Russia's Gerbera drones share a distinctive body shape with Iranian-designed Shahed-136 drones. *Screenshot from Telegram*

Russia's Changes in the Conduct of War Based on Lessons from Ukraine: Adapting Technology, Force Structures, and the Defence Industry

Col. Vytis Andreika
Chief of Staff of Training and Doctrine Command of the LAF

The article was first published in the US Army Journal Military Review: https://www.armyupress.army.mil/Journals/Military-Review / English-Edition-Archives/September-October-2025/Lessons-from-Ukraine/

Abstract

Russia has demonstrated a remarkable ability to quickly learn and innovate despite suffering substantial losses in Ukraine. This makes Russia a challenging enemy that defies previous assumptions about its military strengths. This article argues that the Armed Forces of the Russian Federation (AFRF) has successfully adapted their conduct of war by integrating new technologies and tactics, thereby enhancing their combat effectiveness against the Armed Forces of Ukraine (AFU). By focusing on drone and electronic warfare (EW), this adaptation has led to demonstrable shifts in battlefield dynamics and has boosted operational capabilities, presenting a serious challenge to traditional NATO defense strategies.

Using the military innovations theory developed by Michael C. Horowitz and Shira Pindyck, this article examines how the AFRF has adapted its conduct of war based on lessons from the ongoing war in Ukraine, particularly where the AFRF has demonstrated significant technological and tactical advancements [1]. Horowitz and Pindyck's theory outlines the stages of invention, incubation, and implementation, which are applied to analyze three specific case studies: the use of Iranian one-way attack (OWA) Shahed drones, first-person-view (FPV) drones, and lightweight EW systems. Of note, this article does not explore other military innovations like glide aviation bombs or reconnaissance-strike complexes, as their examination would exceed the scope of this article.

This analysis shows the AFRF's ability to innovate, challenging perceptions of its rigidity and resistance to change. Military innovations in the use of Shahed drones, FPV drones, and counter-unmanned aerial vehicles (C-UAV) while also using lightweight EW systems illustrate Russia's capacity to institutionalize innovation within its doctrine, force structures, and the military-industrial complex. These changes are a potential threat to the Baltic States and their NATO allies, given its geographical proximity. It highlights the urgent need to address these challenges to prepare for future wars.

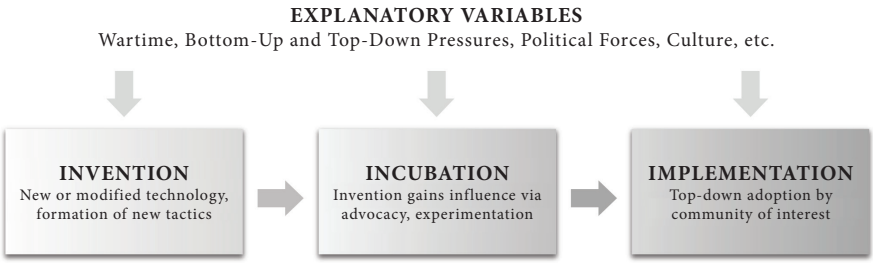
Keywords: *military innovations, Shahed drones, war in Ukraine, FPV drones.*

A Theory of Military Innovations

Examining military innovation theory enables us to assess if Russia has adapted its way of war through lessons from the war with Ukraine. In their study, "What Is a Military Innovation and Why It Matters," Horowitz and Pindyck argue that there is no consensus on the wide range of conceptual definitions of military innovation. They propose a new theoretical framework for understanding military innovations [1].

They define military innovations as "changes in the conduct of warfare designed to increase a military's ability to generate power" through invention, incubation, and implementation [1]. The first stage, invention, is creating new technologies or tactics, or modifying existing ones to solve specific problems in new ways. The second stage, incubation, is the products of invention gaining status and influence through advocacy or experimentation via bottom-up or top-down processes. The third stage, implementation, is the top-down process of political leaders leading the relevant community of interest to adopt the invention. Often, after adoption, the innovation can diffuse and spread to other countries [1].

Note that these changes must occur at the operational level or be tactical by nature, but they must also be operationally significant to be adopted and be intended to enhance or translate into actual military power. Moreover, military organizations change their way of war when they undergo a military innovation process (see figure 1) that begins with the invention, includes a period of incubation in which the invention is seen as significant, and ends with the implementation of the invention [1].



