SNAKE ISLAND INSTITUTE

Defense TECH MONTHLY

Edition 9.0

IN THIS EDITION:

Gerbera & Shahed as FPV Drone "Motherships"

Chinese Mesh Modems Linking Russian UAVs

Starlink and the Battle for Connectivity

DRONE FAILURE

Western Allies' Warfare Gap — What Should be Learned from Ukraine

February 2026

TABLE OF CONTENTS

NORTHEAST (SUMY–VOVCHANSK–KUPIANSK–LYMAN):

Assaults continued in the Vovchansk sector, with reported Russian advances near Tykhe and Dehtiarne, and toward Zelene. **Ukrainian forces continued clearance operations in Kupiansk,** while Russian infiltration groups east of the city attempted to advance toward Petropavlivka, Kurylivka, and Kivsharivka. The pressure increased toward Yampil; the city remains under Ukrainian control but is reportedly at risk of encirclement. Russian forces also sustained activity in Sumy Oblast, including near Oleksiivka, Andriivka, and Varachyne, and across the border in Kursk Oblast, with continued attempts to penetrate the border, including near Pokrovka and Hrabovske.

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

Near Siversk, Russian forces advanced near Zakitne, Sviato-Pokrovske, Nykyforivka, and Vasiukivka, maintaining pressure toward Ozerne, Kryva Luka, and Riznykivka. Intelligence suggests **additional reinforcements were reportedly deployed toward the Sloviansk–Kramatorsk axis,** preparing for a broader encirclement effort. Fighting continued in Chasiv Yar, with reported advances near Shevchenko, Yuzhne, and Zemlyanky, and toward Stupochky. In the Kostiantynivka direction, attacks persisted near Pleshchiivka, Berestok, and Illinivka, with Russian forces reportedly striking infrastructure near the Kostiantynivka dam to disrupt logistics. East of Dobropillia, Russian forces advanced near Sofiivka, Nove Shakhove, Nykanorivka, Dorozhnie, and Suvorove. Russian forces control most of Pokrovsk and Myrnohrad, with continued advances near Rodynske, Rivne, Svitle, and Hryshyne.

SOUTH (OLEKSANDRIVSK–HULIAIPOLE–ORIKHIV–STEPNOHIRSK):

On the Oleksandrivsk and parts of the Huliaipole axis, Ukrainian forces conducted localized counterattacks. Various sources indicate the **liberation of approximately 300–400 square kilometres and up to eight settlements,** including Andriivka, Ostapivske, Pishchane, Nechaivka, Radisne, and Nove Zaporizhzhia. Near Huliaipole, Russian forces reportedly expanded control, advancing toward Tsvitkove, Staroukrainka, and Zaliznychne. Fighting continues along the Orikhiv–Stepnohirsk direction, where Russian units are attempting to reach rear positions.

WINDOW OF LIFE — TIMING IS EVERYTHING

Mechanized platforms now operate in narrow “windows of life” — pushing forward under EW cover and during rare periods of drone-sparse skies, unloading fast, and withdrawing before response cycles close. This applies across the fleet: IFVs, APCs, MRAPs, logistics trucks, MEDEVAC, and light vehicles rarely remain forward beyond minutes.

Vehicles are used less for maneuver and more for short-cycle mobility: rapid insertion and forward resupply. Armored CASEVAC and last-mile logistics are increasingly shifted to UGVs, while dedicated MEDEVAC remains largely rearward. Fiber-optic drones have further compressed these windows, with no reliable way yet to localize — let alone neutralize — them.

LIVING DRONES: THE EXPANDING DOMAIN OF BIO-ROBOTICS

In late February, **German startup SWARM Biotactics disclosed that its bioelectronic insect-based robotic systems have completed field testing and transitioned into operational use with NATO customers.** The announcement confirms operational progress in programmable cyborg insect swarms designed for sensing and reconnaissance missions.

Insects with Equipment “Bag”. Source: SWARM Biotactics

The system integrates live insects equipped with miniature electronic modules containing neural interfaces, sensors, onboard AI processing, and secure communications, enabling remote guidance and coordinated swarm operation.

The technology is designed to access confined or dangerous environments where traditional systems face constraints. Also, unlike traditional drone production, scaling relies on biological reproduction combined with electronic augmentation rather than conventional manufacturing lines.

Within 12 months of its founding, SWARM Biotactics expanded to more than 40 engineers and scientists operating across Germany and the United States. The company confirmed paying defense customers, including Germany’s Bundeswehr, and reported field validation in both European and U.S. operational environments. SWARM Biotactics **has raised approximately €13 million in funding to support further development and expansion.**

Though interest in biologically integrated systems is not limited to Western developers. In December 2025, **the Russian neurotechnology company Neiry initiated early real-world trials of its “bio-drones,”** involving birds fitted with neural interfaces, solar modules, and cameras, reportedly guided along preset routes, with the system’s obvious potential for military reconnaissance.

Taken together, those systems’ development may signal broader military interest in the emergence of a bio-robotic reconnaissance platform that combines biological mobility with digital command-and-control.

FROM MOBILITY TO SURVIVABILITY: ANTI-DRONE ADAPTATIONS ON UGVS

With more than **7,000 logistical missions conducted in the first month of 2026**, UGVs continue to expand their operational footprint. To increase survivability in a drone-contested environment, where a UGV valued at approximately $14,000–18,000 can be neutralized by a UAV strike, Russian forces have begun **mounting anti-drone structures** previously observed on vehicles.

Russian Courier UGV Fitted with "Mangal" and Protruding Barbed Wire. Source: Army Inform

In February 2026, **footage from the Kostiantynivka direction documented an enemy "Courier" UGV fitted with a mounted "mangal"**, a metal cage reinforced with protruding barbed wire. Although the added mass reduces mobility and useful payload, the structure can force premature detonation on an external frame, shifting blast effects away from critical components and reducing structural damage.

Russian Courier UGV With "Mangal" and Tree Branches. Source: Defense Express

In a similar configuration, tree branches were added for visual concealment.

