SNAKE ISLAND INSTITUTE

Defense Tech Monthly:

Ukraine-Russia Battlefield

Edition #5

October 2025

Section I:

Frontline Update

Northeast (Kupiansk–Lyman Axis):

Russian forces intensified assaults near Kupiansk, expanding their control in the central part of the city and now attempting to advance toward its southern districts to reach the crossing point at Kupiansk-Vuzlovyi. The situation along the eastern bank of the Oskil River remains relatively stable, though Russian units are trying to press forward along the railway near Stepova Novosilka. Near Lyman, Russian troops pressed attacks from Kreminna, Torske, and Dibrova toward Zarichne and captured most of Shandryholove. In October, Russian troops have reportedly reached the outskirts of Lyman.

East (Pokrovsk–Siversk Axis):

On the Pokrovsk Axis, the situation remains tense and contested, with the enemy's small infantry units reportedly reaching the railway line in the city center and entering the Shakhtarskyi and Sonyachnyi neighborhoods. Reports indicate that most of the city's south is under enemy control; however, experts stress that the incursions are limited and should not be considered a full loss of western Pokrovsk. Russian forces continue efforts to seize Chasiv Yar and Toretsk, create conditions to surround Kostyantynivka, encircle the Pokrovsk–Myrnohrad agglomeration, and move towards Siversk. In mid- to late October, Ukrainian forces launched a counter-offensive near Dobropillya, liberating Kucheriv Yar, Nove Shakhove, Suvorove, and nearby villages, pushing Russian troops several kilometers back.

South (Zaporizhzhia–Orikhiv):

In the Zaporizhzhia region, Russian attempts to advance toward Stepnohirsk have failed; Ukrainian units carried out successful counteractions, liberating Mali Shcherbaky, Shcherbaky, and partially Stepove. Throughout October, Russian forces intensified attacks along the Orikhiv axis, launching several large-scale mechanized assaults. Intelligence indicates Russian preparations for an escalation of offensive actions across the southern front, potentially aimed at diverting Ukrainian reserves from the Pokrovsk area and establishing a bridgehead on the right bank of the Dnipro River.

Ukraine Pushes UGV Warfare Forward: From Combat Breakthroughs to Battlefield Testing

Ukrainian forces are rapidly developing unmanned ground vehicle (UGV) capabilities through successful combat missions and systematic industry testing, establishing new standards for robotic warfare. "NC13" UGV unit of the 3rd Assault Brigade recently revealed details of a complex **operation inside enemy territory**. The crew navigated undetected through friendly positions, crossed the grey zone, and, unnoticed, breached enemy defenses. Despite communication interruptions, operators successfully **delivered three FAB-250 aviation bombs totaling 750kg and remotely detonated them**, marking the first known instance of aviation bombs being delivered by a UGV in modern warfare. The mission completely destroyed a single enemy crossing point across the water barrier, cutting off supply lines, halting mechanized assault operations, and compelling Russian forces to revise their offensive plans in the area entirely.

To accelerate battlefield-ready development, Ukraine conducted the country's first full-scale **strike UGV crash test on October 22–23**. Organized by the "NC13" strike UGV company of the 3rd Assault Brigade, together with the Snake Island Institute, AB3Tech, and the Third Army Corps, the event was designed to move beyond theory and expose manufacturers to the same unforgiving conditions that operators face at the front. It served as the practical continuation of the August Strike UGV Forum: problems identified in discussions were now stress-tested in the field.

"NC13" unit using UGV "Zmiy" to deliver three FAB-250. Source: 3rd Assault Brigade

Strike UGV Crash-Test. Source: Snake Island Institute

Strike UGV Crash-Test. Source: Snake Island Institute

Manufacturers operated from a **dugout without line of sight, relying only on onboard cameras and a Mavic drone while navigating through** mud, trenches, debris, mined lanes, and more than 5 km of broken terrain. Any UGV that became stuck was left in place as an obstacle for others, recreating the cascading failures common in real missions. Thirteen strike UGVs participated, representing manufacturers including DevDroid, FRDM, UGV Robotics, Moroz, Rovertech, Tank Bureau, Terra Traverse, Overland Defense, Zhyraf, Ukraina Tekhnolohichna and Ark Robotics.

"Until recently, **100% of the UGVs we received had to be completely refitted**," said Makar, commander of the strike UGV company "NC13". "That's enormous work the military shouldn't have to do." He emphasized operators need to understand system vulnerabilities, not just advantages. Teams received detailed feedback on key areas, including maneuverability, mounting systems, battery performance, and cable protection. **Less than 40% of UGVs completed the crash test**, underscoring the need for more robust engineering standards. The 3rd Assault Brigade, together with its partners, is committed to creating an ongoing communication between manufacturers and operators.

Another notable development for the UGV community this month was the **expansion of the e-points program to include UGVs**. Troops who earn combat bonuses for verified target destruction can now exchange those points for verified UGVs, giving units a direct pathway to acquire the platforms they need without relying solely on centralized procurement.

Strike UGV Crash-Test. Source: Snake Island Institute

Russia Expands "Mothership-FPV" Precision Strike Tactics Across the Front

Russian forces have increasingly shifted toward **precision FPV attacks delivered by "mothership" UAVs**, a tactic now being reported across multiple frontline sectors. These larger carrier drones, **often Molniya-type platforms, transport several FPVs deep into Ukrainian airspace, releasing them near the target area for a strike**. This method preserves FPV battery life, improves terminal guidance accuracy, and reduces the chance of early detection. Ukrainian sources report some attacks used **commercial LTE** as a control channel: motherships ferry FPVs to areas with reliable mobile coverage, release them 5–10 km from the objective, and the FPVs then switch to cellular control.

A recent example occurred on 25 October in Kharkiv, where two FPV drones carried by a Molniya UAV struck residential structures in the Shevchenkivskyi district. While the physical damage was limited, the incident illustrates the broader pattern: Russia is transitioning from massed, high-visibility drone salvos to small, distributed, low-cost precision strikes that complicate Ukraine's air-defense planning and force a wider, more resource-intensive defensive posture.

