pershotravneve, Solodke, Pryluky, and Varvarivka, with pressure extending toward Ostapivske, Nechaivka, and Nove Zaporizhzhia. The situation around **Stepnohirsk** also deteriorated, as Russian forces attempted infiltration operations in the settlement and in nearby Prymorske, Malokaterynivka, Richne, Lukianivske, and Pavlivka.

FROM FIREPOWER TO CAPTURE: MACHINE-GUN-ARMED UGV TAKES POWS

In January, video footage showed **three Russian servicemen surrendering to a Ukrainian machine-gun-armed UGV**. Supported by UAVs, UGV operators located the enemy personnel, with the footage showing the soldiers leaving cover and surrendering with their hands raised. This marked the **first confirmed case of a machine-gun-equipped UGV taking prisoners of war**. The incident followed an earlier case in June 2025, when **Russian personnel surrendered to Ukrainian kamikaze UGVs** after being threatened with imminent detonation.

Unmanned ground systems are becoming increasingly integrated into combat operations, expanding their role as first-contact platforms, reducing risks to personnel, and further complicating operational planning for both sides.

Footage From the UGV's Onboard Camera Showing Russian Personnel Leaving Cover. Source: DevDroid

FROM SATELLITES TO SADDLES: RUSSIA MOUNTS STARLINK ON HORSES

Recent imagery shows **Russian forces mounting Starlink satellite terminals on horses**, likely to maintain covert communications in areas where infrastructure has been damaged or is absent. Animals fitted with welded frames carrying flat-panel terminals and cameras appear to be used as mobile relay nodes for communications and reconnaissance. This setup enables frontline units to **transmit video and positional data to commanders in near real time**.

The adaptation reflects an attempt to circumvent sustained attacks on Russian communications infrastructure and to compensate for the loss or unavailability of vehicles by employing low-tech transport platforms to sustain high-tech connectivity.

Starlink Terminal Mounted on Horseback. Source: Special Kherson Cat

GERAN-5: RUSSIA'S HIGH-SPEED SHIFT WITHIN THE GERAN FAMILY

In early 2026, **Russian forces reportedly employed the Geran-5 strike UAV for the first time**. Compared to the Geran-3 and Geran-4, the Geran-5 operates at **significantly higher speeds and altitudes**, placing it closer in role and performance to a long-range cruise missile than to a loitering munition. Its aerodynamic configuration — a straight wing, cylindrical fuselage, and twin-fin tail — simplifies manufacturing and supports higher production throughput.

Parameter	"Geran-2"	"Geran-3"	"Geran-4"	"Geran-5"
Wingspan, m	3	3	3	3.2
Length, m	3.5	3.5	3.5	6.5
Engine Type	ICE	Turbojet	Turbojet, 160 kgf thrust	Turbojet, 200 kgf thrust
Takeoff Weight, kg	245	300–350	450	850
Warhead Weight, kg	50–90	50–9	≥50	90
Cruise Speed, km/h	180	280–330	350–500	450–600
Range, km	1,200	600–3,500	850	950
Operating Altitude, m	60–4,000	100–3,000	100–5,000	up to 6,000
Endurance, hours	up to 7	2	2.5	2

Source: Defense Intelligence of Ukraine

The Geran-5 uses a component set largely consistent with earlier Geran variants, including a flight controller unit, the SADRA/MINSOO inertial navigation system, the Kometa-M12 satellite navigation system with a 12-element CRP antenna, a Tracker V3 telemetry transmission system based on a Raspberry Pi microcomputer and 3G/LTE modems, and an Xingkai Tech XK-F358 mesh modem.

As with earlier Geran variants, the platform cannot be considered an indigenous Russian design. Its airframe and onboard systems demonstrate clear structural and technological **continuity with Iran's Karrar UAV**.

Available information indicates that Russia is also assessing air-launch options for the Geran-5, including potential **deployment from Su-25 aircraft**, in order to extend range by approximately 100 km while reducing operational costs. The integration of R-73 air-to-air missiles is reportedly being examined as a counter-aviation measure.

Downed Russian Geran-5. Source: Defense Intelligence of Ukraine

Top: Iranian Karrar UAV. Bottom: Geran-5. Source: VictoryDrones

At its current speed, the Geran-5 remains largely inaccessible to helicopters, interceptor drones, and mobile fire groups, requiring refinements to interception tactics, adjustments to radar coverage, and shorter reaction timelines. Overall, the system represents another Russian attempt to field a low-cost cruise-missile analogue designed to bypass Ukraine's existing counter-Shahed defenses.

MANPADS IN THE AIR: RUSSIA ADAPTS GERAN-2 UAVS TO HUNT AIRCRAFT

Following earlier attempts to mount R-60 air-to-air missiles on Shahed-type UAVs, Russia has continued experimenting with aerial engagement concepts by **integrating a Verba MANPADS onto its Geran-2 platform.**

Upon detecting an aerial target, the operator sequentially activates two servo drives: the first initiates the chemical battery and punctures the nitrogen cylinder to begin cooling the MANPADS seeker head, while the second opens the protective cover once the seeker reaches its operating temperature. The missile, with an engagement range of approximately **6–6.5 km**, is configured for automatic launch, with the trigger permanently depressed using cable ties, enabling immediate firing once target lock is achieved.

Operator control is enabled through a Chinese-made Honpho TS130C-01 optical camera and an Xingkai Tech XK-F358 mesh modem. Employment of the system remains constrained by communications range, with available estimates indicating that **reliable control is unlikely beyond approximately 150 km from the frontline**.

