SNAKE ISLAND INSTITUTE

Defense Tech Monthly:

Ukraine-Russia Battlefield

Edition #7

December 2025

TABLE OF CONTENTS

Section I 03

Section II 04

Land 04

Containerized Stand-Off: Russian Improvised Tank Protection 04
Crossing Without Soldiers: UGVs Take on High-Risk Engineering Tasks 04
Tactical Adaptation: Logistics Platforms as Modular Strike Systems 05

Air 06

Mining, Reconnaissance, and Starlink: The Expanding Battlefield Role of Molniya-2 06
Rising Tempo, Rising Costs: Ukraine's Strike Campaign in Occupied Crimea 07
December's Deep Strike Campaign: From Refinery Attrition to Maritime Energy Interdiction 08
When Shaheds Shoot Back: Russia Arms Drones with Air-to-Air Missiles 11

Maritime 12

From Shadow Fleet to Submarines: Drones Drive Ukraine's Black Sea Campaign 12
Britain's Underwater Front: Atlantic Bastion Takes Shape 12

Space 13

Beyond Starlink: Ukraine's Push for Sovereign Satellite Communications 13
Russia Launches Obzor-R: Step Toward Domestic SAR Reconnaissance 13

EW 14

Starlink on Both Sides: How Starlink Is Reshaping the Communications Battlefield 14

Cyber 15

Selective Denial: Russia's IMEI Registry Play 15

Section III 16

Year Wrap Up 16
A Year of Accelerated Adaptation: Shahed Drones 16
The Costliest Losses: Deep Strikes 18
Shift of the Year: UGVs in 2025 18
Scaling Asymmetry: Ukrainian USVs in 2025 19
The Persistence of Simplicity: Low-Tech Decisions in a High-Tech War 19
Sapsan: Ukraine's Long-Awaited Ballistic Missile 20
Beyond Hacks: Cyber Operations as a Tool of Battlefield Disruption in 2025 20

Sources 22

Section I:

Frontline Update

Northeast (Sumy–Vovchansk–Kupiansk–Lyman):

Along the South Slobozhanskyi axis, Russian forces intensified assaults on Vovchansk, seeking to disrupt logistics toward Vovchanski Khutory and advance toward Vilcha, Tsehelne, and Tykhe. In the Kupiansk direction, Ukrainian forces conducted counteractions, pushing Russian units out of Kupiansk, Myrne, Radkivka, Holubivka, and Kindrashivka. Russian troops advanced north of Lyman near Serednie, Novoselivka, and Kolodiazi. Further advances were recorded from the Yampil direction toward Ozerne and Lyman. In Sumy Oblast, Russian forces attacked Hrabovske.

East (Siversk–Konstantynivka–Dobropillia–Pokrovsk):

The situation in the Pokrovsk–Myrnohrad agglomeration remains critical. Russian units continued pressing into Pokrovsk, while Ukrainian forces retained control of approximately 40 percent of the city. Enemy troops also advanced in Myrnohrad and near Novoeconomichne, with reports indicating Russian presence across the urban area, operating from concealed positions and conducting intermittent fire engagements. Russian forces occupied Sukhyi Yar, Lysivka, Novopavlivka, Hnativka, and Rih. Russian units took control of Siversk, entered Serebrianka, and advanced near Dronivka, Sviato-Pokrovske, Zvanivka, Vyimka, Pazeno, Pereizne, and Orikhovo-Vasylivka, moving toward Minkivka. The Kostiantynivka direction remains among the more stable sectors in terms of the ratio of assaults to territorial gains; Russian forces continue to attack Kostiantynivka and nearby settlements, probing toward Predtechyne, Stupochky, and Kleban-Byk. The enemy continued efforts to develop an offensive toward Dobropillia, with advances recorded toward Sofiivka, Shakhove, Nykanorivka, and Volodymyrivka.

South (Oleksandrivka–Huliaipole–Orikhiv):

Russian forces continued attacks in the areas of Andriivka-Klevtsove, Zelenyi Hai, Oleksandrohrad, Vyshneve, Rybne, Zlahoda, Krasnohirske, and Pryvilne. With additional forces committed, Russian units reached the central parts of Huliaipole, also captured Solodke, and moved toward Pryluky, Varvarivka, and Zelene. On the Orikhiv axis, Russian forces attempted to advance toward Lukianivske and Pavlivka, while fighting persisted around Stepnohirsk. Russian units advanced along the shoreline of the former Kakhovka Reservoir, conducting infiltration toward Malokaterynivka.

Containerized Stand-Off: Russian Improvised Tank Protection

Recent footage shows Russian forces fielding a low-tech survivability modification: **standard maritime ISO containers mounted over tanks**, likely modified T-80BVMs. The result is a vehicle encased in a **steel shell with crude cut-outs for the main gun and exhaust.**

Container walls, typically made of 1.5–2 mm Corten steel, do not provide armor protection. However, similar in function to the so-called "Tsar-Mangal" cage structures, they can **force premature detonation on an external structure**, shifting FPV explosions away from the hull and slightly reducing blast and fragmentation effects. They do not defeat shaped-charge warheads or anti-tank munitions.

The trade-off is unfavorable. Even after modification, the added **mass (~2 tons) reduces mobility, stresses the powertrain, restricts turret movement, and degrades situational awareness**, all critical in a drone-saturated fight.

Overall, the containers offer marginal survivability gains at disproportionate cost. More importantly, they underline a deeper reality of the war: high-end, scalable counter-drone solutions are absent, leaving both sides to rely on crude, improvised measures driven by urgency rather than effectiveness.

Two Tanks With Maritime ISO Container "Armor". Source: region22ua

Crossing Without Soldiers: UGVs Take on High-Risk Engineering Tasks

In December, documented footage showed Russian **logistics UGVs conducting an engineering task traditionally performed by troops**: **preparing a shallow river crossing in a kill zone.** One ground drone deposits stone into the riverbed while a second UGV compacts the fill, creating a passable route. Tasks that once required infantry or engineer units under direct threat are increasingly reassigned to unmanned platforms to reduce personnel risk.

The episode reflects a broader shift observed throughout 2025: **UGVs have moved beyond trials and niche use and are now deployed for logistics, resupply, evacuation, and increasingly for field engineering tasks.** Even with limited autonomy, they are effective at taking repetitive, high-risk work in UAV-saturated environments. As reliability improves, UGVs are consolidating their role as standard battlefield tools, setting the stage for the broader adoption of engineer and strike-capable variants in 2026.

First UGV Dumps Stones Into The Riverbed. Source: LandminesAndCoffee

Second UGV Compacts The Stones. Source: LandminesAndCoffee

Tactical Adaptation: Logistics Platforms as Modular Strike Systems

At the end of 2025, the NC13 Strike UGV Company of the 3rd Assault Brigade conducted **Operation Alphabet**, **employing a single mid-size UGV to neutralize a fortified enemy infantry position**. The platform was primarily designed and routinely used for logistical missions but was deliberately repurposed into a strike asset, carrying a stacked payload of 12 anti-tank mines. Operating in complex terrain and despite repeated Russian FPV interdiction attempts, the UGV traversed more than 20 km under remote control.