Courier UGV Equipped with Rotating Metal Cables for Anti-Drone Protection. Source: texBPLA

Another experimental variant featured **rotating metal cables mounted around the box-like superstructure,** intended to prematurely detonate or deflect approaching drones.

February Protection Configuration of Unknown UGV — "Mangal" and Gas Cylinder Used as Anti-Mine Trawl. Source: texBPLA

A February modification replaced its earlier chain trawl with an empty gas cylinder and added an improvised "mangal," reflecting rapid field adaptation.

Although some of these solutions remain ad hoc, the shift toward enhanced UGV survivability supports mission continuity, facilitates platform evacuation for recovery and repair, enables component reuse, and mitigates financial losses.

DELIVERING FIRE AND FUEL: THE COURIER AS A UNIVERSAL GROUND PLATFORM

In February, **Russian sources published footage of the Courier UGV specifically reconfigured for fuel delivery to frontline positions**.

The UGV was modified with a cargo-release mechanism, allowing it to drop canisters in the designated area without requiring infantry to approach the platform to unload supplies, reducing personnel exposure.

Theoretically, if a UAV is detected, the UGV could jettison its load to prevent onboard fuel ignition and limit secondary damage. In case of attack, the platform is also fitted with a “mangal” metal frame designed to trigger premature drone detonation away from the main structure, as well as an anti-drone poncho to reduce thermal signature and increase survivability.

The Courrier became one of the most frequently used Russian ground robotic platforms, with some variants adapted for **thermobaric systems**, machine guns, and grenade launchers, **aerosol smoke deployment**, mine laying and demining, and evacuation configurations. As with Molniya UAVs, **rather than developing separate platforms for different tasks, Russia continues to adapt a single base model** for multiple combat missions, preserving modularity and accelerating iteration.

Russian UGV for Fuel Delivery. Source: Zvezda

Cargo-Release Mechanism for Canisters. Source: Zvezda

UKRAINE ON THE GLOBAL DEFENSE STAGE: FROM BATTLEFIELD TO BREAKTHROUGH AT MSC 2026

On February 13, on the sidelines of MSC, **the Snake Island Institute, together with partners, hosted From Battlefield to Breakthrough**. The event convened defence-tech innovators, investors, military operators, and ecosystem stakeholders for a candid fireside conversation on the evolution of Ukrainian air defense systems and the operational maturation of strike UGV units. Insights from the battlefield were presented by frontline operators and commanders, including the Deputy Chief of Air Defense, the Chief of the Electronic Warfare Department, and the Head of the R&D Lab of the Anti-Aircraft Regiment of the **3rd Army Corps**; the Commander of the **Strike UGV Company "NC13" of the 3rd Separate Assault Brigade**; the Company Commander of the UAV Interceptor Battalion DARKNODE of the **412th Brigade of the Unmanned Systems Forces**; and a Platoon Instructor from **Killhouse Academy**.

The discussion highlighted concrete Ukrainian breakthrough cases from the battlefield, underscoring how rapid iteration, frontline feedback loops, and cross-sector collaboration are shaping modern warfare.

Panel Discussion. Source: Snake Island Institute

The event also featured **Killhouse Academy** — a drone training academy led by veterans of Ukraine's 3rd Separate Assault Brigade. The Academy prepares UAV operators through a combat-informed curriculum shaped by real frontline experience. Speakers shared lessons from training both military personnel and civilian drone operators, emphasizing the need to expand Ukraine's battle-tested methodology through structured cooperation with international partners.

A key point underscored during the discussion was clear: **flying a drone is not the same as applying drone tactics in combat**. Technical proficiency must be integrated with tactical awareness, coordination, survivability, and mission execution under fire.

From Battlefield to Breakthrough. Source: Snake Island Institute

A broader theme emerging in Munich was "Build with Ukraine" — shifting from procurement toward joint production and integrating Ukraine's defense-industrial base into the European ecosystem. Agreements announced at MSC included:

- Ukraine's TAF Industries and Germany's Wingcopter signed an MoU to establish a joint venture focused on reconnaissance UAV platforms.
- Tencore LLC partnered with Germany's Fernride to jointly produce the Termit UGV and develop AI-enabled autonomous logistics solutions.
- Auterion and Ukrainian firm Airlogix announced a joint enterprise to manufacture AI-powered UAVs.
- JSC Ukrainian Defense Industry formalized cooperation with Sweden's Saab in aviation and radar technologies.

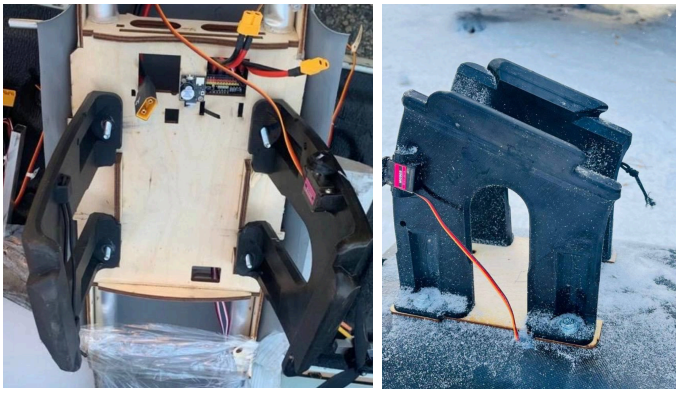
THE RISE OF DRONE CARRIERS: GERBERA AND SHAHED AS FPV DELIVERY PLATFORMS

In early February, **Russia reportedly employed the Gerbera UAV for the first time as an FPV drone mothership**. Gerbera is now configured to carry between one and two FPV drones mounted externally on hardpoints.

Launched from a comparably cheap Gerbera platform, they can be released in proximity to designated targets, effectively bypassing the first lines of air defense. **They are deployed over areas with stable LTE mobile network coverage**, allowing operators to maintain control of the FPVs via cellular communications, **similar to tactics used with Molniya-style "motherships."**

Gerbera as an FPV Drone "Mothership". Source: Life

After releasing the FPVs, if equipped with a warhead, the "mothership" likely retains the ability to execute its kamikaze mission. However, given useful load limitations, **priority in onboard equipment is most likely given to the more important role of communications relay** rather than additional munitions. The installation of external antennas or signal amplifiers indicates an effort to maintain a stable link between the UAV operator and the deployed FPVs.