(Figure from Michael C. Horowitz and Shira Pindyck, "What Is a Military Innovation and Why It Matters," *Journal of Strategic Studies* [2023])

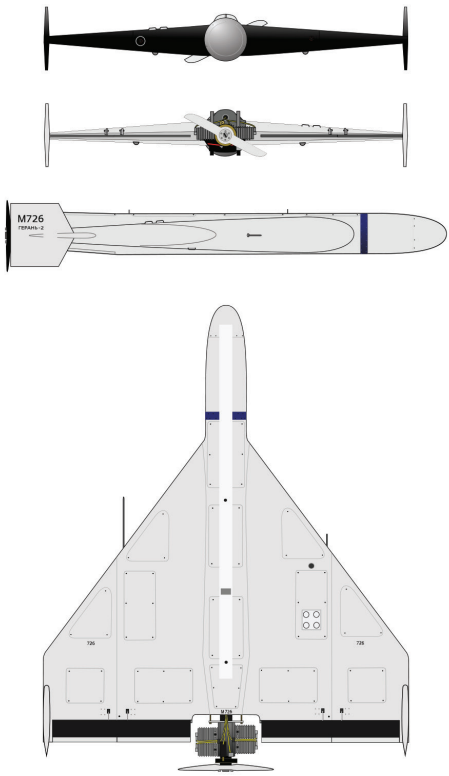
Figure 1. Military Innovation Process

Russia may undergo the process of military innovation differently. However, Horowitz and Pindyck's proposed military innovation theory allows for the organization and comparison of innovation cases to address whether the AFRF is changing its way of war based on lessons from the war in Ukraine. Using this framework, three military innovations from the ongoing war—Iranian OWA Shahed drones, FPV drones, and C-UAV EW systems—are analyzed.

One-Way Attack Shahed Drone

Applying Horowitz and Pindyck's framework to the AFRF's adoption of Iranian OWA Shahed drones demonstrates each stage of military innovation. These low-cost drones enable Russia to continue targeting critical infrastructure and terrorizing the civilian population, thereby overstretching Ukrainian air defenses (AD) and enabling the AFRF to rebuild depleted stocks of more expensive missiles.

The Shahed drones—Shahed-136 and Shahed-131—are delta-wing drones capable of carrying up to 40 kg of explosive payloads to preplanned targets over long (900 to 1,500 km) distances at speeds up to 170 km/h (see figure 2) [2]. They are an attractive alternative to ballistic and cruise missiles due to their low cost and ease of production.

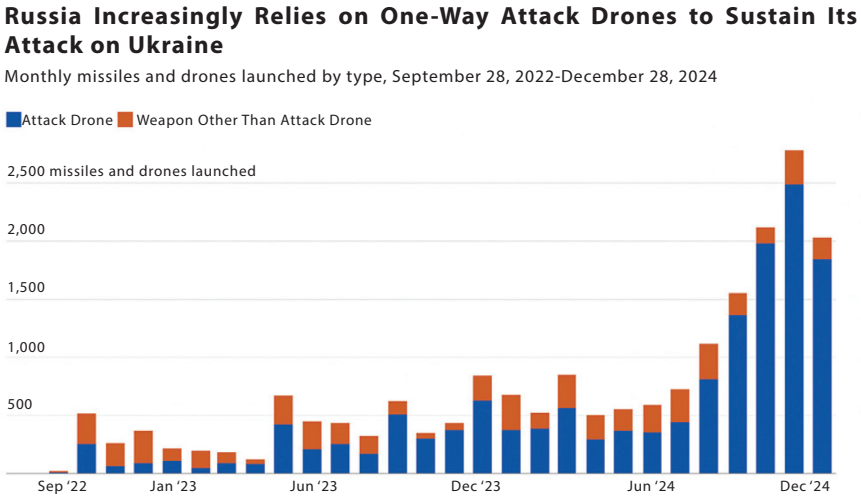


(Figure by Alexpl via Wikimedia Commons)

Figure 2. Shahed-136 / Geran-2 One-Way Attack Drone

The impetus for the diffusion of Iranian Shahed technology into Russian warfare was the depleted stocks of traditional missiles and the need to conduct sustained attacks on Ukrainian infrastructure. The AFRF began using Shahed drones in early September 2022, with Russian operators receiving training in Iran [3]. The AFRF had probably used 86 percent of its Iskander missiles, 46 percent of its sea-launched Kalibr cruise missiles, and 52 percent of its air-launched cruise missiles by October 2022 [4]. According to Russian military experts, the Shahed drone represents a new type of weapon that is transforming the Russian strategy of saturating military and civilian infrastructure deep within Ukraine at a fraction of the cost [5]. With an estimated cost of $35,000 per unit, Shahed drones offer a cost-effective alternative to the Iskander M ballistic missiles (approximately $2 million) and Kalibr cruise missiles ($1 million) [6]. To counter this saturation strategy, Ukraine was forced to allocate its resources and adapt its AD tactics.