The payload was remotely detonated, **destroying a fortified enemy position** located inside a building below ground and **liquidating all enemy personnel inside**, assessed to be approximately **one infantry squad**. Ukrainian infantry secured the area without a direct assault.

The operation demonstrates Ukraine's **expanding UGV tactics**, with l**ogistics platforms increasingly used as modular strike systems**. This approach **reduces infantry exposure** and continues to blur the line between using UGVs as support and as direct attack assets. It also reinforces the growing role of UGVs as a first-contact tool for neutralizing hardened positions before infantry maneuver.

Mines Mounted On The UGV. Source: Third Army Corps

UGV Approaches The Enemy Position. Source: Third Army Corps

Detonation Of The UGV. Source: Third Army Corps

Mining, Reconnaissance, and Starlink: The Expanding Battlefield Role of Molniya-2

Toward the end of 2025, Russia expanded the **Molniya UAV's mission set through modular enhancements, including remote minelaying, reconnaissance, and Starlink-based control.** In December, imagery confirmed a Molniya variant configured for **remote anti-personnel mine deployment** using an externally mounted, servo-actuated release mechanism.

The appearance of a reconnaissance-configured Molniya-2R reflects the platform's expansion beyond one-way strike missions, repositioning it as a reusable ISR asset rather than a disposable munition.

The Molniya-2R setup employs a commercial computing stack built around a Raspberry Pi 5 paired with a Chinese Mini PC F8 rebranded under a Russian shell entity and **operating on licensed Windows 11.** Beyond the standard forward FPV camera, the platform features a SIYI ZR10 electro-optical sensor with a **10× optical zoom and three-axis stabilization**, expanding the observation and fire-correction ranges previously unavailable to the Molniya series. Crucially, all **Molniya series are now capable of routing video, telemetry, and command-and-control links via Starlink**.

This modification removes dependence on local RF relay chains, reduces vulnerability to electronic warfare, and significantly extends operational reach.

FPV Drone Of The Airplane Type Molniya-2R. Source: Defence Intelligence of Ukraine

Molniya-2 UAV Adapted For Remote Minelaying. Source: bpla_inform

Russian Molniya With Starlink Terminal. Source: saintjavelin

Rising Tempo, Rising Costs: Ukraine's Strike Campaign in Occupied Crimea

December strikes in occupied Crimea continued Ukraine's systematic campaign against Russian military infrastructure. Crimea has become a military hub, reinforced with radar systems, missile defenses, aviation, and naval platforms redeployed from across Russia. That concentration increasingly works against it.

Throughout 2025, Ukraine's Defence Intelligence and the Security Service of Ukraine steadily degraded Russia's integrated air-defense network in Crimea, **eliminating close to 500 radar systems**. In December alone, Ukrainian strikes **neutralized Russian military assets assessed at nearly $1 billion.**

Among the high-value targets identified were:

System	Estimated Cost
Three "Nebo-SVU" radar	$60–100 million each
55Zh6M "Nebo-M" radar	$60–100 million
92N6 radar (S-400 "Triumf" SAM system component)	$30–60 million
"Kasta-2E2" radar	$60–70 million
96L6E radar (S-300/400 key sensor)	$50–60 million
9S36M fire-control radar (Buk-M3)	$40–45 million
Pantsir-S2 air-defense system	$12–19 million
MiG-29 fighter	$30–40 million
MiG-31 fighter	$30–50 million
Two Su-27 fighters	$30–40 million each
Su-24 fighter-bomber	$24–30 million
S-300V launcher	$40–50 million

Ukraine also **struck storage and maintenance sites for uncrewed surface vessels near Myrne (December 24th)** and **Chornomorske (December 28th)**, disrupting Russia's ability to sustain naval drone operations in the Black Sea.

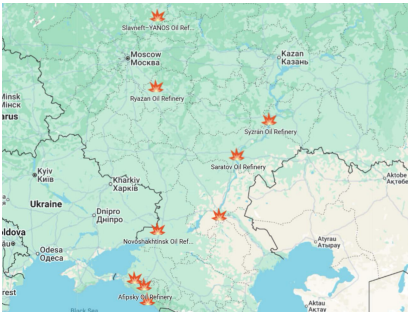
Additional attacks targeted Russian naval assets, including **a temporary basing point for vessels from the Dnipro River Flotilla in Olenivka, Crimea (December 22nd)**, and a **deployment area for high-speed landing craft of the Black Sea Fleet (December 26th)**.

Taken together, these strikes reflect a coordinated, multi-domain campaign aimed at weakening Russia's defensive architecture in Crimea, transforming what was once considered a fortified hub into a persistent operational liability.

Russian "Nebo-SVU" Radar Moments Before It Was Struck. Photo: Unmanned Systems Forces

December's Deep Strike Campaign: From Refinery Attrition to Maritime Energy Interdiction

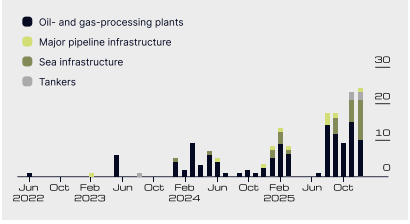
In December, Ukraine struck the **widest range of Russian energy targets observed to date**, spanning refineries and oil storage facilities, the Druzhba oil pipeline, Black Sea ports at Taman and Rostov, elements of the shadow fleet, and offshore oil infrastructure in the Caspian Sea.



December Strikes on Russian Oil Refineries. Source: robert_magyar

December's Sustained Pressure: Repeated Refinery Strikes Deepen Operational Uncertainty

After striking 14 oil-processing plants in November, Ukraine maintained the tempo in December, **attacking at least 10 refineries and at least 24 energy assets overall**, the highest monthly total recorded.



Hits On Russian Energy Assets 2022–2025. Source: Bloomberg

The repeated attacks on several facilities have intensified uncertainty regarding Russia's capacity to safely resume operations, even once repairs are finished. This, in turn, further complicates the prospects for consistent crude throughput and refinery reliability.

