SNAKE ISLAND INSTITUTE

Defense Tech Monthly:

Ukraine-Russia Battlefield

Edition #4

September 2025

Section I:

Frontline Update

Northeast (South Slobozhanskyi–Kupiansk–Lyman–Siversk Axis):

- Russia's operation in **Sumy failed to gain traction**, with forces redeployed elsewhere. Along the South Slobozhanskyi axis, Russian troops continue daily **assaults on Vovchansk** and intensify pressure toward Lyptsi in an effort to build a buffer zone. Kupiansk remains a focal point, with sabotage groups infiltrating the city and complicating Ukrainian defense. On the Lyman axis, Russian units **consolidated gains in the Serebrianka forest** and launched **repeated assaults on Shandryholove**, where heavy fighting continues amid conflicting claims of control. Further south on the Siversk front, Russian forces advanced toward the village of Serebrianka, seeking to destabilize Ukrainian lines along the **Oskil–Siversk corridor**.

East (Pokrovsk–Kramatorsk–Sloviansk):

- In the first week of September, Russian forces **launched 350+ assaults on Pokrovsk**, aiming to **encircle the Pokrovsk–Myrnohrad agglomeration**. In the Dobropillia sector, fighting focused on Kucheriv Yar, Zolote Kolodiaz, and Maiske, though Ukrainian defense stabilized the line by late September. At the same time, Russia **sought to establish fire control over the northern approaches to Sloviansk** in a broader push to seize the Pokrovsk–Kramatorsk–Sloviansk cluster, but Ukrainian forces have continued to hold ground.

South (Zaporizhzhia Front):

- Russian forces maintain pressure along the Zaporizhzhia axis, with repeated assaults near Novodanylivka, Mala Tokmachka, and Novoandriivka, and reported advances toward Novoivanivka, Kalynivske, and Udachne. Fighting continues in the Huliaipole sector around Poltavka, while localized clashes were noted near Kamianske, Plavni, and Prymorske, where Ukrainian defenses are holding. No confirmed breakthrough has occurred, but intelligence points to possible Russian reinforcements on this front, suggesting preparations for an escalation of offensive actions.

The Snake Island Institute is Ukraine-U.S. initiative dedicated to strengthening strategic cooperation in defense through:

- **Analytics:** Advancing understanding of modern warfare and doctrine
- **International partnerships:** Aligning Ukrainian, U.S., and international decision-makers
- **Defense Tech:** Enabling integration of critical technologies into combat operations

Editorial & Design Team

- **Viktoriia Honcharuk** – Director, Defense Tech at Snake Island Institute
- **Yaroslav Makodzeba** – Defense Tech Associate at Snake Island Institute
- **Serhii Halushko** – Independent Contributor
- **Oleksandra Balabukha** – Intern, Defense Tech at Snake Island Institute
- **Andrii Sheiko** – Intern, Defense Tech at Snake Island Institute
- **Olha Kovalenko** – Visual & Layout Design

The Decoy Arms Race: Countering Drone Reconnaissance

At operational ranges these **decoys closely resemble genuine systems**, forcing UAV operators to adapt with **multisensor verification, behavioral analysis, and database cross-referencing**. Both sides are escalating: as decoys grow more sophisticated, countermeasures now include thermal pattern analytics, AI recognition models, and enhanced operator training to move beyond single-sensor tactics.

Decoy M777. Source: Center Rubicon

This month Russian sources released footage of a strike drone hitting a **decoy M777 artillery system**. Earlier decoys were simple inflatables or wooden replicas, but **modern variants now combine mobility, thermal signatures, and firing simulations**: robotic platforms, solar-powered barrel heaters, and smoke launchers that mimic live fire.

Inflatable decoy Su-33. Source: Unian

Yet **full automation of decoy recognition remains out of reach**, the human factor continues to be decisive, underscoring a new level of technological competition.

Decoy M777 Howitzer with solar panel. Source: Decoy for frontline «Apate»

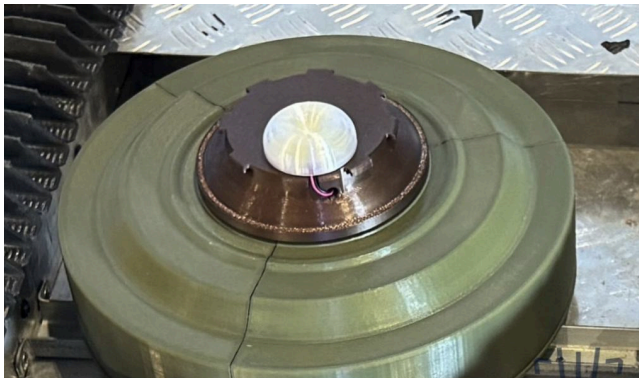
Minefield Modernization: Progress Toward Networked Defense Systems

The challenge of developing “smart minefields” is still largely unresolved: **Ukraine requires systems that are safe to deactivate, flexible, and remotely operated**. In the state of an unstable frontline, their main task is protecting troops and controlled minefields allow to minimize accidental risks to friendly forces as positions shift.