Identical FPV Attachment Systems on Molniya and Gerbera Platforms. Source: serhii_flash

Notably, both Molniya and Gerbera "motherships" series use **identical attachment systems for FPVs**, indicating production-level unification rather than field improvisation. The presence of factory-standardized hardpoints suggests scaling, **with some reports indicating that Gerbera-FPV combinations are now observed daily**.

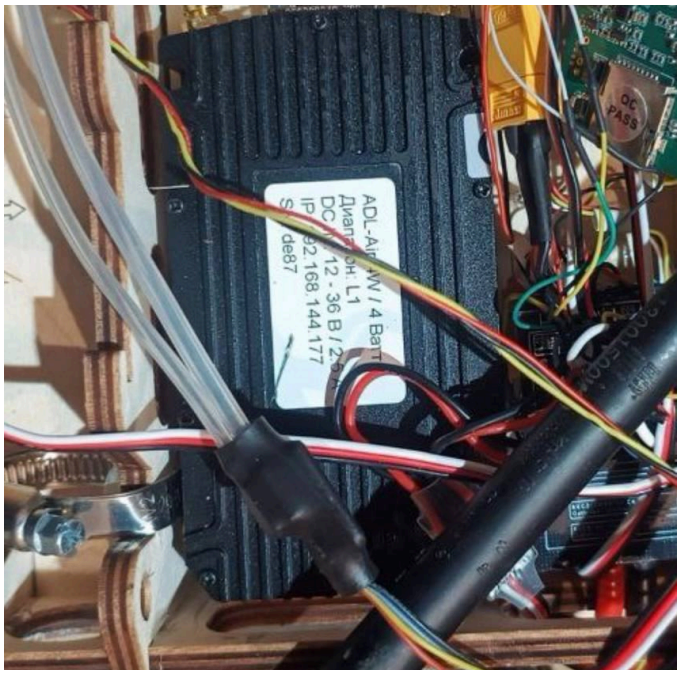
Shahed Deploying an FPV Drone. Source: serhii_flash

By mid-February, **similar tactics were reportedly detected on Shahed platforms**, with claims that modified variants can carry up to two FPV drones.

This evolution further complicates air defense. By transporting small, low-signature FPV drones closer to the target area, the mothership concept compresses reaction timelines and reduces interception windows. It also degrades detection, as the distinctive noise signature of FPV engines is reportedly masked by the bigger carrier platform if it stays in the zone of interest after detachment.

STANDARDIZING THE SIGNAL: MESH MODEMS ACROSS RUSSIA'S UAV FLEET

In February, a **Chinese mesh modem was identified on two additional Russian UAVs — Molniya and V2U.** Footage confirms the integration of equipment produced by Shenzhen Sinosun Technology, **previously documented on Gerbera, Shahed, and Kub platforms**. It indicates efforts to **unify the UAV command-and-control segment, a goal that has not yet been fully achieved**.



Smaller Version of Mesh Modem Integrated Into Russian Molniya UAV. Source: serhii_flash

Smaller Version of Mesh Modem on Downed Russian V2U UAV. Source: serhii_flash

Mesh architecture **enables each drone to function as both transmitter and relay**, creating a distributed airborne network across strike, decoy, and reconnaissance UAVs, with predictions of scaling to UGVs. If one drone is downed or jammed, traffic is automatically redirected through another. **The link is preserved even after the loss of individual platforms.** This extends the control range and increases resilience to electronic warfare.

Smaller mesh modems identified on Molniya and V2U allow integration of compact, lower-signature UAVs into the same network layer.

Characteristics Comparison of the Mesh Modems (Top: Variant Used in Molniya and V2U UAVs). Source: Shenzhen Sinosun Technology

Open-source data indicate that the manufacturer produces mesh modems operating across multiple frequency bands, including up to 6–7 GHz. Combined with **Ukrainian intelligence reporting on Russian forces' negotiations for contracts covering hundreds of thousands of units**, the expanding use of mesh modems poses a significant challenge to electronic warfare countermeasures.

FEBRUARY DEEP STRIKE CAMPAIGN

Ukraine maintained its deep-strike operations, consistently weakening Russia's energy infrastructure and military-industrial base. However, compared to earlier months, February saw a slight decrease in the total number and intensity of Ukrainian attacks against Russian oil and energy infrastructure, pumping stations, plants, and pipelines.

TARGETING REFINERIES: UKRAINE'S FEBRUARY OIL STRIKES

According to available sources, Ukraine struck at least 4 oil refineries in February 2026 — a noticeable decline **compared to at least 7 in January and at least 11 in December 2025**.

Facility	Date	Assessment
Volgograd Oil Refinery (Volgograd Oblast)	February 10–11	Halted operations after drone attack. The capacity of the AVT-1 unit is about **18,600 tons per day.** In 2024, the plant processed 13.5 million tons of oil **(5% of the total volume in the Russian Federation)** and produced 6 million tons of diesel, 1.9 million tons of gasoline, and 700 thousand tons of fuel oil.
Ukhta Oil Refinery (Komi Republic, ~1,750 km from Ukraine)	February 12	The facility was struck by AN-196 "Liutyi" UAVs, igniting fires at the refinery's AVT (primary atmospheric distillation) unit and the visbreaking unit. **The refinery processes about 4.2 million tons of oil per year.** Key products include gasoline, diesel fuel, fuel oil, and vacuum gasoil.
Ilsky Oil Refinery (Krasnodar Krai)	February 17	One of the largest refineries in southern Russia. The total primary processing capacity is about **6.6 million tons of oil per year.**
Albashneft Mini-Refinery (Novominskaya, Krasnodar Krai)	February 28	**Four RVS-5000 storage tanks were destroyed,** three RVS-2000 tanks were damaged, along with pipelines and an underground reservoir. The strike significantly reduced fuel storage and local logistics capacity.