Notable refinery strikes in December included:

System	System	System	Estimated Cost
December 5	Syzran Oil Refinery	Capacity: 9 million tons Operational role: fuel supplier to the Samara, Saratov, and Penza regions, and the Russian military	Long-range strike damaged the AVT-6 primary processing unit, which accounts for about 70% of the plant's capacity, and halted operation.
December 28			The strike hit the ELOU-AVT-5 installation, a primary oil processing facility.
December 6	Ryazan Oil Refinery	Capacity: 17 million tons (top-5 largest) Operational role: produces 840,000 tons of aviation kerosene annually for the Russian Aerospace Forces	The ninth attack in 2025 on the refinery damaged the low-temperature isomerization unit, disrupting production of high-octane gasoline.
December 12	Slavneft-YANOS Oil Refinery	Capacity: 15 million tons (top-5 largest) Operational role: major fuel supplier for the central regions of Russia, including military logistics	Ukrainian drones damaged a CDU-4 processing unit, which handles about one-third of the plant's output, and a loading rack.
December 25	Novoshakhtinsk Oil Refinery	Capacity: 5 million tons (only refinery in Rostov Oblast) Operational role: primary supplier of petroleum products in southern Russia and directly fuels the Russian armed forces	For the first time, Storm Shadow missiles were used to strike the refinery, halting its operations.
December 26	Volgograd Oil Refinery	Capacity: 14.5 million tons Operational role: fuel flows along the Volga corridor	Ukrainian drones damaged the primary oil refining units AVT-1 and AVT-6, and the control cable for air coolers.

From Coastal Defense to Global Reach: Ukraine Strikes Russia's Shadow Fleet

In mid-December 2025, Ukraine's Security Service conducted its **first confirmed strike against a Russian shadow fleet tanker in the Mediterranean Sea neutral waters.** According to SBU sources, several long-range UAVs struck the Russian-owned tanker QENDIL, registered in Oman and sailing under the Omani flag, at a distance exceeding 2,000 km from Ukrainian-controlled territory.

The vessel was reportedly empty at the time of the strike, **sustained critical damage, and is no longer operational.** Moscow **has relied on such shadow fleet tankers to bypass international sanctions** and sustain energy revenues, financing the war. From both a legal and operational perspective, these vessels represent legitimate military-economic targets under the laws and customs of war.

Beyond logistics, the shadow fleet has increasingly supported hybrid operations, including suspected involvement in **subsea cable damage in the Baltic Sea and potential use as platforms for signals and electronic intelligence.**

The strike fits Ukraine's broader maritime campaign against Russian energy and export capabilities. In late November and early December, Ukrainian Sea Baby drones disabled the shadow fleet tankers Virat, Kairos, and Dashan, preventing them from reaching Novorossiysk to load oil.

The Moment Of The Drone Attack. Source: Pravda

The Caspian Line Crossed: Deep Strikes Against Russia's Caspian Oil Infrastructure

In mid-December 2025, Ukraine expanded its long-range strike campaign into a new strategic domain by targeting Russian offshore oil infrastructure in the Caspian Sea, challenging long-standing assumptions about the sanctuary of Moscow's rear-area energy assets.

The Filanovsky Oil Production Platform In The Caspian Sea. Source: NV

On December 11, **Ukrainian forces struck the Filanovsky offshore platform**, one of the largest developed oil fields in Russia's Caspian sector, **possessing reserves of 129 million tons of oil and 30 billion cubic meters of gas. At least four direct hits disabled critical equipment**, forcing the suspension of oil and gas extraction across more than 20 wells connected to the platform.

Targeted Oil Platform. Source: Security Service of Ukraine

On December 12, Ukrainian drones struck the Filanovsky platform and the nearby Korchagin platform, followed by a second strike on the Korchagin platform on December 15. Preliminary reporting indicates that critical equipment on both platforms was damaged, resulting in a halt to production.

On December 14, strike UAVs targeted the Valeriy Grayfer drilling installation at the Rakushechnoye field, damaging the platform's gas processing and pumping module and shutting down all 14 wells, which have a combined stated output of approximately 3,500 tons per day.

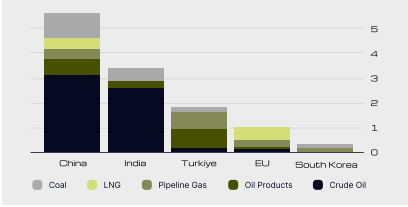
According to the available data, **the incapacitation of these three platforms targets 11% of Lukoil's domestic crude production.**

All strikes were conducted using long-range attack UAVs operated by the Security Service of Ukraine and Ukrainian Special Operations Forces, likely including FP-1, FP-2, and Lyutyi variants. The Caspian Sea's distance of roughly 900 kilometers from Ukrainian-controlled territory highlights the expanding reach and operational maturity of Ukraine's deep-strike drone capabilities.

The Drone's Onboard Camera Confirmed A Hit Near The Gas Turbine Unit. Source: Security Service of Ukraine

Cheap Oil, Fewer Buyers: How Sanctions Tightened Russia's Export Options

In December 2025, Russia's oil export system entered its most acute phase of strain since the initial post-2022 reorientation. The mechanisms that sustained volumes over the past three years–discount pricing, shadow fleets, and a narrow circle of compliant buyers–are now increasingly constrained. The stress is concentrated on Russia's three core outlets: China, India, and Turkey.



Russian Crude Oil Buyers in November 2025 (Billion EUR). Source: CREA

Russian crude imports to India are expected to drop significantly in December, falling to an **estimated 0.8–1.3 million barrels per day** from November's 1.9 million barrels per day. The decline follows intensified port inspections, expanded banking scrutiny, and tighter enforcement against shadow-fleet tankers. Indian authorities have intensified checks on certificates of origin, flag registries, and shipping documentation, while banks have slowed or blocked payments associated with sanctioned entities. These steps align with New Delhi's efforts to secure a broader trade deal with Washington, following the U.S. imposition of 50% tariffs on Indian goods in August, partly in response to India's purchases of Russian oil. Still, four of India's seven largest refiners remain active buyers of non-sanctioned Russian crude, drawn by widening discounts amid ample global supply.

China continues to take Russian oil, but only on increasingly restrictive terms. In mid-December, ESPO crude was sold to a Chinese independent "teapot" refinery at a discount of $7–$8 per barrel to Brent, the steepest seen this year. The pricing reflects a sharp decline in demand following the introduction of new U.S. sanctions targeting Rosneft and Lukoil, which have increased compliance risks across the trade. Before the war, Chinese state-owned refiners were the core buyers of ESPO. That role has now narrowed significantly, with large firms stepping back to avoid sanctions exposure. While China's overall seaborne imports of Russian crude are projected to rise to around 1.35 million barrels per day, the increase is driven by price opportunism rather than strategic expansion.

In mid-December, Russian crude deliveries to India, China, and Turkey fell to their lowest level since 2022. Turkey's imports were temporarily halted altogether.

By late December, Russia could still load barrels, but turning them into sales now requires steeper discounts, longer transit times, and heavier reliance on opaque intermediaries.

When Shaheds Shoot Back: Russia Arms Drones with Air-to-Air Missiles

Russia continues to experiment with new payloads, roles, and target sets for Shahed-type platforms, expanding their mission profile. In December, **Russia modified a Geran-2 to carry a Soviet short-range infrared-guided R-60 (R-60M) missile** mounted on an external pylon above the forward fuselage. While technically crude, the concept signals Russia's intent to contest Ukraine's growing dominance in counter-UAV air patrols.