This month, Ukrainian defense firm **ZMIYAR unveiled a new smart minefield system**, advancing efforts in this field. A single controller can link up to 200 mines, reducing operator exposure and enabling centralized command. Integrated sensors provide remote monitoring of each mine's status and environment, modernizing management compared to standalone detonators.

Yet centralized designs also carry risk: a single controller malfunction can neutralize an entire field. That makes redundancy, robust C2, and lifecycle protocols just as critical as the detonators themselves.

Strategically, ZMIYAR's solution mirrors Ukraine's move toward data-driven, networked defense systems, but the key obstacle remains advancing from remote detonation to truly intelligent minefields that balance effectiveness, long-term safety, and international commitments.



T-62 anti-tank mine with a smart fuse from Zmiyar on a ground drone. September 2025. Source: Military

UGV Race: Hybrid Platforms on Both Sides of the Front

Following last month's UGV coverage, September brought two new entries. Vyriy Drone's Dzhankoi system, presented at Defense Tech Valley 2025, stands out for its **ability to launch up to six FPV drones directly from the platform**, transforming it into both a logistics vehicle and a mobile strike pad. A similar approach had earlier appeared in **the Karakurt UGV by Ukrainian company IRV**, pointing to a broader domestic trend toward hybrid ground–air platforms. Strategically, it reflects Ukraine's shift toward multi-role, networked platforms that combine ground and aerial capabilities. Russia has showcased similar UGV-FPV hybrids, **illustrating the race between Ukraine and Russia to field functional hybrid UGVs**.

At the same time, the Ukrainian MoD authorized the UNEX UGV, a domestically developed **amphibious ground platform** built on a unique chassis with extreme mobility across marshes, sand, ice, and even open water.Initial controlled tests suggest UNEX can roll over delicate items without damage, cross rivers, and overcome obstacles — indicating potential for difficult terrain. At the same time, its high cost raises questions about applicability on the Ukrainian battlefield, where the focus has been on cost-effective solutions. How well UNEX balances advanced capabilities with practical affordability remains to be seen.

Yet, like many expo-stage concepts, **Dzhankoi, UNEX, and Karakurt have not yet proven their capabilities on the frontline.**

Karakurt UGV. Source: Oboronka / Amphibious UNEX UGV. Source: MoD

Poland's Expensive Struggle Against Cheap Drones

On September 10, 2025, Russian Shahed/Gerbera drones breached Polish airspace, forcing NATO fighters, including Norwegian F-35s and F-16s from Denmark, the Netherlands, and the UK, to engage. The incident exposed a stark imbalance: Moscow spends as low as $10,000 per some of those drones used in the attack, while Warsaw spends millions to intercept them.

The growing disparity between NATO's reliance on expensive air-defense interceptors and Russia's use of inexpensive drones is driving Poland's urgent search for low-cost counter-UAS alternatives. The war in Ukraine has already proven that Shahed-type drones and FPVs can steadily deplete air-defense systems worth millions, creating an unsustainable cost exchange. Poland, on the front line of NATO, sees its current mix of Patriots, IRIS-T, and legacy artillery as either prohibitively expensive or operationally ineffective.

Warsaw is testing layered, lower-cost options from drone interceptors like AP-Flyer's ASSASIN to Poprad launchers with Piorun MANPADS and radar-guided guns. But analysts stress Poland should not reinvent the wheel: instead of chasing wholly new solutions, Poland and NATO can benefit most by drawing on Ukraine's hard-won experience. Kyiv has already begun providing instructors and technical expertise to Polish units, sharing battlefield-tested methods in detection, jamming, and drone-on-drone combat.

Just as critical as technology, however, is planning and doctrine: Ukraine's example shows that counter-UAS must be coordinated nationally, combining EW, interceptors, guns, and drones into a single architecture rather than siloed systems. Without adopting this layered, tactics-driven approach, NATO risks burning through resources faster than Russia expends drones, leaving frontline states like Poland dangerously exposed.

Reported Russian Drone Debris. Source: ISW

Ready-to-fly ASSASIN interceptor drone by AP-FLYER. Source: M. Dura

Air Space Control System: The Core of Russia's Counter-UAV Grid

In September 2025, Ukrainian intelligence identified the radar network powering Russia's growing drone interception capability. At its core is Rostec's Air Space Control System, supported by Enot, Raduga, and Chinese-supplied radars. This integration explains the improved effectiveness of units like Rubicon and Kochevnik against Ukrainian reconnaissance, strike drones, and rotary bombers.