The mass production of Shahed drones highlights Russia's commitment to integrating this technology. As Iran supplied several hundred Shahed drones to the AFRF, there were initially a few cases of its usage [7]. After seeing its effectiveness, Russia made a top-down decision to acquire more Shahed drones. In early 2023, the Russian military-industrial complex signed a $1.75 billion franchise deal with Iran to supply six thousand Shahed drones to the AFRF by September 2025 and to build a factory in Alabuga, Tatarstan, to manufacture a modified version of the drone under the names Geran-1/2. The factory started production in May 2023 and averaged about twenty drones per workday [8]. Between January and September 2024, the factory produced 5,760 drones, fulfilling the contract agreement [9]. In mid-2023, the Russian military made another top-down decision to mass produce the ten times cheaper, low-tech decoy drones Gerbera, which were intended to make themselves conspicuous to radars and deplete or distract the AFU AD, thereby improving the penetration rate of the armed Shahed drones [10]. As drone production ramped up, the number of drone attacks significantly increased in its efforts to oversaturate the AFU AD (see figure 3) [6]



(Figure from Neil Hollenbeck et al., "Calculating the Cost-Effectiveness of Russia's Drone Strikes," Center for Strategic and International Studies, 19 February 2025, https://www.csis.org/analysis/calculating-cost-effectiveness-russias-drone-strikes)

Figure 3. Monthly Missiles and Drones Launched by Type (September 2022 – December 2024)

While specific unit designations remain unconfirmed, the AFRF has likely integrated Shahed drones into specialized units under the Russian Aerospace Forces. Dedicated Shahed drone units and the constant increase in usage suggest an evolution of tactical thought regarding the drones, even if it is not formally codified in AFRF doctrine.

Early on, between September and December 2022, Russia used drones in uncoordinated attacks during the day using nap-of-the-earth flight profiles along highways or riverbeds. The AFU responded by establishing mobile fire groups and destroying the drones using machine-gun fire [3]. However, in early 2023, the AFRF refined their tactics to include swarm attacks, launching six to eight Shahed drones at night. The AFU responded by using all available means to defeat the attacks, including mobile fire groups, EW systems, man-portable air defense systems, short-range air defenses, tactical aircraft and helicopters, and hardening

infrastructure [3]. By the end of 2023, the AFRF began targeting critical infrastructure with massive waves of Shahed drones combined with traditional precision missiles. The AFRF would employ the Gerbera decoy drones to trigger Ukraine's AD radar illumination, recording their positions and then being followed by Shahed drones. Hours later, cruise missiles would be launched to either bypass or overwhelm the AD systems, and then be followed by ballistic missiles timed to coincide with the approaching Shahed drones and additional cruise missiles from various directions at multiple targets. This tactic aimed to overload the AFU AD and saturate selected targets with high aerial threats, thereby depleting Ukraine's limited AD resources [11]. To counter this tactic, the AFU began using EW teams equipped with the Pokrova EW system to spoof the Shahed drones' internal global navigation satellite system (GNSS) signals, leading to significant flight path errors [12]. To reduce the vulnerability to EW spoofing, Russia began installing a separate navigation system called Kometa, which featured an eight-element GPS-controlled reception pattern antenna that enhanced the drone's resilience against GNSS signal jamming and spoofing, unless the AFU also employed EW suppression triangulation [13]. In late March 2025, open-source evidence suggested that the AFRF has since updated their tactics. Russia now strikes a target simultaneously rather than sending drones in waves [14]. This evolution demonstrates Russia's ability to adapt and innovate in response to battlefield realities.

Russian state-media-released video on 20 July 2025 details one of the country's key drone assembly centers in Alabuga, Tatarstan. This production facility domestically manufactures the Iranian-designed Shahed drones under the name Geran-2, supporting Russia's ongoing war against Ukraine. *Screenshot from Zvezda TV*

In conclusion, deploying Shahed drones demonstrates how the AFRF has learned, evolving its military strategies through innovation. Russia diffused Iranian technology during the invention stage to solve missile stock shortages and sustain long-range strike capability. During incubation, the AFRF experimented with uncoordinated attacks, refined tactics, and institutionalized drone production through partnerships and domestic manufacturing. In the implementation stage, Russia mass-produced and upgraded Shahed drones, incorporated them into new drone force structures and integrated them into swarm tactics and deep strikes with precision missiles to overload Ukrainian AD.