The R-60 missile, **initially designed for fighter aircraft**, relies on a passive infrared seeker and does not require onboard radar illumination. When launched from an aircraft, its engagement range reaches up to 7–8 km; however, when deployed from a UAV, the effective range is likely to be drastically reduced. Target acquisition is dependent on visual confirmation through the drone's onboard cameras, with launch by an operator rather than autonomous targeting logic.

The concept is most effective when the missile-armed Shahed trails behind or operates slightly outside the main drone swarm, positioning itself to engage Ukrainian helicopters, light aircraft, or fighters such as the MiG-29 and Su-27 as they close in from the rear to intercept UAVs. In doing so, the interceptor aircraft exposes a hot engine and maintains a relatively stable flight profile, placing it within the missile's narrow forward engagement cone. Crucially, this escort role is only viable if the missile-armed Shahed maintains a live communication link with an operator. Russian forces are already converting Shaheds into FPV-like platforms with real-time control and video transmission, enabling operators to observe the airspace and manually authorize missile launches.

At the same time, the R-60's sensitivity to infrared countermeasures and its questionable rocket launcher mechanism, which can block the rocket itself, suggest that this is an experimental configuration rather than a mature capability.

Nevertheless, even limited deployment forces Ukrainian aviation to treat every detected Shahed as a potential air-to-air threat, complicating interception tactics. **Subsequent versions, if refined, could represent a more severe threat to counter-swarm interception efforts.**

Downed A Modified Shahed That Carried An R-60 Missile. Source: serhii_flash

Geran-2 UAV (series "Э", with R-60 missile). Source: Defence Intelligence of Ukraine

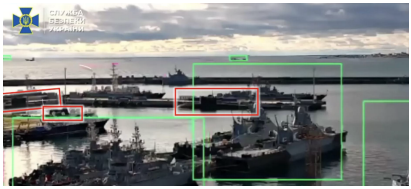
From Shadow Fleet to Submarines: Drones Drive Ukraine's Black Sea Campaign

On December 15th, the **Security Service of Ukraine reported a successful underwater drone strike against Russia's Novorossiysk naval base**, disabling a Project 636.3 Varshavyanka (Improved Kilo-class) submarine armed with Kalibr cruise missiles. According to Ukrainian officials, this marks the first confirmed use of underwater strike drones against a submarine of this class.

The operation employed Sub Sea Baby underwater drones and was conducted jointly by the SSU's 13th Main Directorate of military counterintelligence and the Naval Forces of Ukraine. The targeted submarine reportedly carried four Kalibr launchers that Russia regularly uses in long-range strikes against Ukrainian cities, energy infrastructure, and civilian targets.

The Varshavyanka class, often referred to as the "Black Hole" due to its low acoustic signature, represents one of Russia's most survivable conventional submarine platforms. **With an estimated unit cost of approximately $400 million and potentially rising to $500 million under sanctions, the disabling of such a vessel further reduced Russia's Black Sea submarine force to just two operational boats out of the original six.**

The results of this operation carry greater significance for Ukraine than merely disabling a single Kalibr launcher. After sustained Ukrainian strikes forced Russia to withdraw much of its fleet from occupied Sevastopol, Russia viewed Novorossiysk as its second primary naval hub and a relatively secure haven. The strike on the Varshavyanka submarine shows that the Russian fleet can no longer consider itself safe, even within the confines of the Novorossiysk naval base.



Three Kilo-Class Varshavyanka Submarines At The Moment Of The Strike. Source: YouTube H I Sutton

The Moment Of Impact. Source: Security Service of Ukraine

Britain's Underwater Front: Atlantic Bastion Takes Shape

The **UK Ministry of Defence has unveiled work on its Atlantic Bastion programme**, designed to enhance the protection of underwater infrastructure in British waters. The initiative will integrate warships and maritime patrol aircraft with autonomous underwater and surface vehicles to detect, monitor, and deter interference with critical subsea assets. The programme reflects lessons from the Ukraine–Russia war, where subsea infrastructure has emerged as a contested domain with strategic effects far beyond the frontline.

Since Russia's full-scale invasion of Ukraine, **the British government reports a 30% increase in the number of Russian vessels threatening UK waters**. Concerns intensified in November after the **Yantar, a Russian oceanic research vessel suspected of mapping British undersea cables and pipelines, shone lasers at RAF pilots tracking its progress near UK waters**. UK Defence Intelligence assesses that Russia is modernizing its naval capabilities, with a growing emphasis on targeting subsea infrastructure, including telecommunications cables and energy pipelines. These systems are critical to UK national resilience, carrying roughly 99% of international telecommunications traffic alongside vital electricity, oil, and gas supplies.

Beyond Starlink: Ukraine's Push for Sovereign Satellite Communications

Ukrainian company STETMAN is developing UASAT LEO, a sovereign low-orbit satellite constellation. The war has demonstrated that satellite communication is no longer a supporting capability but a decisive element of modern combat. **Ukraine's reliance on externally controlled systems such as Starlink and OneWeb has exposed a strategic vulnerability:** access to critical communications depends on foreign political and corporate decisions.

UASAT LEO plans to deploy up to 245 LEO communications satellites with domestically developed user terminals and ground infrastructure, compared with Starlink's roughly 9,300-satellite constellation.

The first satellite, UASAT-NANO, is scheduled for launch in October 2026, with a launch slot already reserved on a launcher and the satellite registered with the International Telecommunication Union, marking Ukraine's first ITU satellite filing in years. The UASAT LEO constellation aims to create a secure, dependable, nationally controlled satellite communication link for Ukraine's defense and critical infrastructure. This initiative is strategic, rather than commercial, benefiting both Ukraine and its partners.

Russia Launches Obzor-R: Step Toward Domestic SAR Reconnaissance

On December 25th, **Russia successfully launched a Soyuz-2.1a rocket from the Plesetsk Cosmodrome**. The payload was the Obzor-R No.1, **Russia's first dedicated space-based synthetic aperture radar (SAR) reconnaissance satellite**, whose launch had been repeatedly postponed since 2020.

The Obzor-R system has been in development since 2012 at RSC Progress and carries the Kasatka-R radar payload developed by NIITP. The satellite reportedly features an X-band AESA antenna measuring roughly 4 by 1.7 meters, designed to support high-resolution imaging. Russian sources claim a maximum resolution of around 1 meter, while some modern commercial systems, such as ICEYE or Capella, routinely achieve 0.5 meters.

Achieving orbit, however, is merely the first step. Obzor-R must then complete several critical phases: stabilization, antenna deployment, radar activation, and calibration processes. Sustained operational performance can only be evaluated after these steps are completed.