FPV drone delivered by Molniya. Source: Serhii Flash

Ukrainian Intelligence Strikes Weaken Russian Air Defense Network in Crimea

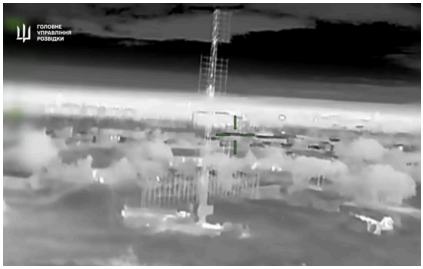
Defence Intelligence of Ukraine (HUR) has executed a sophisticated **multi-wave strike campaign against Russian air defense infrastructure** in occupied Crimea, eliminating several cutting-edge radar systems.

On October 20, HUR operatives destroyed a **Russian "Valdai" radar complex** at Dzhankoy airbase - one of Moscow's most advanced counter-UAV platforms. The system, featuring a three-coordinate X-band radar with optoelectronic tracking and electronic warfare integration, was specifically engineered to detect small drones at ranges from 300 meters to beyond 15 kilometers.

In a coordinated follow-up operation, HUR's elite "Ghosts" unit penetrated Russian airspace to destroy three separate radar installations: a 96L6 radar integral to the S-400 "Triumph" system, a P-18 "Terek" radar, and a 55Zh6U "Nebo-U" radar. The strikes also damaged a BK-16 high-speed landing craft.

The **systematic destruction of Russian radar systems**, including the Valdai counter-drone platform, signals a growing vulnerability in Moscow's defensive architecture. Ukrainian UAVs are now regularly penetrating systems built specifically to counter them.

By **degrading these radars and creating localized "blind spots"** across Crimea, Ukraine is applying a cost-effective strategy in which relatively inexpensive drones disable far more complex and expensive air-defense assets. This dynamic forces Russian commanders into a difficult trade-off: reposition limited systems and risk exposing other sectors, or tolerate reduced coverage in areas of high strategic value. In either case, Ukraine gains greater tactical freedom along the southern front.



55Zh6U "Nebo-U" radar. Source: HUR

Extended-Range Guided Bombs Marks Evolution in Russian Aerial Strike Capability

In October, Russia introduced a significant tactical innovation in its air campaign against Ukraine: **guided glide bombs equipped with jet engines that can strike targets up to 200 kilometers**, placing previously secure rear areas at risk.

First documented in spring 2025, these UMPB-5R bombs had already demonstrated their extended reach with strikes on cities like Lozova, hit from 130 kilometers away, and Poltava. Russia simultaneously developed improved aerodynamic kits for FAB-500T bombs, pushing their range beyond 100 kilometers even without jet propulsion. But it was October that marked the true escalation in their operational use.

On October 17, Russian forces launched a record 268 guided aerial bombs (KABs) in a single day against Ukrainian positions, delivered primarily by Su-34 fighter-bombers operating from safe distances beyond Ukrainian air defense reach.

While KABs are classified as precision-guided munitions, they are far from the most accurate weapons in Russia's arsenal.

Their effectiveness relies more on volume and destructive power than pinpoint accuracy, with targeting precision significantly lower than modern cruise missiles or dedicated precision strike systems. This lower accuracy poses particular risks to Ukrainian civilians, as strikes frequently impact residential areas and civilian infrastructure.

New UMPK for FAB-500T bombs for Su-34.Source: Militarnyi

The threat escalated further when, on October 24, Russia struck Odesa Oblast for the first time with these extended-range weapons. While air defenses intercepted two of three bombs, the attack exposed Odesa's vulnerability to aerial bombardment that defenses cannot always counter.

The following day, Kamianske in Dnipropetrovsk Oblast experienced a similar strike. Located over 120 kilometers from the front line, monitoring resources tracked three high-speed munitions before explosions rocked the city, which had previously only faced drone, cruise missile, and ballistic missile strikes.

The UMGB-5R system uses Chinese-made SW800Pro-Y turbojet engines from Swiwin Company, originally designed for large drones.

This addition transforms conventional glide bombs into powered munitions capable of reaching targets up to 200 kilometers from launch. The weapon carries approximately a 100kg warhead and allows Russian Su-34 aircraft to strike deep into Ukrainian territory while remaining safely behind front lines.

This development creates serious problems for Ukrainian air defenses. While the October 24 interception showed these weapons can be defeated, Ukraine's Deputy Intelligence Chief Vadym Skibitsky confirmed Russia has begun mass production, suggesting the threat will intensify.

Urban Reconnaissance Advances with Fiber-Optic Drone Use

Ukrainian operators have adopted a specialized tactic for urban warfare reconnaissance, utilizing **fiber-optic drones to explore multi-story residential buildings** on the front lines.

Unlike radio-controlled drones, whose signals are severely degraded or completely blocked by concrete walls and building structures, fiber-optic drones **maintain a clear, uninterrupted video feed** through a thin optical cable that trails behind the aircraft as it flies. This technology provides operators with a reliable picture even deep inside buildings, **where traditional RF-controlled drones would lose connection**. The fiber-optic link is immune to electronic warfare jamming and physical obstacles that plague radio signals in dense urban environments.

Innovations like fiber-optic reconnaissance drones provide critical intelligence advantages in the complex, signal-degraded environment of multi-story buildings.

Fiber-Optic Drones inside destroyed apartment building. Source: Shershni Dovbusha

Low-Tech, High-Impact: Ukrainian Pole-Charge Method Adopted by Russia

Russian drone operators have begun using a counter-UAV technique first used by Ukraine, mounting poles on drones for **multiple-mission capability.** Ukrainian operators originally developed the **stick method to physically ram** Russian Zala reconnaissance drones. Russia has now refined this approach by adding a small explosive charge to the pole's end, enabling standoff engagement while preserving the drone for reuse.

The system works through direct contact - the operator maneuvers their drone to strike the enemy UAV with the explosive tip. Upon detonation, the blast destroys or disables the target while the carrier drone remains operational and flies back for rearming.