Moment of Impact Volgograd Oil Refinery. Source: war_home

Smoke After the Attack at Ukhta Oil Refinery. Source: VictoryDrones

Fire Breaks Out at Ilsky Oil Refinery. Source: Pravda

In addition to inflicting long-term production damage, Ukraine targeted fuel depots, terminals, and pumping stations to eliminate immediate reserves and disrupt distribution networks.

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

Facility	Date	Assessment
Tamannaftogaz Oil Terminal (Volna, Krasnodar Krai)	February 14–15 & February 16–17	One of the largest oil terminals in the Black Sea basin with storage capacity exceeding 1 million cubic meters (crude oil, petroleum products, LPG, ammonia). Two strikes within three days caused a fire covering ~7,000 sq.m. Berths and storage tanks were damaged.
Velikolukskaya Oil Depot (Velikiye Luki, Pskov Oblast)	February 18–19	The facility was struck by AN-196 "Liutyi" UAVs, igniting fires at the refinery's AVT (primary atmospheric distillation) unit and the visbreaking unit. The refinery processes about 4.2 million tons of oil per year. Key products include gasoline, diesel fuel, fuel oil, and vacuum gasoil.
Kaleykino Oil Pumping Station (Tatarstan, >1,200 km from Ukraine)	February 23	One of Russia's key blending and pressure-regulation nodes feeding the Druzhba pipeline and refineries in Tatarstan. Critical for maintaining uninterrupted crude export flows. Six explosions triggered a large-scale fire with oil storage tanks burning.

Results of the Attack on Tamannaftogaz Oil Terminal. Source: exilenova_plus

Fire Broke Out After the Attack at Velikolukskaya Oil Depot. Source: exilenova_plus

Massive Fire After Attack on Kaleykino Oil Pumping Station. Source: exilenova_plus

INDUSTRIAL FACILITIES & ENERGY: STRIKING THE CORE OF RUSSIA'S WAR MACHINE

Ukraine also maintains systematic pressure on Russia's industrial facility capacity that sustains the enemy's frontline operations, as well as targeting power infrastructure to further disrupt supporting functions.

Facility	Date	Assessment
Redkinsky Experimental Plant (Redkino, Tver Oblast)	February 6–7	A producer of Decylin (T-10), a high-energy aviation fuel used in Kh-101, Kh-555, and Kalibr cruise missiles. The facility is critical to Russia's missile program, and its destruction poses a serious challenge to enemy logistics and production continuity.
Novobryanskaya Substation (Vygonichi, Bryansk Oblast)	February 7–8	Confirmed impact near the 220 kV busbar portal, leaving a crater approximately 5×5 meters. Following the strike, a technical failure occurred at the facility, leading to scheduled temporary power outages in Bryansk and surrounding districts from 9 to 15 February.
Progress Plant (Michurinsk, Tambov Oblast)	February 11–12	Strike on a manufacturer of equipment for Russian aviation and missile systems.
GRAU Arsenal (Kotluban, Volgograd Oblast)	February 11–12	"Flamingo" missiles struck one of the largest Russian Armed Forces arsenals storing missiles, ammunition, and explosives. Powerful explosions and secondary detonations reported.
Metafrax Chemicals (Gubakha, Perm Krai, ~1,600 km from Ukraine)	February 16–17	A producer of methanol, urotropine, urea, and pentaerythritol — key explosive precursors for the Russian military.
Dorogobuzh Chemical Plant (Smolensk Oblast)	February 25	FP-1 drones struck the ammonia fertilizer production, storage, and transport area, triggering a chain of explosions at the vehicle loading site, railway terminal, and finished-product warehouse. Ammonium nitrate units were also affected. One loading overpass was destroyed, and nearby production facilities were damaged within several hundred meters.

Attack on Redkinsky Experimental Plant. Source: region22ua

Attack on Redkinsky Experimental Plant. Source: VictoryDrones

"Before" and "After" the Attack on Dorogobuzh Chemical Plant. Source: kiber_boroshno

BLOCKING HORMUZ: FROM REGIONAL STRIKES TO GLOBAL ENERGY MARKET SHOCK

On February 28, 2026, **Iranian authorities reportedly closed the Strait of Hormuz, a narrow channel between Iran and Oman, following military strikes by the U.S. and Israel against Iran**.

Strait of Hormuz. Source: The Guardian

The Strait of Hormuz is a critical maritime corridor handling approximately **20% of global oil and gas exports and around 30% of global urea trade.** The reported closure disrupted commercial shipping flows, with roughly 150 vessels delaying transit, anchoring outside the Gulf, or rerouting amid increased security risks.

At least **four vessels were reportedly damaged in recent incidents**:

- MKD Vyom: Marshall Islands-flagged crude tanker carrying gasoline; one crew fatality following an engine room explosion.
- Skylight: Sanctioned chemical tanker; fire onboard, four crew injured, 20 evacuated.
- Hercules Star: Gibraltar-flagged commercial tanker; strike confirmed off the UAE coast.
- Sea La Donna: Incident unverified; GPS spoofing/ jamming indicators observed; no confirmed casualties.

A prolonged blockade would significantly raise global oil and gas prices, highlighting the escalation of regional military conflict into wider energy and economic disruption. Given repeated hostile strikes on its energy infrastructure, **Ukraine has grown more reliant on gas, oil, and petroleum products, as well as on their stable pricing**. Prolonged instability in global energy markets could cause serious economic consequences.

BARAZH-1: A STRATOSPHERIC ALTERNATIVE TO SATELLITE COMMUNICATION

Following the reported **disabling of Starlink services on Russian territory in February 2026**, Russia accelerated testing of a domestic alternative known as Barazh-1 (Barrage-1). The project is presented as an unmanned stratospheric aerostat platform intended to reduce reliance on foreign satellite systems and restore digital connectivity between military units. The initial trial launch reportedly took place on February 13, approximately one week after the termination of Starlink access.

Launch of Barazh-1. Source: Obozrevatel

Barazh-1 is reported to operate at altitudes of up to 20 km and carry payloads of up to 100 kg. The platform employs **a pneumatic ballast system** for altitude control, allowing it to exploit wind currents for directional movement. Rather than functioning as a conventional satellite, **it resembles a high-altitude pseudo-satellite (HAPS)**, potentially providing localized 4G/5G coverage along the frontline.