The system operates in the S-band (2700–3100 MHz), **detecting UAVs out to 20 km**. Russia now fields four-panel 360° arrays, networked for overlapping coverage across frontline sectors. Positioned 5-7 km behind the front, often camouflaged in tree lines, they provide **real-time targeting data to interceptor crews 2-5 km forward**.

This creates a systemic challenge. Instead of chasing individual interceptors, **Ukrainian forces may need to prioritize the radar backbone**, striking installations and their power sources, which rely on continuous 1kW generators. At the same time, Ukraine must pursue its own networked radar and interceptor systems, coupled with adaptive drone tactics such as terrain masking and ultra-low flight profiles.

Radar station operator directing Russian interceptor. Source: Militarnyi

Dual-Camera Drones: Russia's Bid to Outsmart Interceptors

Ukrainian forces recently intercepted a Russian Gerbera UAV equipped with two cameras intended to detect and localize interceptor drones and air-defense assets by tracking their optical or thermal signatures. This setup helps Russian operators see when, where, and how Ukrainian interceptors are deployed, giving them insight into defensive tactics and timing. The Gerbera is cheaper than the Shahed, making it a logical testbed for such technology. Analysts suggest Russia may refine these dual-camera systems on Gerberas first before migrating them onto more expensive long-range UAVs. If successful, this could improve the survivability of strike drones, loitering munitions, or cruise missiles by allowing them to bypass or overwhelm Ukrainian defenses.

Although the development poses a growing challenge, intercepting and studying captured Gerberas gives Ukraine valuable intelligence on Russia's evolving suppression-of-air-defense strategy and an opportunity to adapt countermeasures accordingly.

Captured Russian "Gerbera" UAV, equipped with two cameras for visual detection of interceptor drones. Source: Militarnyi

Supply Routes Under Siege: Long-Endurance Ambush Drones

Russian fiber-optic drones along the road. Source: The New Voice of Ukraine

Russia has increasingly weaponized ambush tactics against Ukraine's fragile supply routes, shifting from simple FPVs to fiber-optic relay drones and **solar-assisted FPVs** that can loiter far longer and resist jamming. In contested sectors where only a few roads remain viable, attackers land small drones directly on key routes and keep them in surveillance mode for hours. When a convoy appears the drone launches and strikes on impact.

Fiber-optic linkages make these systems hard to defeat with conventional methods, and solar panels further extend standby time.

To blunt this threat, Ukraine should implement layered, route-focused countermeasures: install fixed camera and motion sensors at chokepoints such as bridges and narrow passes to spot landed drones visually; run reconnaissance sweeps ahead of convoys; maintain ready **interceptor drones to engage ambush UAVs before takeoff;** and vary routes and timing to reduce predictability. These steps emphasize detection and preemption rather than relying solely on jamming or costly kinetic intercepts.

A Russian improvised solar drone seen in the Kherson region. Source: New scientist

Flying Through Winter: How Russia Prepares Its Drones For Cold

September 2025 saw Russian engineers unveil an **anti-icing system intended to keep drones operational in extreme cold**. The design uses electrically conductive polymer threads woven into fabric panels that heat to prevent ice and snow from adhering to the airframe.

Russian developers, working under the National Technology Initiative platform, emphasize that the thread can reach up to 110°C, while also providing antistatic properties, electromagnetic shielding, and electronic detection capabilities.

Unlike metallic filaments, the polymer is lighter, easier to manufacture, and **produced entirely from domestic raw materials**. Analysts note, however, that durability is uncertain. Polymers can weaken after repeated heating cycles, especially in humid, freezing conditions. For Ukraine, the takeaway is significant: if Russia achieves reliable year-round UAV operations, cold weather will no longer suppress incursions. Counter-drone defenses will need to adapt to a battlefield where winter offers no respite.

Ukraine's Deep Strikes Broaden in Scale, Scope, and Impact

From Refinery Raids to Multi-Domain Pressure

Ukraine's long-range campaign in September 2025 demonstrated a qualitative extension of strategy. August's signature strikes on oil refineries not only persisted but also gained even greater traction. Russian media reported that by September 28, **38% of Russia's refining capacity around 338,000 tons per day was offline**. **About 70% of these outages were due to Ukrainian drone attacks, which alone disabled nearly a quarter of total refining capacity (≈236,000 tons per day)**

The result was dire: **1 million tons less gasoline was produced**, and there was a **20% shortage** in the domestic market. At the same time, Ukrainian drones and missiles targeted transportation hubs, radars, missile launchers, command posts, gas and chemical plants, pumping stations, fuel depots, and even naval assets. Although operational secrecy probably makes the actual number higher, at least **30 to 35 different facilities were confirmed** to have been impacted by open sources.