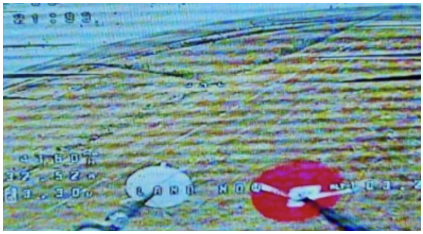
This represents a cost-effective solution in the drone-intensive environment of the conflict, where preserving reusable platforms offers significant advantages over single-use interceptors. The method enables operators to maintain continuous counter-drone operations using the same familiar equipment, thereby building experience with each mission while minimizing equipment losses.

Russian Interceptor Striking Ukrainian UAV "Shark". Source: https://t.me/texBPLA/212

Russian Reconnaissance Tactic for Locating FPV Drone Operators

Russian forces have developed a new method to **locate Ukrainian FPV drone operators along the front lines**. Reconnaissance drones equipped with high-capacity batteries patrol over tree lines, vegetation, and settlements, recording multi-spectrum video signals directly to SD cards. After returning to base, analysts review the footage to identify FPV drone video signatures that reveal operator locations.

This technique exploits a common Ukrainian security practice: using low-power VTX settings to avoid distant radio interception stations. While this defeats remote monitoring, it fails against close-proximity surveillance. Russian reconnaissance drones operating overhead can easily capture even milliwatt-level transmissions during the critical launch phase simply by being near the source.



Reconnaissance drones with multi-spectrum antennas. Source: Serhii_flash

The method's effectiveness lies in its simplicity. By recording locally, operators avoid the distance limits and weak signal problems that affect traditional radio direction-finding systems.. For Ukrainian pilots, this means reducing transmission power no longer provides adequate protection when adversary platforms can loiter directly overhead. Any signal strong enough to control a drone is potentially detectable by airborne surveillance assets within the immediate tactical area.

Russia Returns to WWI-Era Aerostat Barriers for Critical Infrastructure Protection

Russia is reviving a century-old air defense concept to counter daily Ukrainian drone strikes on critical infrastructure. **Aerostat barrier systems, large tethered balloons with nets suspended between them**, create aerial barriers capable of intercepting drones at altitude, including high-speed models. The technology has been upgraded with reinforced cables specifically designed for modern UAVs, offering superior protection compared to ground-based nets mounted on masts.

Aerostat barriers provide passive, continuous protection and remain effective even in GPS-denied or communications-jammed environments, making them a practical kinetic option for point defense of high-value industrial sites where securing specific facilities is more feasible than wide-area coverage.

However, despite their technical advantages, the cost-effectiveness of aerostat barriers remains uncertain. Reports indicate that a single aerostat barrier system **may cost upwards of 9 million rubles (around US $110,000)** and requires up to a month to deploy, making widespread adoption challenging.Continuous 24/7 operation is also difficult to maintain, so the systems are likely to be raised only during periods of increased threat. While they provide localized protection for critical infrastructure, their scalability and practical value for large-area defense have yet to be demonstrated, leaving their overall effectiveness and economic justification in question.

Aerostat Barriers.Source: Defence Express.

October's Deep Strike Escalation: Ukraine Transitions From Disruption to Systemic Attrition

Ukraine's deep strike campaign in October 2025 built on September's momentum while introducing new dimensions of strategic warfare. The month saw Ukrainian forces expand beyond oil infrastructure to target chemical plants with Western precision weapons and execute innovative attacks on critical infrastructure that severed Russian supply lines.

Oil Refineries: Sustained Pressure on Russia's Fuel Complex

October maintained relentless pressure on Russia's energy sector. By mid-month, Ukrainian strikes had **reduced Russia's fuel exports to their lowest levels since early 2022**, with refining output falling below 5 million barrels per day, a nearly 10% decline representing the lowest level in over three years.

The Kirishi refinery in Leningrad Oblast, with an annual capacity of 17.7 million tons (6.4% of Russia's total capacity), was struck on October 4, sparking fires visible from St. Petersburg. On October 23, **the Ryazan refinery**, Russia's fourth-largest. suffered a hit that forced shutdown of its main CDU-4 unit with capacity of 4 million tons per year, triggering cascading failures across neighboring units.

Deep interior strikes continued throughout the month. **The NS-Oil refinery in Ulyanovsk Oblast** came under attack on October 28-29, with residents reporting up to **eight explosions at the 600,000-ton capacity facility**. The same night saw strikes on **the Mariysky refinery in Mari El** and facilities in Orenburg and Stavropol regions.

In occupied Crimea, Ukrainian drones struck **oil depots in both Simferopol and Hvardiiske on October 29**. The Simferopol depot, critical for supplying Russian forces, erupted in flames that spread across multiple storage tanks. Early in the month, **the Orsknefteorgsintez refinery in Orenburg Oblast** (annual capacity 6.6 million tons) was hit by drones.

Satellite imagery from October 3 confirmed the **Sukhodolnaya oil pumping station near Rostov-on-Don was completely offline following the October 1 strike**, with extensive fire damage across the facility and surrounding fields ablaze.

Sukhodolnaya oil pumping station. Source: Maxar.

Strategic Escalation: Storm Shadow Strikes Chemical Warfare Production

October 21 marked a significant escalation when Ukrainian forces employed UK-supplied Storm Shadow missiles against **the Bryansk Chemical Plant**. The General Staff confirmed "a massive combined missile and air strike was carried out, including the use of air-launched Storm Shadow missiles, which successfully penetrated the Russian air defense system."

The Bryansk facility produces gunpowder, explosives, and rocket fuel components for artillery shells and missiles used against Ukrainian cities. The strike, conducted jointly by Ukraine's Air Force with the Navy and Land Forces, demonstrated sophisticated multi-domain coordination and the effectiveness of Western precision weapons against hardened military-industrial targets.

The Bryansk Chemical Plant. Source: Telegraph

On October 3, Ukrainian drones also hit the Azot chemical plant in Perm region, one of Russia's largest nitrogen fertilizer producers and a **key supplier of chemicals used in explosives**. The facility briefly halted operations after two explosions, though it later resumed production.

Infrastructure Warfare: The Belgorod Dam Strike

UAF cut off Russian units near Vovchansk by deploying drones, knowledge of the terrain, and operational awareness. On October 25-26, Ukrainian drones struck the Belgorod Reservoir dam, 13 kilometers north of the border. This targeted strike severed a crucial supply route that Russian forces had been using to support units that had crossed the Siverskyi Donets River, effectively isolating them from their main forces.