However, such platforms would require regular replacement due to material degradation and weather exposure. In addition, stratospheric systems are inherently more vulnerable to interception and electronic warfare than low Earth orbit satellites, raising questions about their survivability and overall resilience in a contested environment.

CONNECTIVITY DENIED: DISABLING RUSSIAN STARLINK TERMINALS

Following an increase in Russian UAVs equipped with Starlink terminals in January 2026, the Ukrainian Ministry of Defence contacted SpaceX and proposed solutions to prevent unauthorized use of systems.

By February 1, **the first measures were introduced**: terminals moving **over 75 km/h faced data limits, and those exceeding 90 km/h were automatically disabled,** making them unusable for drone flights. This temporary solution, while affecting both sides, rapidly halted enemy drone activity until **a "whitelist" was subsequently implemented to separate authorized terminals from those used by Russians**.

The registration process could be undergone:

- For military personnel: registration through the Army+ app
- For businesses and public servants: registration through the Diia portal
- For civilians and individual entrepreneurs: registration through the Administrative Service Center

By February 5, Russian-operated terminals were largely offline. In response, Russia sought alternative access, including **attempts to recruit collaborators in Ukraine, blackmail families of prisoners of war, and use "verification bots."**

The disabling of Russian Starlink terminals has cut Russian drone feeds 11-fold and significantly increased Ukrainian radio intercepts. This shift possibly contributed to the February counterattacks in the Zaporizhzhia direction, where Ukrainian forces liberated 300–400 square kilometers.

The shift from an unresolved threat in January to the solution and its operational results by mid-February highlights the rapid pace of modern warfare. At the same time, the existing threat underscored a structural vulnerability: operational dependence on a system beyond national control, underscoring the need for a domestic or jointly managed communications capability.

WHITE LIST, BLACK TRAP: RUSSIA'S STARLINK LOOPHOLE TURNS INTO AN INTELLIGENCE LEAK

Following Ukraine's restriction of Starlink usage and the introduction of a verified "whitelist" system requiring terminal registration through official administrative channels, Russian forces sought alternative methods to activate and legitimize terminals operating in occupied territories.

In response, **Ukraine's 256th Cyber Assault Division, in coordination with InformNapalm and MILITANT, launched a controlled deception operation.** A network of Telegram channels and bots was established, offering "activation services" for a small payment to Russian personnel attempting to bypass registration controls.

Within one week, the operation collected 2,420 data packages linked to Russian-operated Starlink terminals, including precise geolocation data, which was forwarded to relevant structures for further operational action. Additionally, 31 individuals volunteered to act as intermediaries in the illegal activation procedures; their information was passed to Ukrainian law enforcement. In total, **Russian personnel transferred $5,870 in payments while attempting to restore connectivity.** The funds were redirected to support Ukrainian defense initiatives.

Parallel cyber activity reportedly included the **distribution of malware-infected files disguised as Starlink unlocking instructions,** further exploiting Russian attempts to restore satellite communications.

MAX CONTROL, MINIMUM TRUST: MOSCOW'S MOVE TOWARDS "DIGITAL SOVEREIGNTY"

Russia plans to block Telegram, used by over 90 million Russians, starting April 1, 2026, claiming the platform is being used as a tool of "hybrid warfare" and sabotage by criminals and foreign intelligence services.

Notably, **in February, the Russian government also blocked WhatsApp,** which had more than 100 million users in the country, following earlier restrictions on Meta's Facebook and Instagram, as well as YouTube and Snapchat, now accessible only via VPN.

Amid the Russian "potential blocking of Telegram, some sources **report the forced transition of certain Russian military units to MAX,** a state-backed messenger launched in 2025. Other sources state that **Russian units fighting in Ukraine have been advised not to use MAX due to security and data storage concerns**. Others claim that even if Telegram is fully blocked domestically, **Russian personnel would retain access**, without specifying how.

The messaging app has served as a key platform for military personnel to plan missions, establish communication channels, exchange files, and share coordinates and documents. A disruption to its work could affect the enemy's operational tempo. The Telegram closing also could result in the enemy's **military fundraising efforts falling by 50-80%.** Some reports suggest that restrictions on WhatsApp and Telegram could be introduced prior to a mobilization announcement.

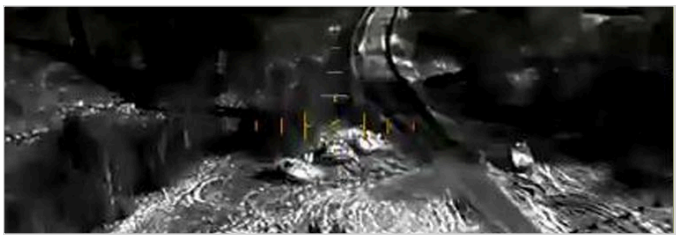
Although a full Telegram blockade reportedly depends on whether **it complies with Russia`s demands to place servers in the country and block selected channels of "fake and prohibited information,"** Russia's efforts to promote the state-controlled MAX platform, tighten control over internet use, and expand its capacity to monitor citizens online are evident.

"WE'RE F—ED": THE DRONE BATTLEFIELD NATO IS NOT READY FOR

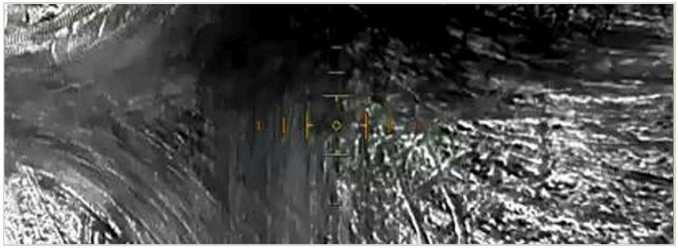
In 2025, during NATO's Exercise Hedgehog 2025 in Estonia, **Ukrainian military personnel invited to act as a notional adversary reportedly "defeated" NATO battalions with drones**.