FPV Drones

The increasing use of FPV drones marks another significant shift in Russia's way of war in Ukraine. During its second year, Russia faced a significant increase in the deployment of cheap and lethal Ukrainian FPV drones, which gradually took a leading role (up to 70 percent) in causing losses to equipment and manpower, making

frontline breaches virtually impossible [15]. Gen. Valery Zaluzhny, former AFU commander in chief, emphasized the role of FPV drones in the war after recognizing Ukraine's disadvantage in weapons and manpower. These drones, a critical tool for precision strikes, minimized direct contact and reduced the number of casualties [16].

Ukraine started mass producing its FPV drones when they faced a deficit of depleted artillery ammunition stocks in August 2023 [17]. An FPV drone is a low-cost ($500) quadcopter with a video camera and a 0.7–3 kg improvised armor-piercing, cluster, or thermobaric warhead (see figure 4). Controlled remotely by pilots, they can engage targets at speeds of 120 km/h over distances from 5 to 10 km. [18].

FPV Drone "Dozor"

FPV Drone "Dozor" designed for reconnaissance, destruction of enemy manpower and military equipment

Parameter name	Meaning
Maximum takeoff weight, kg	2.7
Payload weight, kg	Up to 1.2
Range, km	Up to 10
Flight time, min	Up up to 20
Speed, km/h	Up to 130
Practical ceiling, m	1000
Operating temperature range, °C	From -20 to +40
Launch / landing method	Vertical
Battery capacity, mAh	5000
Operating frequency range, MHz	868 – 915 / 5800
Manufacturer	OOO Prom Kompozit Moscow

FPV Drone "Ghost" 31

FPV Drone "Ghost" is designed to destroy enemy manpower and equipment

Parameter name	Meaning
Maximum takeoff weight, kg	3.5
Payload weight, kg	Up to 1.5
Range, km	Up to 7
Flight time, min	Up to 30
Speed, km/h	Up to 120
Practical ceiling, m	1000
Operating temperature range, °C	From -20 to +40
Launch / landing method	Vertical
Battery capacity, mAh	6000
Operating frequency range, MHz	860 – 1020 / 1200; 5800
Manufacturer	LLC UralDronZavod Yekaterinburg

(Figure translated from General Staff of the Armed Forces of the Russian Federation, *Handbook: FPV Drones Used by the RF Armed Forces in the SMO* [2024])

Figure 4. Example of FPV Drones Available for Order to Frontline Units from Suppliers

Recognizing the effectiveness of FPV drones, the AFRF rapidly diffused the same military innovation within its forces, showcasing an impressive ability to learn and adapt on the battlefield [19].

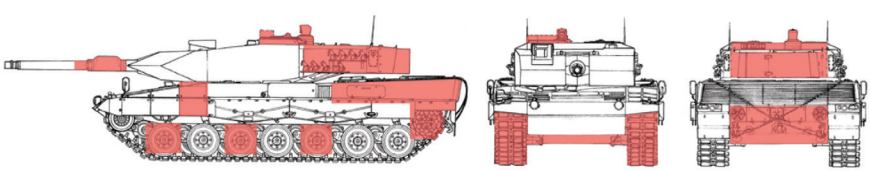
The driving force for the spread of FPV drones was the low-cost precision strikes on Ukrainian combat vehicles and personnel, reducing the need for direct contact and minimizing casualties.

Russia shows its dedication to military technological advancement by using standard, mass-produced FPV drones developed by civilian manufacturers and volunteer organizations. However, Russian military bloggers first pointed out that these drones performed inadequately, and the dominance of a single supplier restricted the AFRF's access to diverse models [20]. In response, in April 2024, the Russian Ministry of Defence (MOD) implemented a top-down decision to accelerate the fielding of FPV drones by funding special projects that united civilian volunteers, sponsors, the "People's OPK" (a public initiative to support the defense industry), and the MOD. As a result, civilian manufacturers increased production volumes of up to forty thousand drones per month and created new types of FPV drones [21]. By the end of 2024, the General Staff of the AFRF published a catalog featuring fifty-eight types of FPV drones, which frontline units could order from suppliers [22]. This decentralization and independence allowed frontline units to increase their strikes from several hundred to almost two thousand per day [23].

Russian troops build a two-kilometer mesh net "tunnel" in early 2025 to protect against Ukrainian FPV drones. In theory, FPV drones on their final attack trajectory will get entangled in the net or go off course. *Screenshot from X*

As the Russian FPV drones became more widespread and proved their effectiveness, Russian troops continuously refined drone tactics from the bottom-up, resulting in a dramatic increase in FPV drone strikes. This increase demonstrates a significant shift in the Russian way of war, with low-cost precision FPV drones increasingly replacing or augmenting traditional ground attacks.