A Russian military truck sunk on one of the supply routes. Source: United24

Ukraine's 16th Army Corps reported **"enemy logistics have become significantly more complicated"** with Russian trenches and bunkers flooded, roads washed away, and supply lines severed. The dam's direct support of Russian military operations, enabling troop crossings and sustaining supply lines, placed it within the bounds of legitimate military targets according to **Article 56 of Additional Protocol I to the Geneva Conventions, which permits attacks on works containing dangerous forces when they provide "significant and direct support to military operations"**.

Strategic Impact and Economic Consequences

By late October, the cumulative impact became undeniable. The International Energy Agency warned **Russian oil companies would continue feeling the effects of Ukrainian attacks for nearly a year**, with one in three refineries hit since August. **The IEA forecast refining output unlikely to return to normal levels before June 2026.**

Russian authorities acknowledged **gasoline shortages in over 20 regions**, with long lines at filling stations and sales restrictions. Moscow banned gasoline exports, suspended all fuel import tariffs through June 2026, and for the first time stopped publishing regional fuel availability data. Retail **gasoline prices rose 2.58% in September alone**, the steepest monthly increase since 2018.

Western Support and Operational Tempo

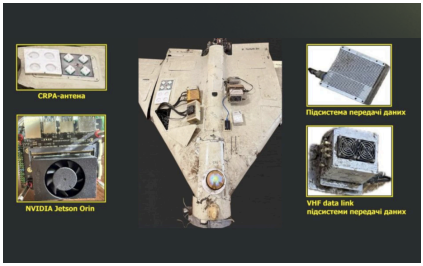
Reports in mid-October revealed **the United States had been providing intelligence** to help plan long-range drone strikes since summer 2025, including flight routes, altitude, and timing to evade Russian air defenses. The successful Storm Shadow integration demonstrated the effectiveness of Western precision weapons against high-value targets.

Russia Deploys Shahed Drones Equipped with First Person View Camera in Railway Strikes

Russian forces have introduced a significant upgrade to their drone arsenal: **Shahed UAVs equipped with night-vision cameras and real-time operator control**, demonstrated in coordinated attacks on Ukrainian railways in early October 2025. On October 1, multiple drones struck a fuel train **150-200 kilometers inside Ukraine, with operators using live video feeds to disable the locomotive** before systematically targeting fuel cisterns. Three days later, similar strikes hit **Shostka's railway station and a passenger train**, while knocking out the city's power grid.

The Shahed-236 variant represents a major technological leap from autonomous models. **Ukrainian intelligence first identified the system** after downing a prototype in June 2025, revealing Iranian origins and an Nvidia Jetson Orin processor capable of AI-powered target recognition. The complete system includes strike drones, communication relay drones, and ground control stations, **enabling precision attacks up to 220 kilometers away under manual guidance**. Captured 2022 documents indicate Iran charged **Russia approximately $900,000 per** Shahed-236 with an optical station, nearly five times the cost of standard Shaheds, reflecting advanced technology transfer costs.

Beyond camera-equipped variants, Russia has introduced **Shahed drones with incendiary warheads** containing liquid **napalm-like mixture weighing approximately 90 kg**. Recent modifications also include **fragmentation-high-explosive warheads with LiDAR sensors enabling airburst detonation at preset altitudes for maximum effect**. The Russian defense industrial complex now deploys multiple warhead types ranging from 40-90 kg, including thermobaric, high-explosive, and combination fragmentation-incendiary models.



Components of a Russian Shahed drone. Source: Militarnyi

Russia's Nuclear Weapon Claims: Strategic Bluff or Breakthrough?

Russia's announcements of successful tests of the nuclear-powered "Burevestnik" cruise missile and "Poseidon" underwater drone have drawn widespread skepticism. **Moscow claims Burevestnik flew 14,000 km over 15 hours on October 21** and that **Poseidon activated its nuclear reactor**, but the technical evidence remains unconvincing.

A nuclear ramjet would emit a detectable radioactive exhaust. **Norway's military intelligence confirmed a launch** from Novaya Zemlya but could not verify the 15-hour flight, and Norway's Radiation and Nuclear Safety Authority reported no radiation spike despite **highly sensitive monitoring stations**.

This leaves several possibilities: the test was shorter than claimed, the radioactive plume has not yet reached sensors, or Russia achieved a rare breakthrough in closed-loop reactor cooling. Historically, Burevestnik has only two partial successes out of 13 known attempts.

The timing of the announcement appears intentional. Former U.S. intelligence officer Scott Ritter suggested President Donald Trump was “confused” by the Russian statements and reacted by calling for a resumption of U.S. nuclear testing.

Ultimately, Russia may not need a fully functional system to achieve strategic effect.In the information domain, perception can be as powerful as capability, and Moscow’s well-timed ambiguity has successfully shaped the geopolitical narrative.

In the information domain, perception can be as powerful as capability, and Moscow’s well-timed ambiguity has successfully shaped the geopolitical narrative.

Launch of the 9M730 'Burevestnik during one of the tests. Source: Wikipedia

Altitude Adjustment: Shaheds Now Flying Lower to Complicate Ukrainian Interceptors

In recent weeks Ukrainian air-defense units have observed a notable shift in Shahed flight profiles. Earlier this year we reported on a period when Shaheds were flying unusually high, routinely staying far above the engagement ceiling of mobile fire groups. This month, however, multiple units along the frontline have documented Shaheds flying lower than their typical cruise altitude.The adjustment complicates work for interceptor drones, which depend on altitude to target, build speed and execute reliable collision angles.

At the same time, the lower flight band once again brings Shaheds into the effective range of mobile fire teams equipped with heavy machine guns and MANPADS. The emerging pattern suggests Russia is experimenting with flight geometries to evade radar coverage and confuse layered defenses, trading protection from interceptors for renewed vulnerability to ground fire.