The training involved approximately 16,000 personnel from 12 NATO member states, alongside Ukrainian active-duty servicemembers. Ukrainian participation reportedly included representatives of the **412th "Nemesis" Separate Brigade of the Unmanned Systems Forces**, pilots of the **427th Rarog Separate Unmanned Systems Regiment**, FPV drone operators from the **International Legion of the Defence Intelligence of Ukraine**, and personnel associated with the DELTA digital military system.

The main goal of the Exercise was to simulate a "contested and congested" battlefield environment to stress-test decision-making and adaptability. Some of the "missions" Ukrainian drone operators conducted, included:



Bridge "Destruction". Source: 412th "Nemesis" Separate Brigade of the Unmanned Systems Forces



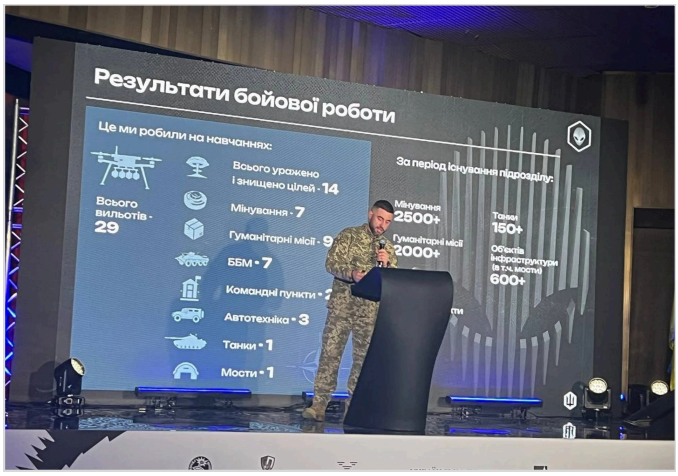
Road Mining. Source: 412th "Nemesis" Separate Brigade of the Unmanned Systems Forces

Delivery of Drinking Water to a Sniper Unit in a Hidden Position. Source: 412th "Nemesis" Separate Brigade of the Unmanned Systems Forces

Overall, within five flight days of the Exercise, Ukrainian operators achieved the following results within an operational radius of approximately 15 kilometers:

- Total sorties conducted: 29
- Total targets hit and "destroyed": 14
- Armored combat vehicles: 7
- Command posts: 2
- Vehicles: 3
- Tanks: 1
- Bridges: 1
- Mining operations conducted: 7
- Supply delivery missions executed: 9

Among the reported targets was a NATO unit command post.



Deputy Brigade Commander of Nemesis, Pavlo Laktionov, at "War 2026: Humans vs. Machines." Source: Oboronka

According to some sources, **Ukrainian-Estonian opposing forces "destroyed" the equivalent of two NATO battalions in a single day**, highlighting the operational threat posed by drones and demonstrating that NATO troops remain insufficiently prepared to recognize and respond to this threat.

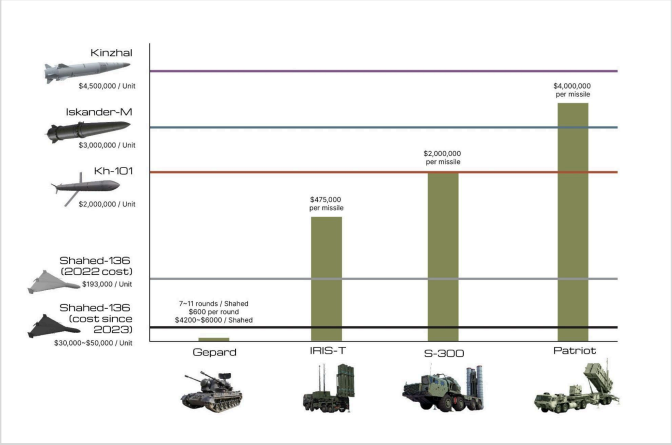
Among NATO's tactical shortcomings observed, the following can be highlighted:

- Movement of vehicles in large groupings, with vehicles reportedly "lined up like in a shopping mall parking lot";
- Insufficient use of camouflage and concealment measures;
- Lack of infantry reaction to approaching UAVs, including failure to take cover before the threat approaches;
- Failure to conduct route clearance and check roads for mines;
- Inefficient use of the DELTA system;
- Outdated NATO training courses, based on doctrines with no drone integration.

The vulnerabilities identified during the training also attracted political attention. Germany's far-right Alternative for Germany (AfD), known for its pro-Kremlin positioning, **requested government information on weaknesses exposed during Hedgehog 2025**. The potential disclosure of such assessments carries security implications, particularly amid heightened pressure on the Baltic region.

Military exercises in Estonia are not the only evidence that NATO troops are likely completely unprepared for a modern full-scale war with a comparable adversary.

The military conflict in the Middle East, which intensified in February, serves as a further sign of the lack of readiness among Western militaries to confront drone threats that are no longer confined to Ukraine. Iranian Shahed drones, flying over Ukrainian territory since 2022, **cost roughly $30,000–$40,000 to produce**. By contrast, interceptors used by the U.S. and its allies are estimated to cost between $500,000 and $4 million per missile.



Cost-effectiveness comparison of intercepting Shahed-class UAVs and Kh-101, Iskander-M, and Kinzhal missiles using Gepard anti-aircraft gun systems and IRIS-T, S-300, and Patriot surface-to-air missiles. Source: Holding Back the Sky: Ukraine's Air Defense Campaign, 2022-2025

Notably, the U.S. primarily relied on aircraft or Patriot air defense systems—**expensive and difficult-to-manufacture platforms with an established production capacity of only around 600 missiles annually**. Combined with Iranian production estimates of 200–500 Shahed drones per month, this cost imbalance raises questions about the sustainability of prolonged high-intensity conflict.

Ukraine's battlefield experience has demonstrated the importance of layered, cost-effective counter-UAS solutions, costing as little as $500, rather than reliance on expensive interceptors alone. While some passive learning is visible—**the U.S. LUCAS drone equipped with Starlink terminals copies concepts first widely used by Ukrainian forces**—systematic integration of Ukraine's battlefield lessons across Western militaries remains limited.