First, the FPV drones are designed to destroy any combat vehicle. For instance, all tanks are designed to sustain fire from the front. The appearance of FPV drones made tanks extremely vulnerable, because FPV drones can maneuver and attack from the side, top, or rear, wherever the armor is weaker [19]. This threat became so prevalent on the modern battlefield that it forced AFU armored vehicles to withdraw from frontal positions and remain hidden 3–10 km away from the front line; consequently, AFU armored counterattacks became highly vulnerable. This frontline withdrawal allowed the AFRF to more easily retain seized strongpoints from AFU counterattacks, as AFU attacks were conducted without combat vehicles in dispersed infantry formations to avoid being lucrative targets (see figure 5) [19].



(Figure adapted from Russian Air Force Military Educational and Scientific Center, *Operation and Use of Unmanned Aerial Vehicles [FPV drones]* [2023])

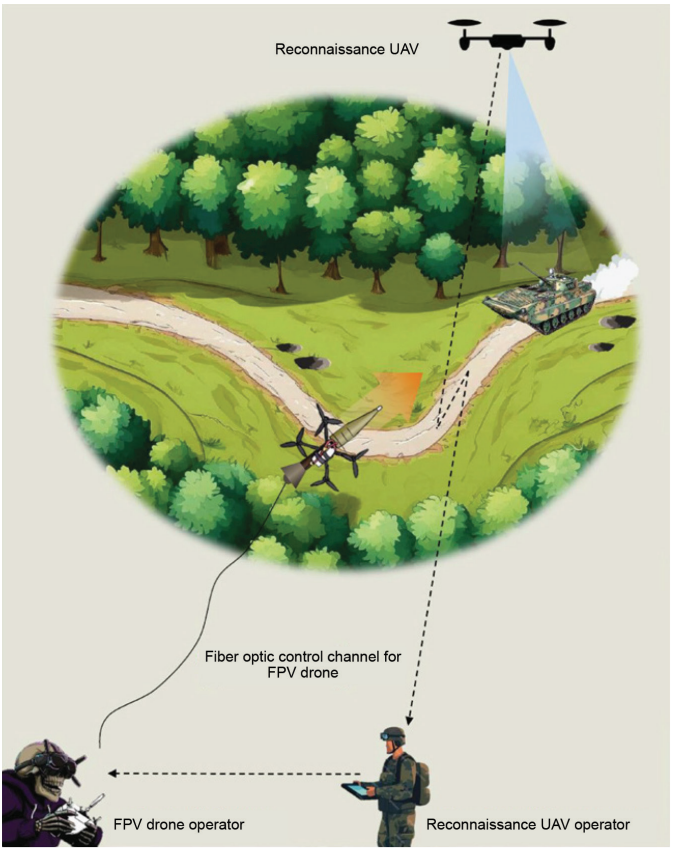
Figure 5. Marked Leopard Tank Indicating Vulnerable Parts to an FPV Strike

Second, FPV drones have become individualized weapons, able to chase a single AFU soldier on the front line. Russian military experts claim that there are sectors on the front line where the AFRF has FPV drone superiority, the AFU has dominance, and there is parity. In these areas, every soldiers movement is immediately targeted by two to three drones within 6 km from the front and either side [19]. The combination of FPV drone strikes in concert with glide aviation bombs and artillery barrages has become so

deadly that it forced the AFU to adapt by dispersing troops and altering its tactics [24].

Third, the AFRF began to isolate Ukrainian strongpoints with FPV drones by interdicting their flow of troops and supplies 3–10 km behind the front [24]. This new tactic forced the AFU to withdraw from some positions or conduct sustainment operations by walking 5 km and carrying up to 40 kg of supplies [25]. To counter the same threat from the Ukrainian side in early 2025, the AFRF started constructing mesh tunnels to protect their ground supply routes [26]. This tactical evolution of FPV usage demonstrates Russia's ability to adapt and innovate in response to battlefield realities.

Most of these bottom-up driven tactics were institutionalized in Russian military tactical publications. The Military Training and Research Centre of the Russian Air Force released a publication in the last quarter of 2023 titled *Operation and Use of Unmanned Aerial Vehicles (FPV Drones)*, which describes FPV characteristics, preparation, piloting, maintenance, safety instructions, and establishing standards for theoretical, simulator, and flight training within the AFRF [27]. Additionally, Russian volunteers released a memo for soldiers describing instructions for preparing warheads for FPV drones, including the dismantling of Javelin missiles [28]. Finally, Russian volunteers also published in the last quarter of 2024 the *Handbook on the Tactics of Using FPV Drones by the Enemy (in Diagrams) and Methods of Counteraction*, which contains nineteen tactical applications of FPV drones (see figure 6) [15]. The development of new doctrine underscores the institutionalization of this innovation within the AFRF.