Ukraine's Sea Baby Evolution: Longer Range, Heavier Payload, Bigger Effects

Ukraine's Security Service has introduced an **advanced generation of Sea Baby surface drones**. The new Sea Baby variants demonstrate technical specifications that significantly broaden their mission profile. The extended **operational range exceeding 1,500 kilometers**, while offering only marginal tactical advantages in Black Sea operations where the previous 1,000-kilometer range already provided access to targets as distant as Rostov-on-Don, holds considerable strategic implications. This expanded envelope suggests **potential operations beyond the Black Sea region**, while also enabling **extended loitering periods for sustained surveillance or time-sensitive strike missions**. Perhaps most significant is the **doubling of payload capacity to two tons**, which transforms these platforms from single-mission strike assets into **potential "mothership" configurations** capable of deploying multiple payloads or supporting more complex operational concepts. The platforms build upon weaponization efforts demonstrated earlier in 2024, including **gyro-stabilized machine gun systems with automated target recognition and naval-adapted 122mm Grad rocket** arrays with ten launch tubes. The enhanced range and payload parameters transform these existing systems into strategic assets capable of sustained operations in distant theaters and sequential mission profiles.

The latest generation's enhanced range and payload capacity represent a **strategic evolution of an already proven platform**, transforming it from a coastal denial asset into a capability that can project power well beyond the Black Sea theater. By combining these expanded parameters with adaptive weapon systems in an autonomous platform, Ukraine has developed an asymmetric naval capability that forces conventional naval powers to fundamentally recalculate their operational planning.

Ukrainian Sea Baby naval drone with a machine-gun mount. Source: SSU

Project Harmony: How Russia Built Hidden Network Beneath the Arctic

Russia has secretly built an Arctic undersea surveillance grid, "Harmony", to protect its nuclear submarine fleet. The project's goal is to deploy an **"invisible web" of seabed sensors and fiber-optic links** stretching from Murmansk to the Franz Josef Land archipelago.

Experts say the system gives Russia a strategic edge, **allowing its submarines to leave port undetected and stay hidden in the open ocean, maintaining the ability to launch a nuclear counterstrike even** if its land-based missile forces are wiped out.

"Harmony" poses a serious security concern, limiting intelligence-gathering and giving Russia even more control over its nuclear capabilities. Investigations by several media outlets published in October revealed that the **"Harmony" project heavily relied on Western maritime technologies**. For years, Russia was buying sensitive hydroacoustic systems, underwater drones, antennas, and hundreds of kilometers of fiber-optic cable through its shell companies (e.g., the Cyprus-based Mostrello Commercial Ltd), acquiring equipment from the United States, Great Britain, Norway, Italy, and Sweden.

Despite years of sanctions, Russia's ability to procure Western technology for the "Harmony" project reveals **significant weaknesses in export-control enforcement**. The continued flow of critical dual-use equipment to Moscow demonstrates that sanctions alone cannot prevent determined state actors from accessing sensitive technologies through intermediaries.

Russian Satellites Actively Stalking British Military Assets

Russia has escalated space warfare against Western military infrastructure, with its satellites **actively tracking British assets** and jamming them weekly since the Ukraine invasion began.

According to the head of the UK Space Command , Maj Gen Paul Tedman, Russian satellites equipped with specialized sensors position themselves near UK military satellites **to collect intelligence, while ground-based systems conduct persistent electronic interference**. Britain maintains only six dedicated military satellites for communications and surveillance. The UK has deployed counter-jamming technology, but harassment continues unabated. Both Russia and China have tested anti-satellite weapons, with warnings of potential Russian space-based nuclear capabilities. The UK is now **testing laser-threat detection sensors** against directed-energy weapons that can disrupt satellites. While the UK has introduced counter-jamming measures, the disruptions remain relentless.

Testing of anti-satellite weapons by both Russia and China, coupled with concerns over potential Russian nuclear systems in space, has prompted Britain to develop laser-detection sensors to guard against directed-energy attacks on satellites.

Satellite. Source: Holyrood

Europe's Three Aerospace Giants Unite to Counter Global Space Competition

The security risks of Starlink dependency in military operations have become increasingly apparent, particularly through Ukraine's experience with service disruptions and external control over critical battlefield communications. In response, three major European defense contractors: Airbus, Leonardo, and Thales, have reached a historic agreement to consolidate their satellite and space divisions into a single enterprise.

This new European entity will focus on key defense technologies: encrypted military communication networks, satellite-based intelligence and surveillance capabilities, and autonomous navigation infrastructure free from foreign dependency.

The collaboration directly addresses the strategic weaknesses revealed by military dependence on commercial providers such as SpaceX's Starlink in recent warfare.

European leaders view this consolidation as vital for developing independent space-based defense capabilities, which have grown increasingly crucial for continental security. Subject to regulatory clearance, the joint venture is scheduled to launch in 2027 and represents Europe's determination to establish its own military space infrastructure amid escalating competition with U.S. and Chinese space initiatives.

Russia's Rolling Internet Blackouts: High Economic Cost, Minimal Impact on Ukrainian Drones

Our August Defense Tech Monthly first examined Ukraine's mobile-network-enabled drone operations and Russia's early reaction. As Ukrainian drones **penetrate deeper into Russian territory** using civilian mobile networks for guidance and targeting, the Kremlin has resorted to a desperate countermeasure: **nationwide internet shutdowns**.

Since May, Russia has imposed over **2,100 mobile data blackouts** across dozens of regions, creating rolling connectivity crises. The defense strategy, however, comes at devastating economic cost. A single day of nationwide shutdowns drains roughly **$323 million from Russia's economy**, with **Moscow alone losing $115 million per shutdown**. Businesses lose revenue, card payments stall, and civilians revert to cash transactions and SMS-based money transfers.

Meanwhile, Ukrainian engineers accelerate innovation. Long-range drones like the Lyutyi now employ **multi-channel communication systems that automatically switch between LTE, radio, and satellite links** when primary signals fail.

Newer Ukrainian systems increasingly rely on direct Starlink connections and autonomous machine-vision navigation, rendering mobile network dependency obsolete.