Oil Refineries and Fuel Infrastructure

The industry most frequently targeted was still the oil sector. Following a **SOF drone raid**, the Volgograd refinery, which has an annual capacity of over **14 million tons, was forced offline**. The Salavat refinery in Bashkortostan, which can produce 6.5 million tons annually, **was hit twice** on September 18 and 24. Images revealed massive fires that temporarily shut down the plant, and Ukrainian **UAVs traveled almost 1,400 kilometers to reach the location**.

Additionally, the Saratov refinery sustained damage, and in a coordinated raid, **two Ufa plants** that processed **over 20 million tons** a year were struck at the same time. **Ukrainian drones demonstrated their ability to strike deep strategic assets** when they made it to the Kirishi refinery in Leningrad Oblast, which is Russia's second largest refinery with an annual capacity of 20 million tons. The underground resistance group "Black Spark" helped **disable** the Ilsky refinery in Krasnodar Krai. In the meantime, **several shutdowns** were required in September due to persistent attacks on Rosneft's largest refinery, the Ryazan, which has a capacity **of 17 million tons**.

Fire erupts from the Kirishi oil refinery in Russia's Leningrad Oblast after a reported Ukrainian drone strike on Sept. 14, 2025. Source: Astra

In addition to refining, **Ukraine set a fuel base** in the Kardymovo district of Smolensk on fire and ignited a strategic fuel depot in **Rosrezerv** in Tver Oblast. Simultaneously, a **chemical plant in Krasnodar was forced offline**, and the Astrakhan gas processing plant **suspended production after drone strikes**. By the end of the month, Russian authorities acknowledged that there were gasoline shortages in over **20 regions**, resulting in lines at filling stations and restrictions on sales. This was the result of these cumulative blows.

Pipelines and Export Terminals

Ukraine purposefully put pressure on Russia's oil transit network. **Drones disrupted throughput** at the Tyngovatovo pumping station in Chuvashia on September 14. Satellite photos taken a few days later verified the devastation at another **Vtorovo hub**. Drones arrived at Russia's biggest crude export terminal, Novorossiysk oil port, at the end of the month, momentarily **interfering with tanker loading**. These strikes have strategic economic significance that goes far beyond local fires, given that nearly 3**0% of Russia's federal revenue** comes from oil and gas exports.

Defense Industry and Military Production

The campaign also targeted Russia's defense industry. Production was temporarily halted after **Ukrainian drones targeted the Elektrodetal** facility in Bryansk Oblast, which supplies electronic parts for radars and missile systems. UAV resupply was further disrupted when the Ukrainian General Staff confirmed another strike against a drone manufacturing facility inside Russia. Even though they are not as severe as refinery outages, these attacks eventually make it more difficult for Russia to continue its war effort.

Map: RFE/RL Source: InformNapalm

Command Posts, Radars, and Missile Systems

Some of the most notable attacks on Russia's military C2 network occurred in September. **Ukrainian drones directly targeted Russia's offensive and defensive capabilities at the Molkino** training ground in Krasnodar Krai, destroying at least two Iskander ballistic missile launchers and damaging a Pantsir-S1 air defense system. Russian forces were deprived of low-altitude detection in the same area when a Kasta-2E2 radar was turned off.

Ukrainian operations in Crimea hit another radar and **destroyed two An-26 transport** planes on the ground. Satellite imagery in Rostov Oblast verified that a dome radar installation had been destroyed. Concurrently, the 41st Army and Russia's "Center" grouping's command posts **were hit by Ukrainian drones and missiles**, resulting in reports of staff officer casualties. The Kanevska traction substation in Krasnodar **was shut down to cause logistical disruptions**, temporarily stopping the rail transportation of equipment and fuel. Strategically, Ukraine **damaged satellite links** essential to Russia's high-level command by **striking** the **Space Communications Center in Crimea**.

Ukrainian servicemen prepare to launch a long-range AN-196 Liutyi attack drone. Source: Evgeniy Maloletka/ AP file photograph

AIR

Innovation and Range Expansion

September saw confirmation of a new Ukrainian technique: **aerostat-assisted drones** designed to extend endurance and reduce detectability. The strikes on Salavat highlighted how Ukraine's strike architecture is evolving, with UAVs now reaching **more than 1,400 km into Russia's industrial heartland**.