The **configuration appears clearly experimental**, featuring improvised cable routing and exposed auxiliary components rather than a production-grade integration. In addition, the cost of a single Verba MANPADS exceeds that of the Geran-2 airframe itself, undermining the economic rationale of the concept. At the same time, the effort reflects Russia's continued **attempts to adapt its unmanned strike systems for counter-aviation roles**, reinforcing the need for a flexible, layered, and resilient air-defense architecture on the Ukrainian side.

Downed Russian Geran-2 UAV With Integrated Verba MANPADS. Source: serhii_flash

UAV "Geran-2" (Series "Э", Equipped With the Verba MANPADS). Source: War & Sanctions

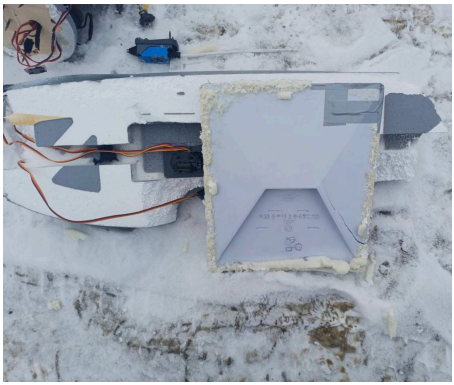
FROM MOLNIYA TO SHAHED: RUSSIA EXPANDS STARLINK-CONTROLLED UAV OPERATIONS

In mid-January, **reports documented the first confirmed case of a Russian BM-35 UAV being controlled via Starlink**, marking the first publicly reported expansion of Starlink integration **beyond the Molniya-series platforms**.

By late January, however, **footage from a Russian Shahed-type strike UAV showed automatic target acquisition and manual terminal guidance** via a live video feed, without nearby UAVs forming a **mesh radio network**, indicating

that Starlink connectivity had already been extended to Shahed platforms beyond the experimental stage. Some sources further report that similar integrations have begun to appear on other **kamikaze and reconnaissance UAVs**.

The use of Starlink-enabled drones allows **real-time long-range control, enabling in-flight retargeting, lower-altitude flight profiles, and increased maneuverability**, while significantly reducing vulnerability to electronic warfare. Although **some sources suggest** that a mass transition to Starlink across Russia's entire UAV fleet remains unlikely in the near term due to financial and technological constraints, Russia's consistent use of Starlink-enabled drones creates new challenges for the Ukrainian military. These include the need to **counter platforms with higher target-engagement efficiency** and reduced interceptability, as well as to **address Russia's ability to procure Starlink terminals** through shell companies and employ them on Ukrainian territory.



Downed BM-35 UAV With Integrated Starlink. Source: serhii_flash

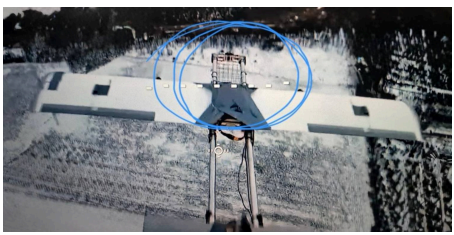
MOLNIYA UAV ANTI-TANK MINE: FIRST COMBAT APPLICATION DEPLOYED

In the **December issue of Defense Tech Monthly**, we noted the emergence of a Molniya configuration adapted for **remote anti-personnel mine delivery**, although no confirmed combat use had been reported at the time. At the beginning of 2026, however, the first indicators of operational use of this modification were observed.

In late January, sources reported the use of **Molniya UAVs capable of carrying PFM-1 ("Lepestok") anti-personnel mines.**

Later in the month, published footage showed a Molniya UAV dropping an **anti-tank mine in Kostiantynivka**, marking a clear expansion of the platform's operational role.

The aerial delivery method of mines significantly complicates battlefield logistics and casualty evacuation. Remotely delivered mines along Ukrainian positions and their approaches directly constrain assault operations, **as observed in January on the Huliaipole axis**, where Russian forces **deployed mines by unmanned platforms to slow Ukrainian advances**. Large-scale remote mine deployment also increases long-term risks to civilians and complicates post-combat clearance efforts.



Molniya UAV With "Basket" for Anti-Personnel Mines. Source: serhii_flash

Molniya UAV Delivers Anti-Tank Mine in Kostiantynivka. Source: serhii_flash

JANUARY DEEP STRIKE CAMPAIGN: SUSTAINED PRESSURE ACROSS RUSSIA'S WAR ECONOMY

Ukraine continued its deep-strike campaign against Russia's oil and energy infrastructure, military-industrial facilities, and the supporting systems underpinning ongoing military operations. January 2026 marked a continuation of this approach, with a noticeably elevated tempo during the first half of the month.

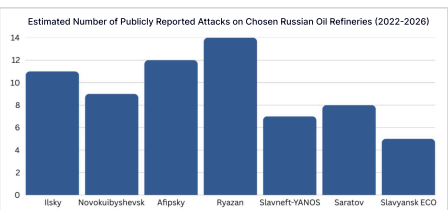
According to figures released by the Russian Ministry of Defense, around **1,400 Ukrainian drones were intercepted during the first six days of 2026** while attempting to strike infrastructure targets that sustain the war deep inside Russia.

OIL & ENERGY: REFINERY STRIKE CAMPAIGN CONTINUES

According to multiple sources, Ukraine struck at least 7 oil refineries inside Russia in January, while 11 refinery strikes were confirmed in December 2025.