Russia's blanket approach - **blocking foreign SIM cards for 24 hours** and testing whitelist systems requiring CAPTCHA verification, proves both technically crude and economically ruinous. The strategy fails to account for Ukraine's technological leapfrog: as **drone systems evolve toward autonomous targeting and satellite communications**, Russia's network shutdowns become increasingly irrelevant to actual drone operations **while devastating civilian infrastructure and commerce**. The result: massive economic hemorrhaging for negligible military gain, a calculation that increasingly favors Ukraine's technological adaptation over Russia's network warfare.

Chinese Radars Power Russia's Drone Defense Network

October 2025 marks a critical shift as compact **Chinese radar systems become the backbone of Russia's anti-drone operations**. **OSINT researchers confirmed** deployment of FSTH-LD02 and FSTH-LD03 radars, manufactured by China's Zhejiang Fanshuang Technology, with Russia's 22nd Anti-Aircraft Missile Regiment. These commercial systems, originally designed for airport security, now provide targeting data for drone interceptors along the front.

The FSTH-LD03 offers **15-kilometer range with 10-meter accuracy**, while the LD02 delivers 10-kilometer detection but superior 5-meter accuracy. Both weigh under 21 kilograms, consume just 1.2 kilowatts, and achieve 0.3-degree angular precision, enabling rapid mobile deployment. Russian forces use these radars against Ukraine's long-range strike UAVs including UJ-22 Airborne and "Liutyi" drones targeting oil refineries.

Despite Western sanctions, the **radars reach Russia through Hong Kong shell companies**, disguised as industrial equipment and routed through Kazakhstan, UAE, and Turkey. Russia is building a cost-effective, **scalable radar network using commercial technology** at a fraction of military-grade costs, creating increasingly dense surveillance coverage that forces Ukrainian drone operations to adapt while demonstrating that commercial dual-use technology from neutral suppliers now determines battlefield outcomes.

FSTH-LD02 radar. Source: Defence UA

Russian hackers turn to AI as Cyber Weapon in War on Ukraine

Russian cyberattacks on Ukraine have intensified dramatically, with over **3,000 incidents reported in the first half of 2025**, a **20 percent increase from the previous year**. However, a concerning shift is underway: as Ukrainian defenses strengthen, Russian hackers are turning to artificial intelligence to maintain their offensive edge.

Ukrainian cybersecurity officials report that attackers are now using AI not only to craft convincing **phishing messages but also to generate malicious code**. This automation allows hackers to launch faster, more frequent attacks while evading traditional detection methods.

Facing more effective Ukrainian defenses, Russian operators have abandoned outdated tactics in favor of quicker "Steal & Go" operations - stealing what they can before disappearing. They're also exploiting zero-click vulnerabilities that infect systems without requiring user action. Adding another dimension to the threat, Moscow continues **coordinating cyber operations with missile and drone strikes to maximize disruption**. Despite these evolving tactics, Ukrainian defenders say they're managing to keep pace, detecting and neutralizing roughly as many infections as they discover. After three years of full-scale war, **the cyber battlefield remains a critical front in Russia's** broader conflict with Ukraine.

Ukrainian Drone Platform Milpilots Hit by Targeted Cyberattack

The Ukrainian military drone coordination platform Milpilots.com has disclosed a **significant security breach spanning** September to October 2025. Hackers compromised a pilot code on September 5th, exploited server vulnerabilities to access the database, and uploaded malware disguised as legitimate software that infected approximately 30 users.

The breach exposed **all pilot access codes, user profiles, and RX/TX encryption keys**, though attackers failed to obtain the critical TX_LOCK key generator that secures live drone communications. Ukraine's Cyber Security Center (unit A0334) is actively investigating affected users and has blocked attacker FTP access to prevent further file uploads. The platform developers are implementing a phased user deactivation and reverification process while transitioning to a more secure system already in development.

Users are urged to change passwords immediately and minimize stored personal information. Notably, computers equipped with **military-grade antivirus software from the Cyber Security Center successfully prevented data loss**, highlighting a critical gap in civilian antivirus solutions' ability to detect targeted military threats.

The Milpilots breach exemplifies the evolving threat landscape facing defense coordination platforms. As drone warfare becomes increasingly central to modern combat operations, securing the digital infrastructure connecting operators, aircraft, and command systems has emerged as a frontline cybersecurity challenge, one requiring specialized military-grade protection beyond civilian security standards.

Rubikon: Anatomy of an Elite Russian UAV Formation

Established in the summer of 2024 on the basis of one of the UAV combat units, the Russian elite Rubikon drone unit became one of the most effective formations within the Russian Ministry of Defense. Rubikon is a higher-level organization responsible for centralized procurement and development of unmanned systems, the implementation of tactics, methods, and procedures for employing ground and naval drones, as well as the training of operators.

The structure of the Rubikon Centre for Advanced Unmanned Technologies includes the following groups:

- Centre for Development of Unmanned Systems and Ground Robotic Complexes: responsible for system design, integration, and bespoke ammunition.
- **Training Centre for Recruits**: focused on preparing drone technicians and pilots through a 1.5-month training course.
- Analytics Centre: engaged in SIGINT/ELINT analysis, target selection, and operational planning.
- Combat Detachments: each detachment reportedly possesses its own logistics and evacuation units.

Starting as a "**small group of 5–7 people**" in the spring of 2025, the unit rapidly expanded into seven detachments of roughly 130–150 personnel each.

By autumn 2025, the formation had grown to twelve detachments, operating across every major sector of the front and total personnel estimated at between 5,000 and 6,000.