Ukrainian battlefield experience represents a tangible contribution to European security and combat readiness. Participation in exercises such as Hedgehog 2025 enables to share the expertise with Western allies, while also expanding collaboration.

Ukrainian Drone Operators Present Their Systems to International Military Personnel at Hedgehog 2025. Source: 412th "Nemesis" Separate Brigade of the Unmanned Systems Forces

This growing acknowledgment of Ukraine's battlefield expertise is already translating into concrete steps. In February, **the German Ministry of Defense signed an agreement with Ukraine that its instructors will teach German servicemen** how to fight and use tactics. Also, **the UK plans to involve Ukrainian experts in the interception of drones over the countries of the Persian Gulf**.

SOURCES

- 412 Nemesis Brigade. “412 Nemesis Brigade”. 412 Nemesis Brigade, 2026. Link
- Army Inform. “Вночі противник евакуював пошкоджений НРК: росіяни додатково захищають цінні наземні дрони”. Army Inform, 2026. Link
- Army Recognition. “Russia Fields Courier UGV Armed with Shmel Thermobaric Rocket Module on the Ukraine Front”. Army Recognition, 2025. Link
- BBC News. “How Ukraine’s battlefield innovations are reshaping modern warfare”. BBC, 2026. Link
- BBC Ukrainian. “Матеріал BBC Україна про сучасну війну та дрони”. BBC Ukrainian, 2026. Link
- Business Insider. “The US Army is mastering drone warfare — but that doesn’t mean it’s always the right weapon”. Business Insider, 2026. Link
- Cukr. “«Гербера» може нести FPV-дрони на Сумщині”. Cukr, 2026. Link
- Defense Express. “НРК ‘кущ’, і це може бути ефективно — як рашисти захищають свій ‘Курьер’ від FPV-дронів”. Defense Express, 2026. Link
- dev.ua. “Russia announced the launch of the stratospheric 5G platform ‘Barrage-1’, which could become a partial alternative to Starlink”. dev.ua, 2026. Link
- Euronews. “Telegram might be fully blocked in Russia — question is when will it happen”. Euronews, 2026. Link
- Foreign Intelligence Service of Ukraine. “Controversy surrounding Telegram: for the first time Russia sees widespread discussion of crisis of confidence in government”. SZRU, 2026. Link
- Gwara Media. “SBU strikes Russian major oil hub in Krasnodar region”. Gwara Media, 2026. Link
- Important Stories. “Российские потери растут, набор контрактников падает: ждать ли мобилизации?”. Important Stories, 2026. Link
- International Legion for the Defence of Ukraine. “International Legion for the Defence of Ukraine”. Ministry of Defence of Ukraine, 2026. Link
- Killhouse Academy. “Killhouse Academy”. Killhouse Academy, 2026. Link
- Kyiv Post. “Full List of Deals Signed at Munich Security Conference 2026”. Kyiv Post, 2026. Link
- Life.ru. “Новейшие российские БПЛА-дрононосцы «Гербера» сняли на видео в тылу ВСУ”. Life.ru, 2026. Link
- LinkedIn. “From Battlefield to Breakthrough: Munich”. LinkedIn, 2026. Link
- LinkedIn. “One year ago this didn’t exist — today...”. LinkedIn, 2026. Link
- LinkedIn NC13 NRK. “NC13 NRK”. LinkedIn, 2026. Link
- Meduza. “Mediazona: российским военным на фронте рекомендуют не пользоваться мессенджером MAX — он недостаточно безопасный”. Meduza, 2026. Link
- Meduza. “РБК: власти России собираются заблокировать Telegram в начале апреля, мессенджер будет работать только на фронте”. Meduza, 2026. Link
- Mezha Media (Oboronka). “В Nemesis розповіли подробиці навчань НАТО в Естонії”. Mezha Media, 2026. Link
- Militarnyi. “Drones strike Redkino plant fuel missiles”. Militarnyi, 2026. Link
- Militarnyi. “US Lucas guided drones equipped with Starlink terminals”. Militarnyi, 2026. Link
- Militarnyi. “Росія шантажує родини полонених”. Militarnyi, 2026. Link
- Ministry of Defence of Ukraine. “Over 7,000 missions in January: Ukraine expands deployment of ground robotic systems”. Ministry of Defence of Ukraine, 2026. Link
- NBC News. “Shahed drones and the expanding drone war between Iran, the U.S., Russia and Ukraine”. NBC News, 2026. Link
- NV. “Калейкино: дроны СБУ поразили стратегическую нефтеперекачивающую станцию в Татарстане — видео”. NV, 2026. Link
- Obozrevatel. “Россия нашла замену Starlink: что известно о запуске стратосферной платформы «Барраж-1» и каковы риски для Украины”. Obozrevatel, 2026. Link
- Politico. “AfD inquiry into NATO vulnerabilities after Hedgehog 2025 exercise raises intelligence fears”. Politico, 2026. Link
- Rarog. “About Rarog”. Rarog, 2026. Link
- RBC-Ukraine. “Sharing battlefield expertise: Ukrainians help NATO prepare for drone warfare”. RBC-Ukraine, 2026. Link
- Reuters. “Iran’s Revolutionary Guards tell ships passage through Strait of Hormuz not allowed”. Reuters, 2026. Link
- Sinosun. “MESH Network Radio & Data Link / HD Video / Industrial Wireless Networks”. Sinosun, 2026. Link
- Snake Island Institute. “Defense Tech Monthly: January 2026”. Snake Island Institute, 2026. Link
- Snake Island Institute. “Snake Island Institute”. Snake Island Institute, 2026. Link
- Swarm Biotactics. “Swarm Biotactics”. Swarm Biotactics, 2026. Link
- Telegram @battle_unit. “С завтрашнего дня во многих подразделениях в приказном порядке заставляют переходить в MAX”. Telegram, 2026. Link
- Telegram @CyberAssault. “Instructions for @Starlink users in Ukraine to register”. Telegram, 2026. Link
- Telegram @DniproOfficial. “Вночі високоточні «уламки» навели «двіжуху» на ТОВ «Албашнефть»”. Telegram, 2026. Link
- Telegram @exilenova_plus. “Резервуар на 50.000 м3 на НПС "Калейкино" вигорів повністю”. Telegram, 2026. Link