January 1	Ilskyi Oil Refinery
January 2	Novokuibyshevsk Oil Refinery
January 2-3	Afipsky Oil Refinery
January 4	Ryazan Oil Refinery
January 5-6	Slavneft–YANOS Oil Refinery
January 18-19	Saratov Oil Refinery
January 21	Afipsky Oil Refinery (second engagement)
January 26	Slavyansk ECO Oil Refinery

Ukraine's refinery strikes follow a **deliberate re-engagement pattern designed to prevent damaged facilities from returning to stable operability**. Repeated attacks during repair and restart phases extend shutdown periods well beyond normal maintenance cycles. Under sanctions that restrict access to Western equipment and spare parts, **Russian operators face prolonged repair timelines** and are increasingly forced to cannibalize already-installed components to restore only partial functionality.



Source: robert_magyar, exilenova_plus & Verstka

Beyond long-term production disruption, Ukraine sustained extensive strikes against fuel depots and oil-handling infrastructure to eliminate immediate reserves and degrade distribution networks.

Confirmed engagements in January include, but are not limited to:

Facility	Date	Assessment
The Northern Commodity Park (Almetyevsk, Republic of Tatarstan)	January 1	PJSC Tatneft facility used for crude oil collection, preparation, and storage prior to transportation; located ~1,400 km from Ukraine-controlled territory.
Gerkon Plus Oil Depot (Lipetsk Oblast)	January 6	Regional fuel depot supplying Lipetsk, Tambov, and Voronezh regions.
Oskolneftesnab Oil Depot (Stary Oskol, Belgorod Oblast)	January 7	Fuel depot supporting Russian forces; one RVS-1000 tank destroyed and six damaged.
Zhutovskaya Oil Depot (Volgograd Oblast)	January 10	Facility supplying fuel to Russian invasion forces.
Penzanefteprodukt Oil Depot (Penza Oblast)	January 23	At least two storage tanks were reportedly damaged; smoke plumes extended ~1 km.
Khokholsky Oil Depot (Voronezh Oblast)	January 28	Ignition of petroleum products confirmed, with dense smoke observed.

In parallel, January saw Ukraine build on the momentum gained during its Caspian Sea **campaign against offshore oil infrastructure**, first initiated in December 2025.

On January 11, one month after the initial strikes, **Ukrainian forces conducted follow-on strikes against the Filanovsky, Korchagin, and Valeriy Grayfer offshore platforms**.

On January 7, **unidentified drones struck the Russian shadow-fleet oil tanker ELBUS** in the Black Sea while it was en route to Novorossiysk to load oil. Follow-on strikes were conducted on January 13, when Greece-managed tankers Delta Harmony, Delta Supreme, Freud, and Matilda were approaching Russian coastal terminals. **Delta Harmony and Matilda were reportedly hit by unidentified drones,** highlighting continued pressure on maritime oil logistics.

Filanovsky Platform (~900 km From Ukrainian-Controlled Territory) Moments Before Impact. Source: Special Operations Force

INDUSTRIAL FACILITIES: DEGRADING THE ARSENAL BEHIND THE FRONT

Ukraine's campaign to degrade Russia's military-economic capacity extended beyond oil and energy infrastructure in January, with Ukrainian forces systematically **targeting industrial facilities directly involved in the production and sustainment of weapons systems.**

On January 4, **Ukrainian strikes hit the Energia plant in Lipetsk Oblast**, a key defense manufacturer producing power sources for Iskander missiles, naval cruise missiles, and guidance modules.

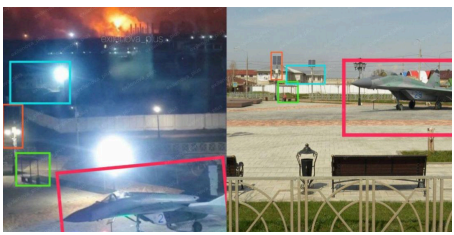
Between January 5–6, Ukrainian forces targeted the **Kirovo-Chepetsk chemical complex** in Kirov Oblast and the **Dorogobuzh chemical plant** in Smolensk Oblast, both major producers of nitric acid and nitrogen compounds critical for explosives manufacturing. On January 6, explosions were also reported at the **Sterlitamak petrochemical plant** in Bashkortostan, a producer of synthetic rubbers and aviation-kerosene components used in military and aviation applications.

On January 7, **a fire broke out at Moscow's ODK-Salyut facility**, which is involved in the production and maintenance of aviation engines for both civilian and military aircraft.

On January 13, domestically produced Neptune cruise missiles **struck the Atlant Aero plant in Taganrog**, a manufacturer of Molniya-type strike-reconnaissance UAVs and components for Orion systems, directly degrading Russia's UAV production and sustainment chain.

Follow-on strikes on January 14 and 16 hit major **chemical facilities in Stavropol Krai** and **Voskresensk**, both critical suppliers of nitric and sulfuric acids used in explosives manufacturing and aviation support, reinforcing Ukraine's focus on degrading upstream industrial inputs that sustain Russia's war effort.

Fire Broke Out After Attack on Atlant Aero Plant. Source: exilenova_plus



Targeted Nevinnomyssk Azot Plant in Stavropol Krai. Source: exilenova_plus

POWER GENERATION: ENERGY AS A PRESSURE POINT

In January, Ukrainian forces conducted a focused campaign against Russian thermal power generation and electricity infrastructure, with a particular emphasis on Belgorod and its surrounding energy nodes.

On January 9, HIMARS strikes hit **the Luch thermal power plant, the Belgorodskaya thermal power plant, and the 330 kV Belgorod substation**, causing fires, destroying transformers, and triggering widespread power outages across the city. On January 20, **Ukrainian forces struck the Michurinskaya thermal power plant**, a smaller facility supplying electricity to industrial sites. This was followed by a **repeat HIMARS strike on January 24 against the Belgorodskaya TPP**, again leaving parts of Belgorod without electricity and heating.