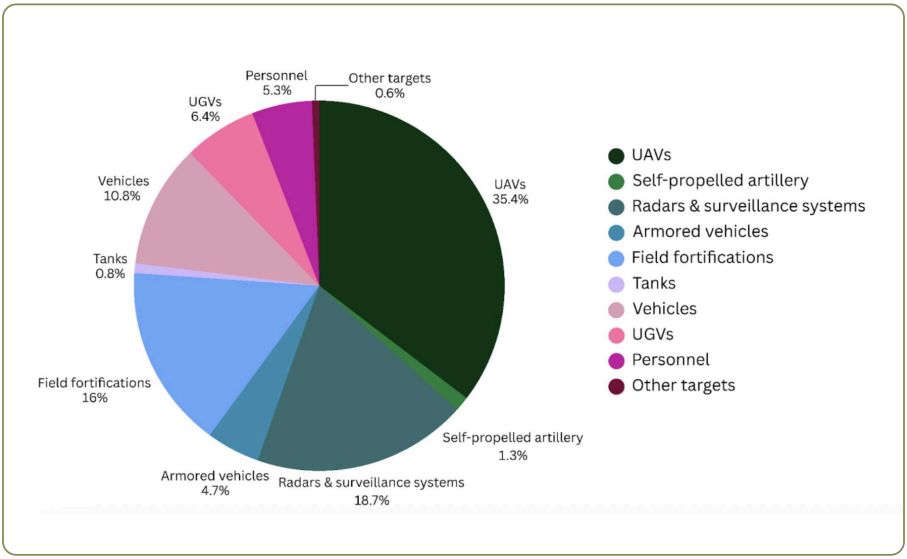
Rubikon employs almost all major strike and reconnaissance drones used by the Russian Armed Forces, except for the Shaheds. These include both standard and fiber-optic FPV drones such as the VT-40 and KVN, strike UAVs like Molniya and Lancet, reconnaissance drones produced by ZALA, Orlan UAVs, SuperCam systems, and specialized air-defense drones. In the summer, naval drones were added to this list as well, with intelligence indicating an increasing threat of Rubikon's expanding activity at sea.

With one of its main goals being the destruction of Ukrainian logistics, Rubikon played a crucial role in the Kursk front, preventing Ukraine from properly supplying its troops and enabling Russia to push the Ukrainian Armed Forces back. With its strong electronic-intelligence capabilities, Rubikon units have systematically targeted Ukrainian drone operators who fly from positions far behind the front lines.

In October 2025 alone, they struck 2,063 targets, surpassing the 2,000-mark for the first time since the unit's inception and exceeding September's result (1,883 targets) by 9.5%.

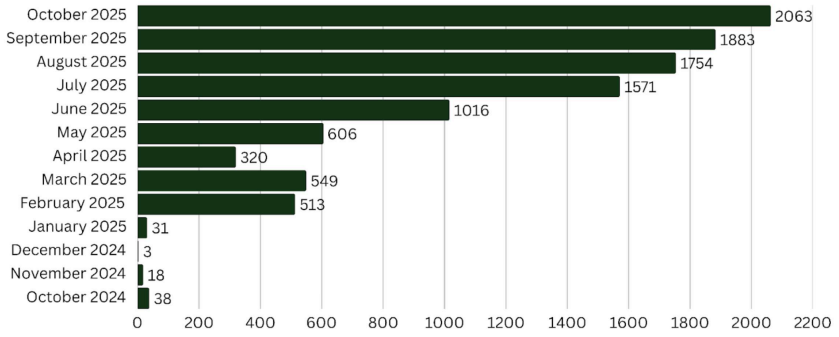
Breakdown of main target types hit in October 2025

- UAVs — 721
- Radars & surveillance systems — 382
- Field fortifications — 327
- Vehicles — 220
- UGVs — 130
- Personnel — 107
- Armored vehicles — 95
- Self-propelled artillery — 26
- Towed guns — 25
- Tanks — 17
- Other targets — 13

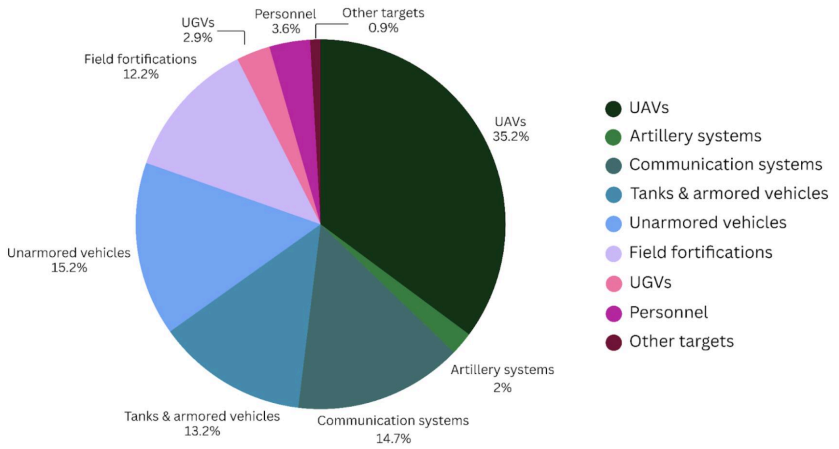


Breakdown of main target types hit in October 2025. Source: Center Rubikon

In late October, approximately 14 months after the creation of the Center, Rubikon reached a total of 10,000 confirmed hits. If the milestone of 5,000 destroyed targets was recorded in early August 2025, a year after the Center was created, it took just over two and a half months to reach the next 5,000.



Number of Rubikon's confirmed hits. Source: LostArmour



Structure of engaged targets over the entire period. Source: LostArmour

Why do Rubikon's tactics work?

- One of the strengths of Rubikon is **rapid prototyping to fielding**. According to Russian sources, team organisation within Rubikon is "**marked by freedom of technical choice, limited formalism, and an emphasis on initiative**."
- Rubikon's horizontal organisational model links front-line UAV operator experience with a network of enthusiasts, small workshops, and minor factories, while substantial Ministry of Defence financing allows serial production of successful prototypes.

- Each detachment is deployed to a **clearly defined sector of the front with a very narrow and specific mission**, making Rubikon an effective instrument of localized tactical pressure. Each Rubikon detachment has its own operational focus.
- Each unit developed its **own logistics and sustainment**. Reported organic logistics and casualty-evacuation detachments allow sustained deployment in contested sectors and reduce vulnerability to transient interdiction.

What lessons can Ukraine take?

The principal lesson is practical: adopt the practices of the Russian unit to take and scale up breakthrough solutions. **As noted in last month's report**, Ukraine needs a functioning strategic hub to identify disruptive ideas, resource them, and accelerate their transition into operational use.

Some experts propose appointing officers in every brigade to collect, validate, and scale proven technical and tactical solutions, since "adjacent brigades often do not know about or do not share field practices with one another."