The threat of such a system was already proven in December, when it emerged that before the Russian strike on October 5, at least three Chinese SAR satellites flew over the western part of Ukraine. The correlation between satellite passes and Russian attacks indicates a growing level of information exchange between Russia and China. **If the Obzor-R system becomes fully functional, it would reduce Russian dependence on China and improve the ability to conduct all-weather, day-night surveillance.**

Comparison Of 1m And 0.5m Resolution. Source: kiber_boroshno

Starlink on Both Sides: How Starlink Is Reshaping the Communications Battlefield

In December, **the strategy of Russian forces shifted from disrupting the Starlink network to integrating its terminals into their own platforms**, directly challenging Ukraine's electronic warfare.

Ukrainian units report that Starlink-equipped Molniyas are now detected daily, with early improvised installations replaced by standardized, factory-integrated mounts as an indicator of scaled deployment. Crucially, Starlink integration is no longer limited to aerial platforms. Recent engagements have **documented Starlink terminals mounted on Russian armored vehicles.**

Available evidence suggests that the aggressor faces no significant constraints in procuring Starlink terminals, relying on multiple supply channels. As a result, they can bypass Ukraine's electronic jamming and maintain control links at ranges and in environments where radio-based systems fail.

A parallel response is emerging through the evolution of capabilities. **Kyivstar has become the first operator in Europe to deploy Starlink's Direct-to-Cell technology, enabling standard 4G smartphones to connect directly to satellites for SMS**, with voice and data planned for 2026. The system works by satellites transmitting 4G/LTE signals that phones recognize as ordinary cell towers, enabling communication without ground infrastructure. Given that Starlink terminals are also actively used by Russian forces, **it can be assumed that the next step will be testing the Direct-to-Cell mode specifically for the Ukrainian Armed Forces**, followed by the possible shutdown of "grey" Starlink terminals.

Starlink On An Armored Vehicle. Source: serhii_flash

Russia Began Erasing Serial Numbers On Starlink Terminals. Source: serhii_flash

Selective Denial: Russia's IMEI Registry Play

Russia's planned introduction of **mandatory IMEI registration marks a deliberate shift toward treating civilian telecom infrastructure as a counter-UAV layer.** **The Ministry of Digital Development plans to launch a centralized IMEI database in 2026**, framing the initiative as a dual-use tool against phone fraud, gray-market imports, and the growing security risks posed by UAV operations. Officials argue that IMEI-level filtering would enable authorities to distinguish between civilian handsets and devices repurposed for drones, allowing for selective network restrictions rather than blanket mobile internet shutdowns.

Proposed amendments would **allow the FSB, in coordination with Roskomnadzor, to blacklist IMEI ranges associated with specific commercial models or manufacturers**, thereby expanding counter-UAV options without compromising nationwide connectivity. The system, however, creates a single point of failure: disruption or compromise of the IMEI database could trigger cascading outages across mobile networks. By 2027, IMEI–SIM binding may become mandatory, and by 2028, only registered devices would retain network access, potentially extending beyond phones to tablets and laptops.

Year Wrap Up

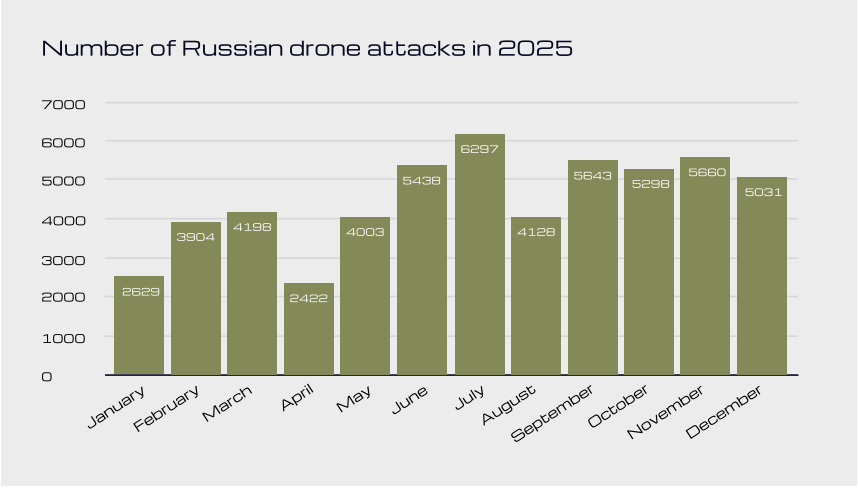
By 2025, Russia's war against Ukraine had evolved into a sustained contest of industrial endurance, technological adaptation, and long-range pressure rather than episodic battlefield exchanges. Homegrown missile systems, mass-produced unmanned platforms, and deep-strike campaigns reshaped the balance between front-line combat and strategic depth. It is this shift toward technology-driven, industrialized warfare that we seek to highlight in this edition of Defense Tech Monthly.

A Year of Accelerated Adaptation: Shahed Drones

In 2025, the employment of Russian Shahed drones entered a phase of operational stabilization. Following a summer peak, **monthly launch volumes remained at roughly 5,000–5,500 UAVs.**

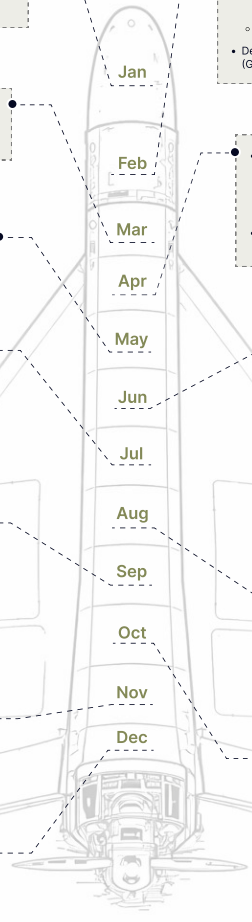
This pattern indicates that production had reached a functional plateau, with Russia shifting away from rapid escalation toward a more regulated and sustainable rate of use.

This adjustment reflects an effort to balance economic constraints while maintaining constant pressure on Ukrainian air defenses. It also enabled resources to be redirected toward incremental capability upgrades, even as Russia retained the ability to conduct short-term massed launches when operationally useful.



Number Of Shahed-Type Drone Attacks In 2025. Source: Air Force of the Armed Forces of Ukraine

Trend continuation 2025



- **High and rising mass-use tempo with large attack waves.**
- Shaheds are employed primarily to exhaust Ukrainian air defenses.
- Continued use of decoy drones alongside real strike UAVs.

- Sharp increase in launch intensity: ~140 drones per day (up from ~85 in January).
- **Multiple hardware upgrades introduced:**
  - Warhead mass increased to ~90 kg.
  - New anti-jamming satellite navigation antennas (8- and 12-channel CRP/Kometa).
  - Accelerated replacement of Western components with Chinese-made alternatives.
  - Widespread use of civilian electronics (Raspberry Pi, webcams, LTE modems, Telegram-based control).
  - Gerbera decoy drones fitted with explosive warheads.
- Development of a jet-powered Shahed-238 analogue (Geran-3) is underway.