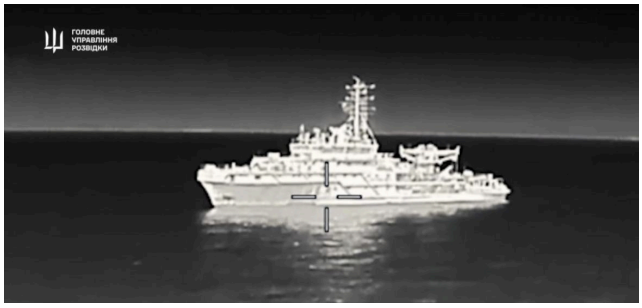
This adaptation signals both increasing range and growing complexity in Ukrainian long-range operations.

August and September deep strikes represents a shift for Ukraine from tactical disruption to a **systematic war of attrition**, one that lowers military capability, causes economic losses, and compels Moscow to make expensive defensive adjustments.

MARITIME

Black Sea Auxiliary Fleet Under Threat

The maritime realm was even touched by the campaign. Ukraine's GUR **damaged a Project MPSV07 auxiliary ship** near **Novorossiysk** using an UAV. Despite not being a warship, its loss makes it harder for Russia to conduct support and rescue missions in the Black Sea and makes it abundantly evident that ports and naval resources are accessible.



Project MPSV07 in the sights of a Ukrainian drone. Source: DIU

Toloka Debut: Scaling Ukraine's Maritime Strike Options

On September 17, 2025, at the Brave1 Defense Tech Valley exhibition in Lviv, Ukraine **showcased its domestically produced Toloka underwater drone family**.

The TLK-150 is engineered for stealth operations just beneath the surface. Its compact dimensions and electric propulsion reduce acoustic and thermal signatures, enabling discreet penetration of adversary defenses.

Larger variants include the TLK-400 (4-6 m length, 1,200 km range, 500 kg payload) and TLK-1000 (4-12 m length, 2,000 km range, 5,000 kg payload), **designed for extended missions and heavier ordnance**.

The system highlights Ukraine's drive toward cost-effective, scalable maritime autonomy. If successfully deployed, Toloka drones could reshape Black Sea operations by disrupting logistics, striking high-value naval targets, and offsetting Russia's conventional fleet advantage.

Ukraine's underwater drone TOLOKA Source: RBC-Ukraine

Ushkuynik: Russia Races to Replicate Ukrainian Naval Drones

According to Russian reports, developers are **racing to replicate Ukrainian unmanned-boat concepts**. Their latest project, the Unmanned Maritime Vessel (UMV) "USHKUYNIK" features **fiber-optic control** and is currently undergoing final trials with the Black Sea Fleet, with combat tests scheduled in the upcoming weeks. Russian sources describe it as the first naval UMV designed for full electronic warfare resistance, capable of serving either as a kamikaze platform or as a floating base for launching FPV drones.

Declared features include:

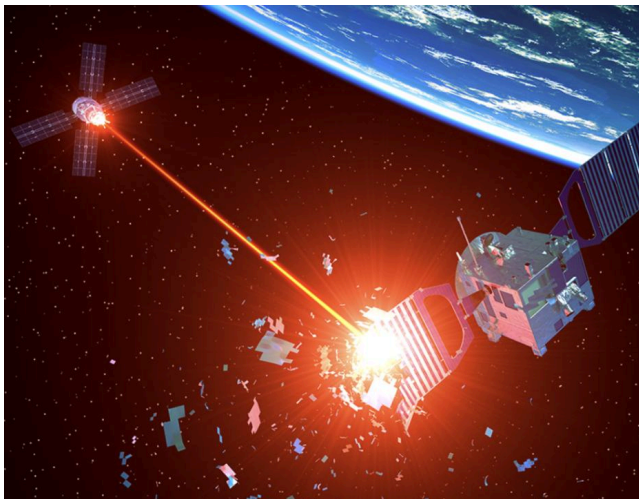
- **Control**: fiber-optic link for secure command and HD video transmission.
- **Sensors:** onboard processing for target recognition, including camouflaged objects.
- **Combat:** range limited by tether length but improved strike accuracy at lower cost than traditional naval assets.

Analysts note that fiber-optic control increases resilience against jamming but reduces range and flexibility, with cable length and vulnerability to physical severing remaining significant constraints.

Russian "USHKUYNIK" UMV. Source: mezha.media

Pistorius: 035B Push to Counter Russian and Chinese Space Weapons

Germany will allocate **€35B ($41B) to develop space defence capabilities by 2030**, citing growing **Russian and Chinese anti-satellite (ASAT) threats**. Defense Minister Boris Pistorius noted both nations have expanded their ability to **jam, disable, or physically destroy satellites** in recent years.