Another recommendation is to form dedicated "Anti-Rubikon" hunter-killer detachments tasked with neutralising Rubikon crews by locating and striking the enemy's radar and sensor nodes, and to shift part of Ukrainian aerial reconnaissance onto cheaper, low-flying platforms for harder detection.

SOURCES

- 24 Kanal (24TV). “Russia struck the Shostka railway station twice — the city is left without gas and water.” 24 Kanall, 2025. Link
- BBC. “Russia targets UK military satellites on weekly basis.” BBC, 2025. Link
- Bloomberg. “IEA Sees Drone Strikes Weighing on Russia Oil Processing Till Mid-2026.” Bloomberg, 2025. Link
- CNN. “Ukraine and Russia’s intensifying energy war brings gas shortages and economic pain.” CNN, 2025. Link
- Defence Express. “Which radar-station of the ‘rashists’ should be sought for striking anti-drone calculations and why it is a priority target.” Defence Express, 2025. Link
- Defender Media. “Crash test of strike UGVs near Lviv: details and photos.” The Defender, 2025. Link
- Dev UA. “Russia massively disables mobile Internet on foreign SIMs and eSIMs.” Dev UA, 2025. Link
- Focus UA. “Balloon-barriers against Ukrainian drones: how Russia is fighting drones with First World War methods.” Focus UA, 2025. Link
- Forbes. “Russia Is Shutting Down Its Own Internet To Stop Ukrainian Drones.” Forbes, 2025. Link
- International Committee of the Red Cross. “API 1977 — Convention (IV) Relative to the Protection of Civilian Persons in Time of War.” ICRC Databases on IHL, 2025. Link
- Le Monde. “‘Russian Secrets’: How Russia built an Arctic spy network using European equipment.” Le Monde, 2025. Link
- Lenta.ru. “‘This is War 2.0.’ The secret Russian center ‘Rubikon’ trains drone pilots for the Air Defense Forces. What is known about it?” Lenta.ru, 2025. Link
- LOSTARMOUR. “Combat work of operators of the ‘Rubicon’ Center for Advanced Unmanned Technologies.” LOSTARMOUR, 2025. Link
- Militarnyi. “750 kg of explosives: a Third Assault Corps drone delivered and detonated three aerial bombs in enemy rear.” Militarnyi, 2025. Link
- Militarnyi. “Defenders of Pokrovsk destroyed an enemy combat UGV for the first time.” Militarnyi, 2025. Link
- Militarnyi. “Drones Attack NS-Oil Refinery in Ulyanovsk Region, Russia — Fire Reported.” Militarnyi, 2025. Link
- Militarnyi. “Ground robotic complexes now available for ‘e-points’: supply launched.” Militarnyi, 2025. Link
- Militarnyi. “New Russian Shaheds struck a Ukrainian railway echelon in Chernihiv region.” Militarnyi, 2025. Link
- Militarnyi. “Russia first attacked Odesa region with guided aerial bombs: two of three were shot down by air-defence.” Militarnyi, 2025. Link
- Radio Svoboda. “Secret ‘Rubikon’ of Russia: What It Does, Where It’s Based, and How It Succeeds on the Battlefield (investigation).” Radio Svoboda, 2025. Link
- Security Service of Ukraine (SBU). “SBU showed a new generation of the legendary maritime drones ‘Sea Baby’ – video.” SBU, 2025. Link
- The Guardian. “Ukraine war briefing: Storm Shadow missiles ‘hit gunpowder plant in Russia’.” The Guardian, 2025. Link
- The Hacker News. “From Phishing to Malware, AI Becomes [Russia’s] New Cyber Weapon in War on Ukraine.” The Hacker News, 2025. Link
- The Kyiv Independent. “One of Russia's biggest oil refineries halts most productive unit after drone attack, Reuters reports.” The Kyiv Independent, 2025. Link
- The Kyiv Independent. “One of Russia’s largest oil refineries reportedly suspends operations after Ukrainian attack.” The Kyiv Independent, 2025. Link
- The Kyiv Independent. “One of Russia’s largest refineries in southern Urals hit by Ukrainian drones, SBU source confirms.” The Kyiv Independent, 2025. Link
- The Kyiv Independent. “Ukraine attacks 2 oil depots, destroys military equipment in Russian-occupied Crimea, SBU source confirms.” The Kyiv Independent, 2025. Link
- The Record. “Russia blocks mobile internet for foreign SIM cards, citing drone threats.” The Record, 2025. Link
- The Record. “Russian hackers turn to AI as old tactics fail, Ukrainian CERT says.” The Record, 2025. Link
- The Telegraph. “Ukraine strikes Russia with British Storm Shadow missiles.” The Telegraph, 2025. Link
- Telegram @icpbtrubicon. “Breakdown of main target types hit in October 2025.” Telegram, 2025. Link
- Telegram @serhii_flash. “Reconnaissance drones with multi-spectrum antennas.” Telegram, 2025. Link
- Telegram @Shershni68. “Fiber-Optic Drones inside destroyed apartment building.” Telegram, 2025. Link

SOURCES

- Telegram @uamesser. “Ukrainian Drone Platform Milpilots Hit by Targeted Cyberattack.” Telegram, 2025. Link
- UK Defence Journal. “UK to defend critical satellites from laser threats.” UK Defence Journal, 2025. Link
- UNITED24 Media. “Videos Show Russian Soldiers and Equipment Washed Away After Dam Break in Belgorod.” UNITED24 Media, 2025. Link
- UNITED24 Media. “Washington is helping Ukraine hit Russia where it hurts most: its oil economy.” UNITED24 Media, 2025. Link
- X (Twitter) @bradyafr. “Sukhodolnaya oil pumping station.” X (Twitter), 2025. Link
- X (Twitter) @OsintExperts. “FSTH-LD02 radar.” X (Twitter), 2025. Link
- YouTube. “‘Ghosts’ of the Defence Intelligence of Ukraine on the hunt: in Crimea three radar stations and a landing craft of the Russians were hit.” YouTube, 2025. Link
- YouTube. “Revolution on the battlefield.” YouTube, 2025. Link
- YouTube. “Ukrainian Drone with a Stick Attacks a Russian Zala Drone.” YouTube, 2025. Link

SNAKE ISLAND INSTITUTE