- Near-daily bombardment continues.
- Sustained launch rates indicate expanding production capacity and stockpiles.

- Flight profiles adjusted from very low altitude to medium and higher altitudes:
  - ~1,500 m over land.
  - ~2,000–2,500 m above sea level.
- Shift aimed at complicating engagement decisions and worsening cost exchange for air defense.

- Introduction of combined-effect warheads, focused on infrastructure damage.

- **First operational use of Iranian Shahed-238 jet-powered drones.**
- Peak launch volume recorded at up to 200 drones per day.
- Counter-interceptor adaptations introduced.

- Recorded first use of the Shahed variants with cameras, radio modems, and AI-like processing modules, implying a move toward operator-in-the-loop control.
- Confirmed use of thermal imaging channels, allowing Shaheds to navigate without GPS and lock onto heat-emitting targets.
- Shahed deployment scaled up to roughly 180 units per day.

- Shahed drones integrated with Starlink.
- Drone incursions recorded in European airspace.
- Rail attacks intensify, focusing on locomotives and critical rail nodes.
- Gerbera is being used as a strike and reconnaissance drone.

- Launch tempo fluctuated:
  - Early August average: ~88 drones per day.
  - Late August average: ~133 drones per day.
- Shift toward systematic disruption of rail infrastructure rather than generalized terror strikes.

- Increased use of Shahed drones against air defense systems.
- Launch of 182 drones per day.

- **Expanded use of real-time operator control and night-vision cameras.**
- Further flight-profile experimentation, including periods of lower-altitude flight.
- Despite fewer launches than September, **strike effectiveness peaked at 18.7%**, the highest monthly rate observed.
- Increased use of jet-powered Shahed/Geran variants.
- Growth in sightings of camera- and modem-equipped Shaheds.
- Expansion of mission set beyond one-way strikes: remote minelaying using PTM-3 anti-tank mines.

- Experimental use of a modified Geran-2/Shahed-136 armed with R-60 air-to-air missiles: testing of Shahed airframes for roles beyond ground strike, including anti-helicopter and interceptor engagement.

The Costliest Losses: Deep Strikes

Over the course of 2025, **Ukraine's deep-strike campaign shifted from episodic demonstrations of reach to a sustained effort aimed at degrading Russia's industrial and logistical base.** Early strikes were largely limited in scale and focused on high-visibility targets. By mid-year, however, targeting patterns became more consistent, with repeated strikes against the same facilities.

By late summer, Ukrainian strikes expanded to **pipelines, pumping stations, chemical plants, drone and munition production facilities, and major rail junctions**, reflecting a shift from one-time disruption to forcing Russia to conduct continuous repairs, protect a growing number of sites, and divert resources from frontline needs. Re-strikes played a central role, extending downtime, preventing rapid restoration of damaged facilities, and deepening uncertainty over the ability to safely resume operations even after repair work.

By autumn, deep strikes were no longer framed as isolated raids but as a **cumulative industrial degradation effort that compounded economic strain and constrained Russia's ability to sustain high-tempo military operations.** By year's end, attacks were deliberately distributed in time and space, creating simultaneous pressure across multiple regions and reinforcing long-range strikes as a strategic tool of pressure.

Ukrainian forces attempted **at least 142 strikes against Russian refineries and oil depots in 2025, representing a 51 percent increase compared to 2024** and the highest annual total since the beginning of the full-scale invasion. Strikes in 2025 also reached greater depth than in previous years, **with targets hit up to 2,000 kilometers from Ukraine's borders.**

Alongside aerial systems, maritime and underwater unmanned platforms also played a role. Their low cost relative to the target value and the difficulty of countering compelled Russia to invest additional resources in port security, barriers, and protective measures. **Unmanned surface and underwater vehicles are increasingly supporting extended-range operations**, including acting as launch platforms for UAVs, which further expands the depth and persistence of Ukraine's strike campaign.

Long-Range Attack Drone "Lutyi" Used For Deep Strikes. Source: Focus

Shift of the Year: UGVs in 2025

In 2025, **UGVs reached a roughly similar maturity level to that of aerial drones in early 2023**: they are already operational, but not yet fully scalable. Throughout the year, UGVs demonstrated their battlefield value across core missions, including **frontline logistics, casualty evacuation, reconnaissance, and limited strike roles.** They transported hundreds of tons of supplies, reduced human exposure to fire, and saved thousands of lives, demonstrating that ground robotics is no longer experimental but operationally relevant.

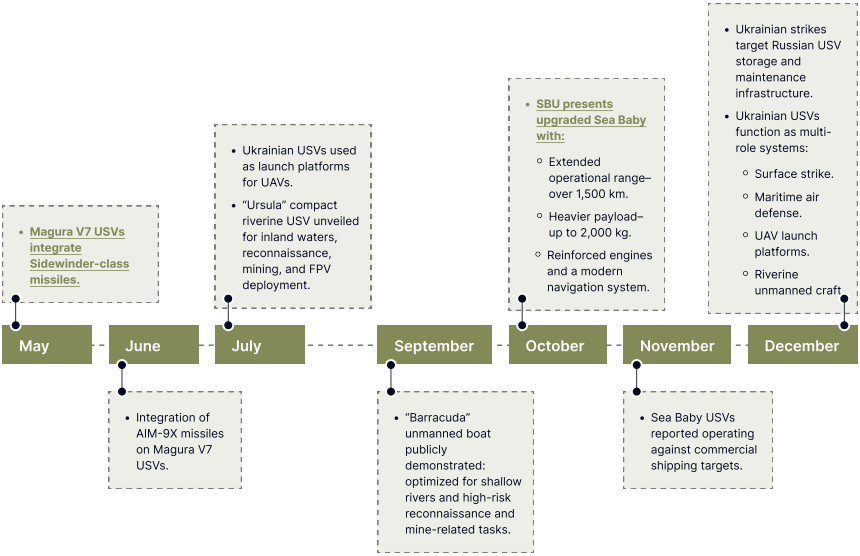
While **the formation of the first UGV battalion within the K-2 regiment** and the establishment of the first strike **UGV company "NC13" within the 3rd Separate Assault Brigade** were significant steps, critical weaknesses were significant steps, critical weaknesses persist in infrastructure, the availability of spare parts, the standardization of training, and the sufficiency of engineering personnel. To address some of these gaps, **the first dedicated strike UGV crash test was conducted in 2025**, organized by the NC13 strike UGV company together with the Snake Island Institute (SII), providing standardized, battlefield-driven validation of platforms, failure modes, and integration challenges across manufacturers.