The repeated targeting of these infrastructure systems reflects **Ukraine's intent to force Russia to divert financial, technical, and human resources toward emergency repairs** and grid stabilization rather than sustaining frontline operations. At the same time, Belgorod functions as a key rear-area hub for Russian activity on the northeastern axis, and the sustained degradation of its power infrastructure complicates logistics, disrupts support functions, and degrades command-and-control processes that are essential for ongoing combat operations.

Moment of the Second Attack on the Belgorodskaya TPP. Source: exilenova_plus

INTERCEPTING THE SHADOWS: U.S. CRACKDOWN ON VENEZUELAN-RUSSIAN OIL FLOWS

In January 2026, the United States intensified efforts to constrain Venezuela's oil exports and enforce a stricter naval blockade against sanctioned shipping. U.S. military and Coast Guard forces seized a total of **7 tankers suspected of facilitating Russian sanctions evasion linked to Venezuelan oil exports**. This total includes 5 vessels intercepted in January, as well as the **Skipper (formerly Adisa)** and **Centuries** tankers, seized earlier on December 10 and December 20, respectively.

Notably, Bella 1—later renamed Marinera and re-registered in a Russian port in an apparent attempt to evade the U.S. blockade—appears to represent the **first seizure in recent years of a Russian-flagged vessel by U.S. forces**.

Coordinated actions by Ukraine and its partners have already **led to over 20% of the Russian shadow fleet's tankers ceasing operations**.

Combined with sustained strike pressure, it **reduces Russia's annual seaborne oil export revenues by at least $30 billion**, limiting resources available to sustain the war in Ukraine.

Name	Date	Seizure location
Marinera (formerly Bella 1)	January 7	North Atlantic (between Iceland & Scotland)
M Sophia	January 7	Caribbean Sea
Olina (formerly Minerva M)	January 9	Caribbean Sea
Galileo (formerly Veronika)	January 15	Caribbean Sea
Sagitta	January 20	Caribbean Sea

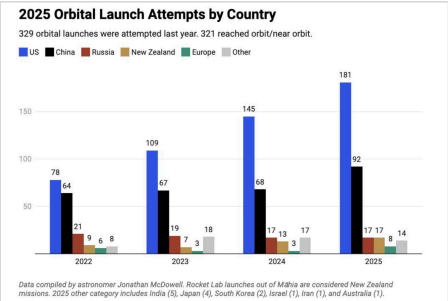
CHINA SCALES FOR SPACE, RUSSIA STRUGGLES TO KEEP PACE

China's space sector continues to **accelerate its drive to become a major space power**. In 2025, China conducted **92 orbital launches**, up from 68 in 2024, setting a new national record. State-owned launch providers continue to dominate activity, accounting for 84 out of 100 launches. By comparison, in the United States, 160 out of 180 launches were conducted by a single private operator (SpaceX). At the same time, Beijing is actively pushing private firms to develop reusable rockets to reduce launch costs and increase deployment rates.

Although Chinese private companies remain behind their U.S. counterparts, recent tests of reusable launch vehicles indicate a shift in leadership dynamics. If successful, these systems would enable **faster expansion of low-Earth-orbit satellite constellations**. Two such constellations are planned: **Guowang (approximately 13,000 satellites) and Thousand Sails (approximately 15,000 satellites)**. At present, both constellations field around 100 satellites each, while Starlink operates more than 9,000.

These satellite networks are **formally presented as civilian infrastructure** but would also provide military utility, including resilient communications, improved situational awareness, and reduced reliance on foreign systems.

Meanwhile, Russia continues to **lose ground in space activity**, conducting 17 launches in 2025, unchanged from 2024, marking a second consecutive year of historically low performance outside the pandemic period. Launch activity has not been this low since 1961, when the Soviet Union conducted nine launches, before peaking at 99 launches in 1982.



2025 Orbital Launch Attempts by Country. Source: PayloadPro

In 2025, **Russia launched 17 systems, including**:

- Soyuz 2.1b – 6
- Soyuz 2.1a – 6
- Angara-1.2 – 3
- Angara-A5 – 1
- Soyuz 2.1v –1

The fact that roughly **three-quarters of Russia's launches relied on Soyuz variants (first launched in 1966–1967)** highlights the country's limited ability to field newer launch systems. Russia's continued dependence on the Soyuz systems likely reflects financial constraints associated with the war in Ukraine, with state resources increasingly redirected toward immediate military priorities at the expense of long-term space-sector modernization.

STARLINK UNDER FIRE: IRAN'S FIELD TEST OF RUSSIAN SYSTEMS

In January 2026, amid a nationwide communications blackout, **Iran conducted a coordinated electronic-warfare operation targeting Starlink terminals** and disrupting GPS signals, reportedly using Russian-supplied systems. Multiple sources indicate Tehran field-tested **an experimental Russian platform, likely "Kalinka," to interfere with Starlink terminals**. Additional reporting points to the use of **"Tobol," capable of geolocating enemy ground stations with high precision** and operating in conjunction with "Tirada-2" to generate layered jamming effects. Alternative assessments suggest **the involvement of "Murmansk-BN" and possibly "Cobra V8,"** a reverse-engineered analogue of Russia's "Krasukha-4."

With an estimated **40,000–50,000 Starlink terminals active nationwide**, Iranian forces reportedly employed broadband noise and swept-frequency jamming, raising the noise floor sufficiently to disable most commercial services, while limited asynchronous messaging remained intermittently available.

Against conventional point-to-point links or fixed geostationary satellites, **this approach can achieve complete denial**. The geometry favors the jammer: signals arriving from distant satellites are already attenuated, allowing a nearby ground-based system to overwhelm the receiver with comparatively modest power output.