(Figure translated from Volunteers, *Handbook on Tactics of Using FPV Drones by the Enemy [in Diagrams] and Methods of Counteraction* [2024])

Figure 6. Tactical Application of FPV Drones Example – Using Fiber-Optic Cable for Control

The implementation of FPV drones led to the formal incorporation of FPV drone crews at the tactical-unit level. Notably, the Russian MOD announced in January 2024 that the first UAV company was formed on the front line with FPV crews engaging enemy targets [29]. The composition of FPV crews was likely diffused from the AFU and included four persons: a senior, an FPV drone operator, an ammunition specialist, and a reconnaissance drone operator [15]. In October 2024, the Russian defense minister ordered the "Rubikon" Centre for Prospective Unmanned Technologies to form

five unmanned detachments for operations in Ukraine [30]. The Russian MOD established an entirely new branch in December 2024, the unmanned systems troops [31]. The Russian unmanned systems troops formed the first drone regiment at the military district level in January 2025 with forty-one FPV drone strike units. Similar regiments may be formed in other military districts in the future [32]. The establishment of specialized units underline the institutionalization of this innovation within the AFRF.

It is important to highlight that FPV drones still have specific vulnerabilities: short flight duration (seven to ten minutes) and range (up to 10 km), as well as vulnerability to EW [15]. To address the short flight time and range, the AFRF sometimes strike preidentified targets (e.g., bunkers) if they cannot hit high-value targets or land the drone and wait (up to six hours) until the target appears to ambush it [15]. To extend the range, the AFRF might use a "mother" agro drone with signal retranslation to lift and launch two to three FPV drones up to 60–70 km. [15]. The final and most significant FPV drone vulnerability is its susceptibility to radio frequency and GNSS signal electromagnetic jamming. In 2024, both sides jammed 60–80 percent of all FPVs operated [24]. In March 2024, Russians were the first to introduce FPV drones with fiber-optic cables to counter electromagnetic jamming, a specific Russian innovation, allowing them to penetrate areas of heavy jamming and hit targets up to 10 km [33]. According to Russian military experts, this innovation played a crucial role in Russia's recent success in retaking Kursk [34].

In conclusion, the adoption of FPV drones by the AFRF illustrates rapid military innovation. Russia diffused Ukrainian innovation during the invention stage to minimize casualties and enable standoff, low-cost precision FPV drone strikes on AFU combat vehicles and troops. During incubation, the AFRF experimented with tactics, technology, drone units and centralized its FPV drone production. Russia institutionalized FPV drone innovation in the implementation stage by enhancing collaborative production, standardizing tactics, and adjusting force structures. The AFRF's

evolving drone capabilities highlight a learning process driven by battlefield necessity, showing that Russia is actively changing its approach to warfare based on lessons learned from the war in Ukraine.

Moreover, inspired by the current war, Russia's allies are diffusing FPV drone innovations into their arsenals. For instance, China is intensifying efforts to develop and integrate FPV and swarm drones into its armed forces [35]. Kim Jong Un, after his troops encountered FPV drones in Ukraine, mass-produced FPV drones in North Korea with technical support from Russia [36]. Similarly, Serbia's armed forces adopted Komar FPV drones developed by Serbian defense industry enterprises in 2024 [37].