The coming year is likely to mark the rise of strike UGVs as a defining feature of modern land warfare. At the same time, Russia is actively advancing its own UGV developments, stressing the importance of moving faster rather than merely keeping pace.

Scaling Asymmetry: Ukrainian USVs in 2025

By 2025, USVs had matured into an essential and integral part of Ukraine's maritime capabilities. No longer limited to niche strike roles, USVs have evolved into multi-mission platforms that integrate advanced payloads, extended range, improved navigation, and increasingly resilient command-and-control architectures.

Their growing technical capability reflects a shift toward systematic, scalable maritime warfare, enabling precision strikes against a wide range of Russian targets, including major surface combatants, patrol boats, naval infrastructure, port facilities, logistics hubs, and vessels linked to military logistics and sanctions evasion.



The Persistence of Simplicity: Low-Tech Decisions in a High-Tech War

In 2025, the Ukraine–Russia war has further underscored a critical reality of modern conflict: innovation does not always mean high technology. Under relentless attrition, financial constraints, and uneven access to advanced systems, militaries increasingly turn to low-tech solutions as the fastest way to address urgent battlefield problems.

On the ground, **inflatable and wooden decoy systems**, as well as **anti-drone nets**, continue to divert, disrupt, or prematurely detonate drones.

In the air, **pole-charge interceptor drones** exemplify mechanical counter-UAV solutions that favor reusability over sophistication.

Supporting this, **low-power VTX settings and SD-card–based reconnaissance drones** avoid complex datalinks, trading real-time awareness for survivability.

Across the battlefield, **metal mesh and improvised cage structures are widely applied to pickup trucks, logistics vehicles, tanks, and APCs**, while Russian **"mangals" and ISO containers** mounted on armor remain commonly observed responses to FPV drone threats. Despite limited effectiveness, these crude stand-off measures persist because scalable active protection systems remain scarce.

Their continued use shows stagnation in protection technology but adaptability in field improvisation.

Taken together, these low-cost innovations show that in 2025, low-tech choices are not disappearing or radically improving–they are being sustained, reused, and modestly refined as practical answers to a high-intensity, resource-constrained war.

Sapsan: Ukraine's Long-Awaited Ballistic Missile

In 2025, Ukraine crossed a long-delayed threshold in indigenous **strike capability with the systemic deployment of the Sapsan ballistic missile**. After nearly two decades of production delays, Ukraine has finally closed the gap between its tube artillery and strategic strike assets.

The highly mobile Sapsan missile system has a destructive capacity and an estimated range of up to 500 km. Carrying a 500 kg warhead, it is effective against critical targets such as enemy infrastructure, logistics hubs, ammunition depots, and command posts.

The missile's quasi-ballistic trajectory, combined with active maneuvering and terminal speeds estimated at 6–7 Mach, significantly complicates interception by modern air and missile defense systems. A reported circular error probable of around 10 meters places Sapsan among the most accurate systems in its category.

From an operational perspective, Sapsan restores a sovereign long-range strike capability, enabling the engagement of key enemy targets in operational depth without reliance on foreign systems or dependence on external decisions. Crucially, Sapsan establishes the foundation of a national missile force as a permanent, systemic element of Ukraine's defense strategy.

Main Characteristics Of The Sapsan System. Source: Root Nation

Beyond Hacks: Cyber Operations as a Tool of Battlefield Disruption in 2025

In 2025, cyber activity in the Ukraine–Russia war intensified, shifting from larger attacks to tighter operational integration with strikes, logistics disruption, and state control. **A total of 3,018 incidents were recorded in the first half of 2025**, which represents a 17% increase in attack volume compared to the second half of 2024.

Due to the strengthening of cyber defense systems, the frequency of critical and high-level incidents decreased, while the number of medium-criticality attacks increased. Primary targets remained local government (34%), defense (23%), and general government (19%). Phishing (27%) and malware (21%) were the most common incidents.

Russia's shift toward **LTE-controlled drones** made telecom infrastructure a battlefield dependency, not a back-office function. Ukraine, meanwhile, expanded its offensive cyber operations beyond espionage into service denial and systemic paralysis, employing large-scale DDoS and destructive attacks aimed at disrupting operations within Russia.

The target set widened beyond strictly military assets: **Russian Aeroflot suffered widespread digital disruption**, while **Russian banks reported a sharp increase in cyber incidents**. At the same time, Russian cyber activity against Ukraine increased in volume, with broader use of automation and early AI-assisted tools to accelerate attacks.

In parallel, **Ukraine completed the nationwide rollout of the Delta digital command-and-control platform**, embedding cyber infrastructure directly into battlefield coordination and decision-making.

By the end of 2025, cyber operations had firmly established themselves as a core element of hybrid warfare, where leaks, intrusions, and espionage served as operational tools to support and synchronize wider military actions.