SOURCES

- Telegram @exilenova_plus. “У ніч на 19.02 Сили оборони України демілітаризували нафтобазу військового призначення «Великолукська»”. Telegram, 2026. Link
- Telegram @exilenova_plus. “Якісні знімки результатів ураження резервуарів на нафтовому терміналі «Таманьнефтегаз»”. Telegram, 2026. Link
- Telegram @GeneralStaffZSU. “Уражено Ухтинський НПЗ”. Telegram, 2026. Link
- Telegram @GeneralStaffZSU. “Уражено нафтопереробний завод, склади ПММ та МТЗ, засоби ППО і місця зосередження противника”. Telegram, 2026. Link
- Telegram @getmantsevdanil. “Коли переговори не спрацьовують, починаються війни”. Telegram, 2026. Link
- Telegram @kiber_boroshno. “В результаті атаки на завод ПАО "Метафракс" двома БПЛА АН-196 "Лютий" було уражено ректифікаційну колону”. Telegram, 2026. Link
- Telegram @kiber_boroshno. “В результаті ураження арсеналу ГРАУ в н.п. Котлубань ракетами FP-5 "Фламінго" було знищено бункер”. Telegram, 2026. Link
- Telegram @payloadUAV. “Спутниковый фишинг”. Telegram, 2026. Link
- Telegram @publicreservestugna. “Уночі безпілотники завдали удару по складу ГРАУ у Волгоградській області”. Telegram, 2026. Link
- Telegram @serhii_flash. “Військовий коллега надіслав мені фото комплектації з нової Молнії”. Telegram, 2026. Link
- Telegram @serhii_flash. “Китайський МЕШ-модем помічений ще на одному російському БПЛА V2U”. Telegram, 2026. Link
- Telegram @serhii_flash. “На відео момент запуску FPV з БПЛА Гербера”. Telegram, 2026. Link
- Telegram @serhii_flash. “Нещодавно я написав, що заводське кріплення для перенесення ФПВ на Молнії та Гербері є поганим знаком”. Telegram, 2026. Link
- Telegram @serhii_flash. “Ось так в ефірі виглядає робота китайського модему на БПЛА Молния”. Telegram, 2026. Link
- Telegram @serhii_flash. “Поганий знак. Герберщики і Молнієводи — це два різних клани”. Telegram, 2026. Link
- Telegram @serhii_flash. “Що зараз відбувається зі скиданням FPV з БПЛА”. Telegram, 2026. Link
- Telegram @texBPLA. “Еще одна кустарная антидроновая защита ("мангал") для НРК от российских военнослужащих.”. Telegram, 2026. Link
- Telegram @texBPLA. “Российский наземный дрон "Курьер" с экспериментальной защитой от FPV-дронов в виде вращающихся тросов.”. Telegram, 2026. Link
- Telegram @VictoryDrones. “Сили оборони уразили НПЗ «Лукойл-Ухтанефтепереработка» у місті Ухта Республіка Комі”. Telegram, 2026. Link
- Telegram @war_home. “Горить НПЗ Лукойл”. Telegram, 2026. Link
- Telegram @war_home. “Результат удару DeepStrike БпЛА FP-1 по хімічному заводу АТ «Дорогобуж» (Смоленська обл.) 25.02.2026.”. Telegram, 2026. Link
- The Eurasian Times. “Starlink rival? India clears AS-HAPS airship as Russia tests Barrage-1”. The Eurasian Times, 2026. Link
- The Guardian. “Russia scrambles after Starlink access deactivated by Elon Musk’s SpaceX”. The Guardian, 2026. Link
- The Jerusalem Post. “Russian cyborg pigeon drones begin real-world testing phases, sparking concern over military misuse”. The Jerusalem Post, 2026. Link
- The Moscow Times. “Russia plans to block Telegram in April, sources say”. The Moscow Times, 2026. Link
- The Moscow Times. “Россия отменила запрет на экспорт бензина для производителей нефтепродуктов”. The Moscow Times, 2026. Link
- The Moscow Times. “Украина атаковала нефтебазу в Псковской области”. The Moscow Times, 2026. Link
- The Third Army Corps. “The Third Army Corps”. The Third Army Corps, 2026. Link
- The Wall Street Journal. “NATO Has Seen the Future and Is Unprepared”. The Wall Street Journal, 2026. Link
- TSN. “Мобільний інтернет ворог використовує як канал керування дронами: подробиці”. TSN, 2025. Link
- Ukrainska Pravda. “Атака дронів на РФ: горить НПЗ, закрито п'ять аеропортів, у Казані проблеми зі світлом”. Ukrainska Pravda, 2026. Link
- UNIAN. “Войска НАТО не готовы к войне — украинские бойцы”. UNIAN, 2026. Link
- UNIAN. “США та Іран: американські війська збили іранський дрон”. UNIAN, 2026. Link
- Windward. “Iran War Maritime Intelligence Daily”. Windward, 2026. Link
- X @FedorovMykhailo. “Ukraine, together with @Starlink, has already taken the first steps that delivered rapid results in countering Russian drones”. X (Twitter), 2026. Link
- X @LaurenDreyer. “Post by Lauren Dreyer”. X (Twitter), 2026. Link
- YouTube. “New War Erupts: US & Israel Hammer Iran”. YouTube, 2026. Link
- YouTube. “US-Iran War: Can Israel & US Replenish Interceptors Faster Than Iran Makes Drones? | WION”. YouTube, 2026. Link
- YouTube. “Робот Курьер ставит дымовую завесу шашкой УДШ”. YouTube, 2026. Link
- Zvezda TV. “Военнослужащие показали «Курьер», переоборудованный под доставку топлива”. Zvezda TV, 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

INTERNATIONAL PARTNERSHIPS:

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

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
- **Oleksandra Onopriienko** – Layout Design

SNAKE ISLAND INSTITUTE

February 2026