In the case of Starlink, however, **satellites move rapidly across the sky and remain in view only briefly before hand-off, continuously reshaping the interference geometry** and quickly misaligning stationary jammers. Starlink terminals further mitigate interference through adaptive antennas that concentrate reception toward the serving satellite while reducing sensitivity toward interference sources.

This dynamic explains the observed **30 to 80 percent packet loss rather than full service denial** and is consistent with conclusions advanced in late 2025 **by researchers at the Beijing Institute of Technology**, who modeled Starlink orbital dynamics over a Taiwan-sized area and assessed that **ground-based jamming alone cannot achieve complete denial**–instead proposing the creation of an "electromagnetic shield."

Operationally, the Iranian case highlights a **critical risk for Ukraine**. Given the Ukrainian Armed Forces' **reliance on satellite-based connectivity, the potential deployment of Iran-validated EW systems could severely degrade command-and-control**. At the same time, expanding technical cooperation between Russia, Iran, and China signals a sustained, coordinated effort to identify and exploit vulnerabilities in Western-developed technology—an effort likely to intensify further.

AI AT THE EDGE: DATAROOM FOR AIR-DEFENSE TRAINING

Ukraine has introduced the Brave1 Dataroom, a secure digital environment designed to accelerate the **development of AI-enabled air-defense capabilities using real battlefield data**. The initiative supports the training of AI and computer-vision models to bridge the gap between theoretical model performance and frontline operational reality, where air-defense systems must operate reliably under degraded conditions, including adverse weather, limited visibility, night operations, and mixed target sets.

The platform aggregates visual and thermal datasets, with plans to expand the collection over time, enabling developers **to train and validate AI models against scenarios that closely reflect combat** employment. It supports AI and computer-vision applications across the air-defense cycle, including target detection, identification, tracking, and interception, with a particular focus on countering strike UAVs, including Shahed-type drones. As a result, the approach is expected to improve air-defense effectiveness while increasing automation reduces operator workload.

WEAPONS FOR SALE: RUSSIA'S FRONT-LINE ARMS PIPELINE

In January 2026, Ukrainian hackers exposed a weapons-smuggling network involving Russian military personnel and soldiers linked to the Chechen-affiliated Vostok-Akhmat battalion. According to the investigation, temporarily **occupied Crimea is being used as a transit hub for siphoning weapons from the frontline**, with arms subsequently trafficked to black markets in Russia, Europe, Western Asia, and Africa, including through logistics channels **linked to Russia's shadow tanker fleet**.

Analysis of compromised accounts belonging to multiple Russian officers indicates that Russian **military checkpoints along key routes from the front to Crimea systematically facilitate the movement of suspicious cargo**, often without inspection or in exchange for bribes.

Intercepted communications further suggest that routine practices, such as **overstating combat losses** or sending personnel into assaults without standard equipment, **create additional, unregistered weapons stocks**, which are then diverted into the smuggling network.

In a parallel operation, hackers reportedly used a compromised Russian officer's identity to deceive administrators of a pro-war Telegram channel into redirecting funds from a 291st Regiment support campaign to Ukraine's Special Operations Forces.

CYBER PRESSURE CAMPAIGN: RUSSIA PROBES POLAND'S POWER GRID

In January, it emerged that Russia, as part of its ongoing cyber campaign against energy infrastructure, had carried out a series of cyberattacks against Poland's power grid in late December 2025. The most serious of these attempts reportedly targeted Poland's energy system to **trigger a large-scale power outage affecting civilian populations**. Adverse winter weather conditions would have significantly amplified the impact had the attack succeeded.

Poland's Minister of Energy confirmed the attempted intrusion and stated that the attack was successfully repelled, noting a high level of preparedness among national institutions. Separately, the Minister of Digital Affairs reported that, during 2025, Russian military intelligence had **tripled the resources allocated to cyber operations targeting Poland's critical infrastructure**.

According to the European Commission, **Russia conducts daily cyber operations across Europe aimed at the energy, financial, and healthcare** sectors as part of a broader strategy of societal destabilization. The episode underscores the persistent vulnerability of critical infrastructure to sustained and coordinated cyber sabotage extends well beyond Ukraine.

FROM CONSUMER TO PRODUCER: UKRAINE'S DEFENSE INDUSTRY

Driven by a shift from a centralized, state-dominated model to a decentralized ecosystem built around private initiative, rapid iteration, and bottom-up innovation, **Ukraine's defense industry expanded from approximately $1 billion in 2022 to $35 billion in 2025**, with some projections indicating that it could reach **$50 billion by the end of 2026**.

Ukraine's domestic defense industry now supplies 60% of the Armed Forces' weapons, significantly reducing dependence on foreign procurement.

In 2025, **the number of codified Ukrainian weapons and military systems reached**:

- UAVs: over 500
- Ammunition: over 270
- Unarmored vehicles: over 50
- Small arms: 13
- Armored vehicles: 11

According to multiple sources, investment in Ukrainian defense technology increased from **$1.1-6.7 million in 2023 to $28.7-59 million in 2024 and reached $105.2-129 million in 2025**, accounting for nearly one-third of all early-stage defense-technology investment in Europe (including the United Kingdom). **Approximately 30% of transactions remain undisclosed**, suggesting that actual investment levels are likely higher.

In 2025 and early 2026, investment has been concentrated in the following areas:

- UAVs and UGVs
- Counter-UAV systems
- EW and jam-resistant communications
- AI-driven targeting, autonomy, and battlefield analytics
- Sensors & navigation (GPS-denied)
- Software & hardware

Ukrainian combat experience and battle-validated technologies are attracting increasing interest from international investors and partners. As the domestic defense technology sector matures, **average pre-seed deal sizes rose from $215,000 in 2023 to $718,000 in 2025, while seed-stage investments increased from $1.8 million in 2024 to $2.9 million in 2025**. In parallel, **twenty-five foreign companies are at various stages of localizing production in Ukraine**, positioning the country as one of Europe's most dynamic and attractive defense-industry investment environments.