- 24 Canal. “Загроза не лише для України: чим небезпечні “Шахеди" з ракетою та куди цілитимуть”. 24 Canal, 2025. Link
- 24 Canal. “Росіяни бояться виходити в море: які ‘жирні’ цілі знищили бійці ГУР у Криму”. 24 Canal, 2025. Link
- Army Recognition. “Drone wreckage confirms that Russian forces employ Iranian Shahed-238 jet-powered drones against Ukraine”. Army Recognition, 2025. Link
- Bloomberg. “Chinese teapot buys Russian oil at deep discount after sanctions”. Bloomberg, 2025. Link
- Bloomberg. “India officials say Russia oil imports to drop on tighter checks”. Bloomberg, 2025. Link
- Bloomberg. “Ukrainian Strikes on Russia’s Energy Assets Hit a Monthly Record”. Bloomberg, 2025. Link
- Debuglies. “Exclusive report: Caspian Shock Doctrine — How Ukraine’s December 2025 kinetic strikes redefined asymmetric warfare against Russia’s energy rear”. Debuglies, 2025. Link
- Espreso TV. “Від Каспію до Середземномор’я українські дрони 'рвуть' нафтодолари Путіна — пояснюємо”. Espreso TV, 2025. Link
- Focus.ua. “Дрон-камікадзе "Лютий" в рейтингу «3 роки війни: ТОП 10 найкращих систем озброєння України»”. Focus.ua, 2025. Link
- France24. “Finland charges captain of Russian ‘shadow fleet’ tanker over Baltic Sea cable sabotage”. France24, 2025. Link
- Glavnoe. “У Ростовській області атаковано Новошахтинський НПЗ”. Glavnoe, 2025. Link
- Hromadske. “Ukraine hits the Russian oil platform in the Caspian Sea, a source says”. Hromadske, 2025. Link
- Instagram. “Ukrainian military reports indicate that Russian Molniya-2 kamikaze drones are using continuous Starlink connectivity”. Instagram, 2025. Link
- Institute for Science and International Security (ISIS). “Updated Analysis of Russian Shahed-136 Deployment Against Ukraine”. ISIS, 2025. Link
- Institute for Science and International Security (ISIS). “Updated Analysis of Russian Shahed-type UAVs Deployment Against Ukraine”. ISIS, 2025. Link
- IT Ukraine. “Phishing, Zero-Click Exploits & AI Attacks: Cyber Threat Trends in Ukraine in 2025”. IT Ukraine, 2025. Link
- Kyiv Independent. “Ukrainian drones struck Russia’s Syzran Oil Refinery, General Staff confirms”. Kyiv Independent, 2025. Link
- Militarnyi. “K-2 Regiment announces formation of unmanned ground systems battalion”. Militarnyi, 2025. Link
- Mind.ua. “Переможці номінацій Mind Reality Check: вибуховий рік українського ОПК — зростання в 15 разів та інше”. Mind.ua, 2025. Link
- Naval News. “First image of Ukraine’s Sidewinder-armed Magura V7 surface drone”. Naval News, 2025. Link
- Novaya Gazeta Europe. “Russia will register mobile phones using identifiers”. Novaya Gazeta Europe, 2025. Link
- Pravda. “Russia deploys jet-powered and advanced Iranian drones — evidence of new threats”. Pravda, 2025. Link
- Pravda. “Ukraine's Security Service unveils upgraded Sea Baby maritime drones with 1,500km range”. Pravda, 2025. Link
- Pravda. “Безпілотники СБУ повторно атакували російські нафтовидобувні платформи в Каспійському морі – джерело”. Pravda, 2025. Link
- Pravda. “СБУ уразила танкер тіньового флоту РФ у Середземному морі – джерело”. Pravda, 2025. Link
- Radio Svoboda. “СБУ уразила нафтовидобувну платформу Росії в Каспійському морі – джерело”. Radio Svoboda, 2025. Link
- Reuters. “Rosneft’s Ryazan refinery suspended crude processing after drone strike, sources say”. Reuters, 2025. Link
- Rigzone. “Ukraine Says It Hit Another Lukoil Field”. Rigzone, 2025. Link
- Root-Nation. “Зброя української перемоги: ОТРК 1КР1 “Сапсан””. Root-Nation, 2025. Link
- RussianSpaceWeb. “Soyuz launches first Obzor radar satellite”. RussianSpaceWeb, 2025. Link
- Skylinker. “Український супутниковий зв’язок - вже не мрії, а реальні плани”. Skylinker, 2025. Link
- Slovoidilo. “Дрони вночі вчергове атакували Волгоградський НПЗ Росії”. Slovoidilo, 2025. Link
- Snake Island Institute. “August Defense Tech Monthly”. Snake Island Institute, 2025. Link
- Snake Island Institute. “Defense Tech Monthly July 2025”. Snake Island Institute, 2025. Link
- Snake Island Institute. “Defense Tech Monthly — November” (PDF). Snake Island Institute, 2025. Link
- Snake Island Institute. “Defense Tech Monthly October Edition”. Snake Island Institute, 2025. Link

SOURCES

- Snake Island Institute. “SII_NEWS_September”. Snake Island Institute, 2025. Link
- Telegram @army_tv. “СБУ уразила вже третю нафтовидобувну платформу рф у Каспійському морі” Telegram, 2025. Link
- Telegram @bpla_inform. “Molniya-2 UAV adapted for remote minelaying” Telegram, 2025. Link
- Telegram @exilenova_plus. “Палає один із найбільших НПЗ росії — Ярославський” Telegram, 2025. Link
- Telegram @GeneralStaffZSU. “Сили оборони України продовжують завдавати результативних ударів по стратегічних об’єктах ВПК та нафтопереробної галузі росії” Telegram, 2025. Link
- Telegram @GeneralStaffZSU. “Уражено завод синтетичного каучуку, місце зберігання БЕК та інші об’єкти окупантів” Telegram, 2025. Link
- Telegram @GeneralStaffZSU. “Уражено нафтовий термінал «Таманьнєфтєгаз», склад боєприпасів та місце зберігання, підготовки і запуску ударних БпЛА” Telegram, 2025. Link
- Telegram @kiber_boroshno. “З’явилась новина про запуск російського військового SAR-супутника”. Telegram, 2025. Link
- Telegram @kpszsu. “Monthly reports”. Telegram, 2025. Link
- Telegram @LandminesAndCoffee. “Logistics UGVs conducting an engineering task” Telegram, 2025. Link
- Telegram @region22ua. “Maritime ISO containers mounted over tanks” Telegram, 2025. Link
- Telegram @robert_magyar. “Вночі Птахи 1 ОЦ СБС відпрацювали низку військових об’єктів у ТОТ” Telegram, 2025. Link
- Telegram @serhii_flash. “Застосування Старлінків у противника набирає масштаби”. Telegram, 2025. Link
- Telegram @serhii_flash. “Сьогодні вперше на Шахеді була виявлена ракета класу повітря-повітря Р-60”. Telegram, 2025. Link
- Telegram @serhii_flash. “Щодня ми фіксуємо удари БПЛА Молнія зі Старлінком”. Telegram, 2025. Link
- Telegram @ssternenko. “Безпілотники СБУ знову атакували російські нафтовидобувні платформи в Каспійському морі” Telegram, 2025. Link
- Telegram @usf_army. “Сили безпілотних систем нанесли значні ураження противнику” Telegram, 2025. Link
- Telegram @VictoryDrones. “KyivStar Starlink Direct to Cell (DTC)”. Telegram, 2025. Link
- Telegram @VictoryDrones. “Модификация «Герани-2»”. Telegram, 2025. Link
- The Guardian. “Russian spy ship escorted away from internet cables in Irish Sea”. The Guardian, 2024. Link
- The National Interest. “Why Russia Is Equipping Its Drones with Starlink Terminals”. The National Interest, 2025. Link
- The New Voice of Ukraine (NV). “SBU drones hit Russian oil production platform in Caspian Sea, halting its operations”. The New Voice of Ukraine, 2025. Link
- UK Government. “UK unveils new undersea warfare technology to counter threat from Russia”. UK Government, 2025. Link
- United24 Media. “Ukraine begins serial production of 1KR1 Sapsan ballistic missile system”. United24 Media, 2025. Link
- Verstka Media. “ВСУ совершили более 140 атак на российские НПЗ и нефтебазы за 2025 год”. Verstka Media, 2025. Link
- War & Sanctions. “FPV drone of the airplane type Molniya-2R”. War & Sanctions, 2025. Link
- War & Sanctions. “Geran-2 UAV (series ‘Э’, with R-60 missile)”. War & Sanctions, 2025. Link
- YouTube. “Russian Submarine hit in Dramatic Attack in Black Sea”. YouTube, 2025. Link
- YouTube. “СБУ вразила підводний човен рф у Новоросійську”. YouTube, 2025. 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

Editorial & Design Team

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

SNAKE ISLAND INSTITUTE