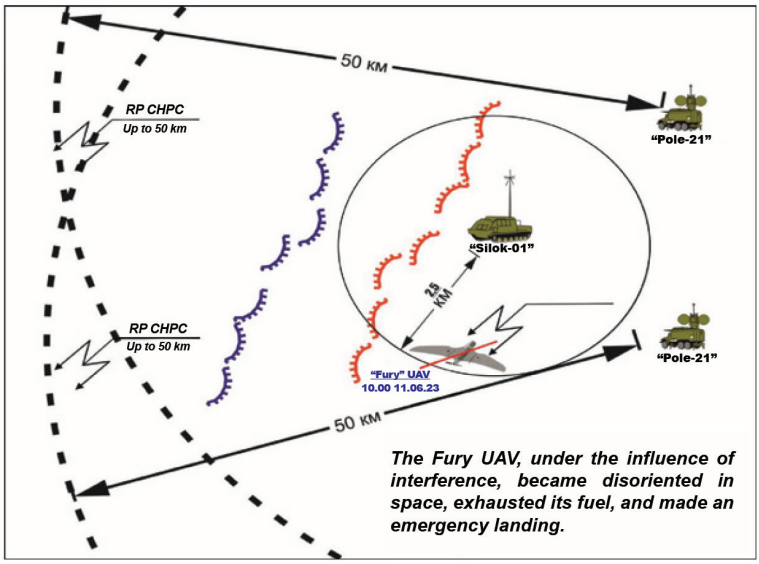
Lightweight C-UAV EW Systems

The extensive use of company-level lightweight C-UAV EW systems represents a third military innovation in the Ukraine war. While not originally a Russian invention, the country's mass production and integration of these systems into its force structures and doctrine have significantly altered its approach to modern warfare. The threat from drones was already evident during wars in Donbas and Syria [19]. Back then, EW systems proved the most effective way to counter drones by jamming their GNSS positioning, navigation, and timing signals or radio frequency links, which control drones or share video data [38]. During that time, Russia had invented and developed mostly vehicle-based C-UAV EW systems like Krasukha-4 (2014), Pole-21 (2016), Shipovnik-Aero (2016), Repellent-1 (2017), Silok-01 (2018), or Palantin (2019) [39]. One issue the AFRF faced after invading Ukraine was that these large and sophisticated vehicle-based C-UAV EW systems became high-value targets for AFU long-range fires [19]. This situation led to another problem: too few of these systems could effectively cover the entire front line.

The rapid proliferation of small drones caught the AFRF somewhat off guard. Ukrainian drones were helping to reconnoitre,

direct or adjust indirect fire, command troops, or drop improvised explosives, mines, or grenades on Russian troops [40]. This issue became very grave for the AFRF because a $200 commercially available off-the-shelf Ukrainian DJI Mavic drone could destroy a $3 million Russian tank by simply dropping a grenade through an open hatch and detonating the ammunition stored inside the turret [41]. The introduction of company-level lightweight C-UAV EW systems significantly improved the AFRF's ability to protect its forces from drone attacks.

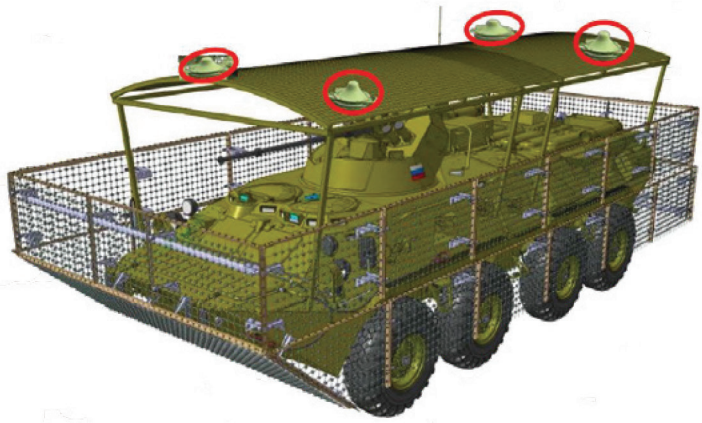
Due to the extensive threat from Ukrainian drones, the AFRF urgently needed to develop both kinetic and nonkinetic solutions to protect frontline units, a need formally acknowledged by the Russian MOD in its tactical manual *REMINDER on Protection and Counteraction Against Enemy UAVs*. The manual institutionalized the use of vehicle-based C-UAV EW systems and antidrone rifles. According to the manual, EW companies had to deploy EW systems like the Lesochek, Pole-01, or Silok-01 to protect high-value targets such as command posts or artillery positions (see figure 7); in contrast, EW assets like the Zhitel and Palantin had to protect frontline units. It was recommended that each infantry platoon have one operator with an antidrone rifle for close protection against drones [40]. As seen from the manual, other company-level lightweight C-UAV EW military innovations such as vehicle-mounted C-UAV jammers, drone detectors, and portable C-UAV jammer domes that the AFU already utilized were still in the incubation period within the AFRF as of mid-2023.



(Figure translated from Russian Ministry of Defence, *REMINDER on Protection and Counteraction AgainstEnemy UAVs* [2024])

Figure 7. Illustration of Russian C-UAV Tactic in Mid-2023 Using Pole-21 and Silok-01

The sudden influx of deadly Ukrainian FPV drones targeting Russian combat vehicles likely spurred the rapid development of vehicle jammers by the Russians. These vehicle-mounted C-UAV jammers create a protective "dome" around the vehicle by jamming multiple frequencies within a specified radius to disrupt drone communications and navigation [42]. By the end of October 2023, the Russian MOD released a series of guidelines to ensure the protection of combat vehicles from FPV drones, including the use of four vehicle-mounted C-UAV jammers (see figure 8) [43]. Two additional vehicle-mounted C-UAV jammers were also codified into Russian doctrine at the end of 2024 [22]. Urgent standardization and mass production of vehicle-mounted C-UAV jammers represent a significant Russian top-down effort to address the devastating threat from Ukrainian FPV drones.