Having evolved from a net consumer of military technology into a driver of battlefield innovation and a live laboratory for modern warfare, **Ukraine may begin securing its first export contracts from the second half of 2026**, with UAVs, naval drones, and artillery systems among the most likely categories. The **launch of Defence City in January 2026**, a special legal regime for defense-industry enterprises, is expected to support this transition by enabling production scaling, introducing targeted tax incentives and relocation mechanisms, simplifying customs procedures, expanding access to international markets, limiting the disclosure of sensitive data, and reducing regulatory and legal exposure for selected categories of activity.

In the **August issue of Defense Tech Monthly**, we highlighted the rapid emergence of a parallel ecosystem of **military-built defense technologies developed inside frontline military R&D laboratories** and unit-level innovation cells. Despite their direct operational relevance and fast iteration cycles, this segment of the innovation pipeline **remains largely underfunded** by both the public and private sectors, creating a growing risk that high-potential battlefield-developed solutions will fail to progress beyond the prototyping stage.

Company	Sector	Round size	Stage	Disclosed Investors
2025				
Aeromotors	Hardware	$550,000	Seed*	Front Ventures
Aetos Space Labs	c-UAS	–	Pre-seed*	Oppenheimer Acceleration
Anvarix Technologies	c-UAS	–	Pre-seed*	Oppenheimer Acceleration
Ark Robotics	UGV	$1,200,000 / $7,500,000	Pre-seed / Seed	– / Inflection
BabAI	Software	–	Pre-seed	Oppenheimer Acceleration Fund
Black Forest Systems	UAV	–	Pre-seed*	Double Tap Investments
Blue Arrow	Software	–	Pre-seed	Big Defence
Deftak	Ammunition	$700,000*	Seed	Darkstar
Drill App	Software	$100,000	Pre-seed	Undisclosed angels
Dropla Tech	Demining	$2,800,000*	Seed	Export and Investment Fund, Maj Invest Equity
Falcons	Navigation	–	Seed	Green Flag Ventures
Frontline	Robotic systems	–	Seed*	Nezlamni, Quantum Systems
Griselda	Autonomy	$600,000	Pre-seed	Double Tap Investments
Hard Cat Drones	UMV	–	Pre-seed	Double Tap Investments
Himera	Electro-magnetic Spectrum	$375,000 / $2,500,000	– / Seed	United Angels Network / Green Flag Ventures
Huless	UAV	$1,000,000	–	–
M-Fly	Hardware	$1,300,000	Pre-seed	Resist.UA, MITS Capital, Freedom Fund
MARA Drone	UAV	$100,000	Pre-seed	Oppenheimer Acceleration Fund
Maxon	c-UAS	$350,000	Pre-seed	Freedom Fund, Defender Ventures
Norda Dynamics	Autonomy	$1,000,000 / $150,000	Seed / –	Varangians / Angel One Fund
Odd Systems	UAV	–	–	Terma Group
Offset Labs	Autonomy	$700,000*	Pre-seed	Archangel Ventures
OSIRIS AI	Software	–	Pre-seed*	–
PanoptesAI	Autonomy	$125,000	Pre-seed	Oppenheimer Acceleration Fund
PZL Defence	UAV	$108,000*	–	Unimot Group
Rightspot.AI	Navigation	–	Pre-seed	Oppenheimer Acceleration Fund
Scopa Industries	Hardware	–	Pre-seed	Oppenheimer Acceleration Fund
Skyeton	UAV	$10,436,300	Series A	–
Sky Spy	Electro-magnetic Spectrum	$1,600,000	Pre-seed	Freedom Fund, Expeditions
Swarmer	Electro-magnetic Spectrum	$500,000 / $15,000,000	– / Series A	Oppenheimer Syndicate / Broadband Capital Investments, R-G.AI, D3 Ventures, Green Flag Ventures, Radius Capital, Network VC
Teletactica	Electro-magnetic Spectrum	$1,500,000	Seed	MITS Capital, Green Flag Ventures
Tencore	UAV	$3,740,000	Pre-seed	MITS Capital
The Fourth Law	Autonomy	–	Seed	Double Tap Investments, 1991 Ventures
Thermopylae	c-UAS	$1,600,000	Pre-seed	Naval Ravikant, UA1, Norgard Capital
Trypillian	UAV	$5,000,000	Seed	Angel
UA Damage	Demining	$400,000	Pre-seed*	Freedom Fund
VYTACH	Navigation	–	Seed	2112 Holding
Zvook	Hardware	$226,000	Pre-seed	–
January 2026				
Farsight Vision & Crystal-Space	Autonomy	$1,500,000	–	Applied Research Programme
Sky Hunter	Software	–	Pre-seed	Front Ventures, Hede Capital Partners