Source: Peraton

Planned investments include:

- Multi-orbit satellite constellations for redundancy and resilience
- Hardened ground stations and secure launch infrastructure
- Cybersecurity integration for all space assets
- Enhanced space situational awareness and defensive countermeasures

This decision comes amid real-world stress tests for space assets: Starlink disruptions in Ukraine have revealed the vulnerability of single-constellation architectures, while recent Chinese high-altitude intercept tests highlight the growing reach of ASAT and missile defense systems. For Ukraine and NATO, Germany's initiative signals a shift toward multi-layered, survivable space networks designed to withstand jamming, kinetic strikes, and cyber attacks in future conflicts.

Cut the Cord: Ukraine's Mechanical Counter to Russian Fiber-Optic FPVs

The rise of fiber-optic UAVs has pushed both sides to hunt for countermeasures. While **sophisticated electronic responses are still in development, frontline units are experimenting with improvised tools**.

One Ukrainian solution is a **rotating barbed-wire snare** designed to cut the fiber-optic cable of enemy drones. **The system uses a 150-metre wire powered by a battery**, programmed to rotate on and off every minute to sustain up to 12 hours of daily operation.

A rotating wire snare. Source: Instagram hm_intelligence

The appeal is obvious: cheap, mechanically resilient, and simple to produce. But its limits are equally clear. It only secures narrow corridors, moving parts pose risks to friendly fiber-optic assets, and deployment exposes crews to danger. Once detected, snares can be avoided, cut, or destroyed, with operators adjusting flight profiles to bypass them. Still, if multiplied and concealed, such traps could force the enemy to waste drones and resources clearing obstacles or to redesign systems, proving that even **wire can buy time against innovation**.

Wire War: Russia's Fiber-Optic Relay Drones Expand the Strike Zone

In September Russia introduced an attempt to extend the "kill zone" **by deploying airborne fiber-optic relay drones**, reportedly increasing effective range by 20 kilometers. The configuration chains a primary drone (repeater) and secondary strike UAVs. Rather than one strike drone spooling the whole line, **repeaters carry part of the fibre** and reduce the weight any single attacker must bear. A repeater can provide observation, effectively amplify the signal, and **extend the usable distance from 10-20 to up to 60 kilometers**. This change can materially expand the area at risk and complicate logistics and evacuation behind the front.

Some Russian sources claim these relay drones are reusable: after releasing strike UAVs, the **repeater could return and re-spool its fiber-optic cable** for a second sortie. That profile is plausible only if hardened re-spooling hardware exists, otherwise the cable is almost certainly single-use. While relay drones themselves are not new, applying a fiber-optic connection is an innovative step.

Still, any such architecture creates a single-point vulnerability: if the repeater is downed or its spool disrupted, all dependent drones immediately lose their feed.

Field in Ukraine covered with fiber-optic threads from drone usage. Source: Forbes

Cyber Frontlines: Russian Businesses Hit by Surging Attacks

Sberbank reports a threefold increase in cyberattacks on Russian businesses in the first eight months of 2025 compared to 2024, **with estimated losses reaching 1.5 trillion rubles ($18B)**.

Key findings:

- 53% of companies targeted; 80% of those suffered major consequences.
- 48% reported downtime; 25% reported direct financial losses and reputational damage.
- Attacks ranged from DDoS disruptions to multi-vector intrusions with malicious software.

The surge highlights the growing role of offensive cyber operations in hybrid warfare. For Russia, it reflects sustained attrition of networks and services. For Ukraine and allies, it underscores the urgency of scaling defensive investments: monitoring, hardening, and rapid incident response must protect not only critical infrastructure but also shared donor systems, supply chains, and battlefield C2.

Illegitimate Elections Targeted by Cyber Ops

On September 14, 2025, during Russia's unified voting day, Defense Intelligence of Ukraine (DIU) launched a **massive DDoS campaign against the Russian Central Electoral Commission (CEC)** and supporting infrastructure. The operation targeted the illegitimate elections staged in occupied Ukrainian territories, **crippling CEC servers, the remote electronic voting system, backbone routers at Rostelecom, and the "Gosuslugi" portal**.

Russian authorities logged **99 attacks in four hours**, forcing partial paralysis of online voting. CEC chair Ella Pamfilova admitted "the internet went down in the CEC building, an attack is underway," while Roskomnadzor confirmed traffic degradation across backbone networks. DIU framed the strike as part of broader efforts to **undermine Russia's digital backbone and delegitimize governance in occupied regions**.

From Frontline Innovation to Systemic Power: Ukraine's Next Tech Leap

Several technologies are often cited as having the **potential to reshape warfare** over the next decade: autonomous swarms across air, sea, and land; high-energy weapons such as lasers and electromagnetic arms; AI-driven operational command; new classes of long-range missiles; and integrated space systems.