Source: Scroll, AVentures Capital & UCDI (estimated)*

SOURCES

- Army Inform. “DIU: New Geran modification carries both a MANPADS and a warhead simultaneously”. Army Inform, 2026. Link
- Army Inform. “Ukraine’s defense industry capabilities have increased 35-fold during the full-scale war — Ministry of Defense”. Army Inform, 2025. Link
- AVentures Capital. “Dealbook of Ukraine — 2026 Edition | Aventures Capital”. AVentures Capital, 2026. Link
- BBC News. “US seizes second oil tanker off Venezuela's coast”. BBC, 2025. Link
- BBC News. “US seizes two 'shadow fleet' tankers linked to Venezuelan oil”. BBC, 2026. Link
- Comments.ua. “Найбільша небезпека модернізованих 'Шахедів' із ПЗРК: що це змінює у війні”. Comments.ua, 2026. Link
- Connectivity Technology. “China’s growing constellations ambitions”. Connectivity Technology, 2025. Link
- Dialog.ua. “В Москве вспыхнул стратегический завод, связанный с военной авиацией РФ”. Dialog.ua, 2026. Link
- Digital State Ukraine. “Ukraine launches Defence City — a new special regime for scaling defense production”. Digital State Ukraine, 2026. Link
- DOU. “В Україні запустили платформу для тренування штучного інтелекту в ППО”. DOU, 2026. Link
- DW. “Дрон атакував у Чорному морі танкер Elbus, що прямував до Росії”. DW, 2026. Link
- DW. “Умеров: контракти на експорт зброї з України будуть з другої половини 2026 року”. DW, 2025. Link
- Euromaidan Press. “First battlefield capitulation to robots: Ukrainian drones force Russian surrender and seize fortified position (video)”. Euromaidan Press, 2025. Link
- Euronews Next. “Iran could be blocking Starlink during internet blackout with methods similar to Russia”. Euronews Next, 2026. Link
- Foreign Policy. “How Russia Is Supporting Iran’s Repression of Protests”. Foreign Policy, 2026. Link
- gCaptain. “U.S. Seizure of Shadow Fleet Tanker ‘Skipper’ Ends Years-Long Sanctions-Evasion Run”. gCaptain, 2025. Link
- Ill Defined Space. “The Ill-Defined Space Global Orbital Launch Summary 2025”. Ill Defined Space, 2025. Link
- Inform.zp.ua. “Штурми, авиабомбы и минирование: что происходит на Гуляйпольском направлении”. Inform.zp.ua, 2026. Link
- InformNapalm. ““Можемо хоч ядерку провезти”: як офіцери 291-го полку ЗС РФ і «Восток-Ахмат» налагодили контрабанду зброї через Крим”. InformNapalm, 2026. Link
- Kyiv Independent. “Ukraine hits Russian drilling platforms in Caspian Sea, military reports”. Kyiv Independent, 2026. Link
- Militarnyi. “Безпілотники атакували підприємства у російській Пензі та Стерлітамаку”. Militarnyi, 2026. Link
- Militarnyi. “В ніч на 1 січня у Росії від ударів дронів запалали Північний товарний парк, НПЗ та нафтобаза”. Militarnyi, 2026. Link
- Ministry of Defence of Ukraine. “Denys Shmyhal: Already 25 foreign defense companies are localizing production in Ukraine”. Ministry of Defence of Ukraine, 2026. Link
- Ministry of Foreign Affairs of the Russian Federation. “Statement by the Ministry of Foreign Affairs of the Russian Federation”. MID.ru, 2026. Link
- Neftegaz.RU. “Афипский НПЗ и объект ТЭК в Орловской области: названы последствия атак на российские регионы”. Neftegaz.RU, 2026. Link
- NV. “Оборонпром України 2025 — виробництво та фінансування зброї, кодифікація нових зразків”. NV, 2026. Link
- Payload Space. “2025 orbital launch attempts by country”. Payload Space, 2025. Link
- Radio Svoboda. “Україна вже на 60% забезпечує Сили оборони власною зброєю – Зеленський”. Radio Svoboda, 2026. Link
- RBC-Ukraine. “РФ вперше використала «Герань-5»: чим небезпечний новітній дрон окупантів”. RBC-Ukraine, 2026. Link
- Reuters. “Drones hit two tankers in Black Sea as Kazakh oil production plummets, managers say”. Reuters, 2026. Link
- Reuters. “US seizes Olina tanker in Caribbean, fifth vessel taken in Venezuela blockade”. Reuters, 2026. Link
- RMF24. “Polsce groził blackout? Gawkowski: cyfrowe czołgi już tu są”. RMF24, 2026. Link
- Scroll Media. “База Інвестицій”. Scroll Media, 2026. Link
- Seatrade Maritime. “US seizes seventh tanker”. Seatrade Maritime, 2026. Link
- Snake Island Institute. “August Defense Tech Monthly”. Snake Island Institute, 2025. Link
- Snake Island Institute. “Defense Tech Monthly — December 2025”. Snake Island Institute, 2025. Link
- Snake Island Institute. “Defense Tech Monthly — November 2025”. Snake Island Institute, 2025. Link
- Substack. “The Night They Tried to Kill the Sky”. Substack, 2026. Link
- Telegram @astrapress. “В Ставропольском крае атакован химический завод”. Telegram, 2026. Link
- Telegram @astrapress. “Генштаб ВСУ подтвердил атаку на нефтебазу «Роснефти» в Пензе, к тушению которой привлекли два пожарных поезда”. Telegram, 2026. Link