The question is not whether these technologies will emerge, but whether **Ukraine will shape them or simply import them**. With unique battlefield experience in drones, EW, and cyber, Ukraine has a rare opportunity to become a driver of asymmetric innovation. But to seize that role, it must move beyond fragmented initiatives and build something akin to **DARPA (Defense Advanced Research Projects Agency)**, an institution capable of harnessing frontline lessons, scaling breakthroughs, and driving the next wave of defense revolutions.

Ukraine has already demonstrated agility in rapid battlefield innovation. Yet **isolated breakthroughs, however impressive, rarely scale on their own**. An innovation agency could channel this momentum, **funding startups, universities, and engineering teams to take on projects that may not pay off immediately**, but could decisively influence the battlefield in 10 years.

Ukraine's defense **governance remains fragmented**, with overlapping roles across MoD, MinDigital, Ministry of Education and Science, the recently dissolved Ministry of Strategic Industries, Ukroboronprom, and the NSDC. Decision-making is often manual and concentrated within a narrow circle, allowing fast reactions but preventing scale. Serial drone production, for example, still depends on ad hoc approvals rather than automated procurement programs.

The absence of centralized strategic analysis leads to duplicated funding of similar projects and resource dilution. As a result, both the military and private sector suffer.

Reform requires a **dedicated institution with a clear mandate and accountability to replace fragmented responsibility**, reduce chaos, and enable predictable, scalable defense innovation.

A Ukrainian version of DARPA could become a useful tool to deliver results thanks to:

- The ability to act as a **direct customer for R&D**, contracting not only with established companies but also with startups, universities, and engineering teams.
- A dedicated **multi-year innovation fund**, enabling projects that may take 5–10 years to mature but could radically shift battlefield dynamics.
- Flexibility to recruit **top technical talent**, including from abroad, on competitive terms.
- **Direct channels for international cooperation**, giving the institution the ability to engage NATO, EU, U.S., or South Korean counterparts.

DARPA in the United States became the driver of technological revolutions precisely because it was **independent from traditional bureaucratic procedures** and maintained a **clear focus on innovation**. Ukraine today finds itself in a similar position: **the military is fighting under conditions of resource scarcity**, yet at the same time serves as a proving ground for the newest military technologies. This experience must not be lost but rather systematized.

A Ukrainian DARPA would function as a strategic hub, **scanning for disruptive ideas, backing them with flexible resources, and pushing them through to operational deployment**. By 2035, such a system could help ensure Ukraine's ability to develop high-risk, high-reward technologies and contribute to the global defense ecosystem, as an equal and recognized partner.