SOURCES

- Telegram @DIUkraine. “Ворог уперше застосував ударний БПЛА Герань-5 — деталі нової розробки буде оприлюднено на порталі War&Sanctions”. Telegram, 2026. Link
- Telegram @DniproOfficial. “Результати ураження 13 січня заводу "Атлант-Аеро" у Таганрозі”. Telegram, 2026. Link
- Telegram @dosye_shpiona. “Удар по ТЭЦ Белгорода”. Telegram, 2026. Link
- Telegram @exilenova_plus. “6 січня 2026 року дальнобійні безпілотні апарати СБУ (центр «Альфа») атакували об’єкт енергетичної інфраструктури”. Telegram, 2026. Link
- Telegram @exilenova_plus. “Момент ракетного удару по Бєлгородській ТЕЦ”. Telegram, 2026. Link
- Telegram @exilenova_plus. “Невинномысск, Ставропольский Край”. Telegram, 2026. Link
- Telegram @exilenova_plus. “Таганрог, местные сообщают что был атакован Атлант Аэро”. Telegram, 2026. Link
- Telegram @exilenova_plus. “У Підмосковному Воскресенську пожежа на території одного з найбільших в рф хімічного заводу «Воскресенські мінеральні добрива»”. Telegram, 2026. Link
- Telegram @exilenova_plus. “У м. Єлєц Липецької області чисельні влучання дронів у цеха заводу "Енергія"”. Telegram, 2026. Link
- Telegram @GeneralStaffZSU. “Уражено НПЗ «Ільський» у Краснодарському краї та низку цілей на ТОТ Донецької області”. Telegram, 2026. Link
- Telegram @GeneralStaffZSU. “Уражено нафтобазу у Волгоградській області рф та низку цілей на ТОТ України”. Telegram, 2026. Link
- Telegram @GeneralStaffZSU. “Уражено російський НПЗ та низку інших об’єктів ворога”. Telegram, 2026. Link
- Telegram @mod_russia. “Официальный канал Минобороны России”. Telegram, 2026. Link
- Telegram @moscowtimes_ru. “Путину сообщили о падении числа космических пусков в России”. Telegram, 2026. Link
- Telegram @robert_magyar. “Птахи СБС подзьобали 21 об’єкт у глибині ворожих та окупованих територій 2-7 січня засобами глибинного ураження”. Telegram, 2026. Link
- Telegram @serhii_flash. “Вчора БПЛА Молния в моїй публікації була носієм пелюсток”. Telegram, 2026. Link
- Telegram @serhii_flash. “Вчора вранці противник завдав удару Шахедами по вертольотах у районі Кропивницького”. Telegram, 2026. Link
- Telegram @serhii_flash. “Пам'ятаєте, я розповідав, що противник обрав концепцію одного типу БПЛА”. Telegram, 2026. Link
- Telegram @serhii_flash. “Противник продовжує шукати способи знищення нашої авіації”. Telegram, 2026. Link
- Telegram @serhii_flash. “Сьогодні вперше зафіксовано факт управління БПЛА БМ-35 через Старлінк”. Telegram, 2026. Link
- Telegram @supernova_plus. “Attack on Saratov Oil Refinery”. Telegram, 2026. Link
- Telegram @The_beauties_of_Iranii. “Нейтрализация сети Starlink системой «Тополь»”. Telegram, 2026. Link
- Telegram @ukr_sof. “Сили спеціальних операцій уразили три бурові установки в Каспійському морі”. Telegram, 2026. Link
- Telegram @VictoryDrones. “Technological continuity of Geran-5 with Iran’s Karrar UAV”. Telegram, 2026. Link
- Telegram @vvgladkov. “ВСУ с помощью беспилотника атаковали нефтебазу на территории Старооскольского округа.”. Telegram, 2026. Link
- Telegram @vvgladkov. “Над Белгородом и Белгородским округом системой ПВО отражена атака воздушных целей”. Telegram, 2026. Link
- Telegram @vvgladkov. “По нашей информации - самый массированный обстрел города Белгорода, предположительно, «Хаймерсами»”. Telegram, 2026. Link
- The Economist. “The big ambitions of China’s private space industry”. The Economist, 2026. Link
- The New York Times. “U.S. Forces Seize Sixth Oil Tanker Linked to Venezuela”. The New York Times, 2026. Link
- UCDI. “UCDI Investor Club Ukraine”. UCDI, 2026. Link
- Ukrinform. “Ukrainian forces hit Khokholskaya oil depot in Russia’s Voronezh region”. Ukrinform, 2026. Link
- Ukrinform. “Zelensky: 20 % of Russia’s shadow fleet has stopped operating”. Ukrinform, 2026. Link
- UNN. “‘Starlink makes these drones almost invulnerable to electronic warfare’: a new serious threat from Russian UAVs and how to combat it”. UNN, 2026. Link
- Verstka. “Oil Refinery Attacks Visualisation”. Verstka, 2025. Link
- War & Sanctions. “Geran-2 UAV (series ‘Э’, with Verba MANPADS)”. War & Sanctions, 2026. Link
- X. “It’s 2026, still no Armata, but cutting edge warfare brought a horse with Starlink instead”. X, 2026. Link
- YouTube. “Ударний НРК взяв у полон 3 військових рф | Droid TW-7.62 у реальному бою”. YouTube, 2026. Link

SNAKE ISLAND INSTITUTE

The Snake Island Institute is an independent defense analytics and coordination center established to strengthen the strategic partnership between Ukraine and its western allies in the security sector through:

ANALYTICS:

Advancing understanding of modern warfare and doctrine

ADVOCACY:

Aligning Ukrainian, U.S., and international decision-makers

DEFENSE TECH:

Enabling integration of critical technologies into combat operations

You can find more on our website.

snakeisland.org

AB3 TECH

AB3 Tech is a specialized defense tech team set up to support the structured selection, acceleration, and scaling of technology solutions for the 3rd Army Corps of the Armed Forces of Ukraine.

You can find more on our website.

ab3.tech

EDITORIAL & DESIGN TEAM

- **Viktoriia Honcharuk** – Director, Defense Tech at Snake Island Institute
- **Oleksandra Balabukha** – Defense Tech Analyst at Snake Island Institute
- **Catarina Buchatskiy** – Visual Design, Director of Analytics at Snake Island Institute
- **Olha Kovalenko** – Layout Design

AB3TECH

SNAKE ISLAND INSTITUTE

Edition 8.0

January 2026