SOURCES

- BBC. “Inflatable tanks and flat-pack guns - inside Ukraine's decoy war.” BBC, 2025. Link
- Business Insider. “A Russian decoy for the Shahed was found with cameras on its back, highlighting how Moscow is adapting in the drone war.” Business Insider, 2025. Link
- Bloomberg. “Key Russia Black Sea oil ports pause loadings after drone alerts.” Bloomberg, 2025. Link
- Defence24. “Polska obrona przed dronami, czyli strzelanie z armaty do komara.” Defence24, 2025. Link
- Defence UA. “Ukraine’s Neptune strike on the Elektrodetal plant shows the enemy has decommissioned an entire GRAU arsenal.” Defence UA (English), 2025. Link
- Defence UA. “Ukrainian drones deliver unprecedented blow to the Iskander system brigade.” Defence UA (English), 2025. Link
- Defence UA. “Ukrainian Defense Intelligence drones hit Russian MPSV07 vessel violating law of war.” Defence UA (English), 2025. Link
- Economic Times. “Germany pledges €35 billion for space defence against Russia, China.” The Economic Times, 2025. Link
- Euromaidan Press. “Ukrainian drone engineers suggest dropping nets on Russia’s roadside ambush drones.” Euromaidan Press, 2025. Link
- Forbes. Mittal, Vikram. “Russia introduces fiber-optic repeater drones to increase strike range.” Forbes, 2025. Link
- Hromadske. “Drones massively attacked 13 Russian regions, Lukoil ship burned, UAVs flew to Moscow.” Hromadske, 2025. Link
- Interfax. “Cyberattack damage to Russian economy estimated at 1.5 trillion rubles.” Interfax, 2025. Link
- Interfax Ukraine. “Ukraine strikes at Vtorovo fuel facility again.” Interfax-Ukraine, 2025. Link
- Izvestia. Belyi, Anton. “Не морозь ни дня: российская разработка позволит БПЛА летать в экстремальные холода.” Iz.ru, 2025. Link
- Kyiv Independent. “Ukrainian drones strike major Russian oil refinery in Leningrad Oblast, governor says.” Kyiv Independent, 2025. Link
- Kyiv Independent. “Ukrainian drones reportedly strike oil facilities in Russia’s Ryazan Oblast, occupied Luhansk Oblast.” Kyiv Independent, 2025. Link
- Kyiv Post. “Ukraine’s deep strike campaign hits Russian oil assets.” Kyiv Post, 2025. Link
- Kyiv Post. “Satellite images reveal major Russian aviation losses.” Kyiv Post, 2025. Link
- Mezha. “Ушкуйник UMV: росіяни розробили морський дрон на оптоволокні.” Mezha, 2025. Link
- Militarnyi. “Up to 200 mines per one controller: Zmiyar develops smart mine detonators.” Militarnyi (English), 2025. Link
- Militarnyi. “Amphibious NRK robot joins Ukraine’s defense forces.” Ministry of Defense of Ukraine via Militarnyi, 2025. Link
- Militarnyi. “Taktychni radary okupantiv: чим наводять російські дрони-перехоплювачі.” Militarnyi (Blog), 2025. Link
- Militarnyi. “Supercam S-350 (analysis).” Militarnyi (Blog), 2025. Link
- Militarnyi. “Drone strike hits Russia’s state reserves fuel depot in Tver region.” Militarnyi (English), 2025. Link
- Militarnyi. “Chemical plant shut down in Krasnodar after night drone attack.” Militarnyi (English), 2025. Link
- Militarnyi. “Ukraine strikes at Vtorovo fuel facility again.” Militarnyi (English), 2025. Link
- Militarnyi. “Ukrainian General Staff: missiles and drones hit Russian command centers.” Militarnyi (English), 2025. Link
- Militarnyi. “Ukraine strikes Kanevskaya traction substation in Krasnodar.” Militarnyi (English), 2025. Link
- Militarnyi. “Ukraine hits Russian space communications center in Crimea.” Militarnyi (English), 2025. Link
- Militarnyi. “Ukraine deploys aerostats in drone strike on Russia.” Militarnyi (Ukr), 2025. Link
- Militarnyi. “HUR cyber specialists attacked Russia’s CEC on election day.” Militarnyi (Ukr), 2025. Link
- Militarnyi. “Russia attacks not only with drones: disinformation campaign in Polish media.” Militarnyi (Ukr), 2025. Link

SOURCES

- Moscow Times. “Russia halts nearly 40% of refining capacity after Ukrainian strikes.” Moscow Times, 2025. Link
- New Scientist. “Solar-powered ambush drones can wait for targets like land mines.” New Scientist, 2025. Link
- Novyny Live. “Росіяни будують металеві щити для НПЗ від українських дронів.” Novyny Live, 2025. Link
- Pravda (Ukrainska). “Ukraine’s strikes damage Russian refineries.” Ukrainska Pravda, Sep 7, 2025. Link
- Pravda (Ukrainska). “Ukraine’s strikes continue on oil infrastructure.” Ukrainska Pravda, Sep 18, 2025. Link
- Reuters. “NATO launches Eastern Sentry to bolster eastern flank after Russian drone incursion.” Reuters, Sep 12, 2025. Link
- Reuters. “Poland downs drones in its airspace, becoming first NATO member to fire during war.” Reuters, Sep 10, 2025. Link
- Telegram @apate120. “Decoy M777 photos.” Telegram, 2025. Link
- The Defender. “Vyriy drone at DTV.” The Defender, 2025. Link
- The Defender. “Karakurt ground robot developed by IRV can carry and launch up to six FPV drones.” The Defender, 2025. Link
- UNIAN. “Zapad-2025: Russians showcased inflatable Su-33.” UNIAN, 2025. Link
- United24 Media. “Russian Gerbera drones recovered in Poland had secret long-range tanks.” United24 Media, 2025. Link
- United24 Media. “Ukraine’s massive underwater drone Toloka unveiled at Brave1 Defense Tech Valley 2025.” United24 Media, 2025. Link
- X (Twitter). InformNapalm. “Photos of Ukrainian strikes.” InformNapalm, 2025. Link
- YouTube. “Ukrainian FPV drone destroys Russian Mi-8 helicopter.” YouTube, 2025. Link
- YouTube. “Ukrainian GUR drone strike footage.” YouTube, 2025. Link
- Instagram. “Counter-drone rotating wire reel demo.” Instagram, 2025. Link
- Institute for the Study of War. “Reported Russian drone debris in Poland — September 10, 2025.” Understanding War, 2025. Link

SNAKE ISLAND INSTITUTE