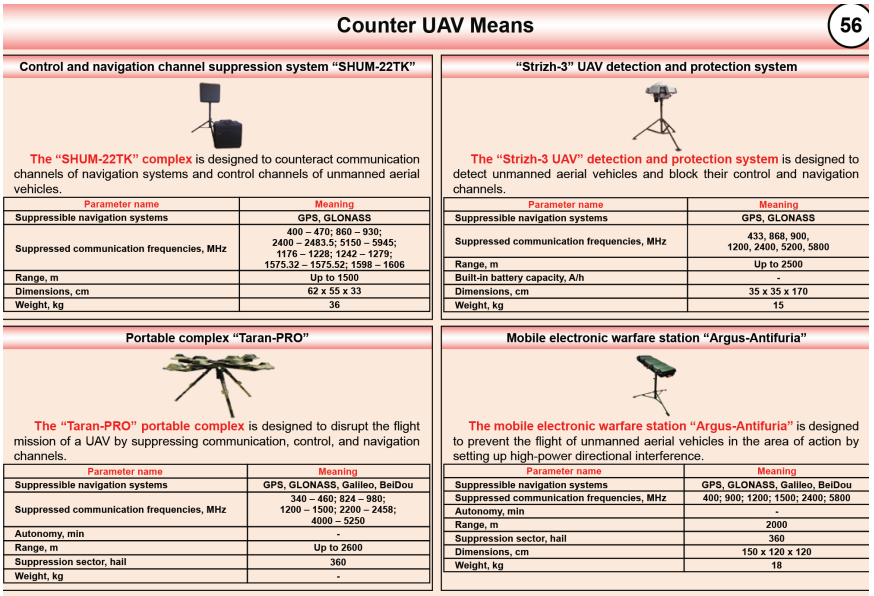


(Figure from Russian Ministry of Defence, *Guidelines for Ensuring the Protectionof APCs from FPV Drones* [2023])

Figure 8. Illustration Explaining How to
Use Vehicle-Mounted C-UAV Jammer Volnorez

The exponential growth in Ukrainian FPV drones has allowed for the targeting of not only Russian combat vehicles but also individual soldiers. Instances of two or three FPV drones pursuing a single soldier have become common, necessitating the dispersion and reduction of troops in the trenches [15]. This lethal battlefield environment impeded Russian leadership from implementing and fielding the remaining military innovations in C-UAV EW at the company level [24]. The objective was to equip each infantry platoon position with a drone detector, a portable C-UAV jammer dome, and an antidrone rifle [15]. The introduction of company-level lightweight C-UAV EW systems has significantly improved the AFRF's ability to protect its forces from drone attacks. A passive drone detector identifies and locates drones and their ground control stations by analyzing video frequencies, while the portable C-UAV jammer dome autonomously detects approaching drones and creates a radio interference "dome," jamming one or multiple frequencies within a 200–500-meter radius to disrupt drone communications and navigation [19; 50]. The antidrone rifle is a handheld device that allows the operator to emit directed energy at drones, jamming their communications and navigation up to 5 km [44].

There was an urgent battlefield demand for these lightweight C-UAV EW devices. Like FPV drones, state firms under Rostec, Russian private companies, and volunteers stepped in to fill these gaps with novel solutions. In April 2024, the Russian MOD made a top-down decision to fund small manufacturers' mass production of lightweight C-UAV EW devices. By the end of 2024, this decision allowed frontline units to quickly field five thousand C-UAV EW devices per month and develop new types of military innovations [21]. Ukrainian military EW experts identified approximately sixteen types of drone detectors developed by Russian companies [45]. The General Staff of the AFRF published a catalog where frontline units could order twelve types of portable C-UAV jammer domes (see figure 9) and twelve antidrone rifles [22]. The mass production of lightweight C-UAV EW systems, supported by state firms, private companies, and volunteers, highlights Russia's commitment to integrating this technology into its military strategy.



Counter UAV Means 56

Control and navigation channel suppression system "SHUM-22TK"

The "SHUM-22TK" complex is designed to counteract communication channels of navigation systems and control channels of unmanned aerial vehicles.

Parameter name	Meaning
Suppressible navigation systems	GPS, GLONASS
Suppressed communication frequencies, MHz	400 – 470; 860 – 930; 2400 – 2483.5; 5150 – 5945; 1176 – 1228; 1242 – 1279; 1575.32 – 1575.52; 1598 – 1606
Range, m	Up to 1500
Dimensions, cm	62 x 55 x 33
Weight, kg	36

"Strizh-3" UAV detection and protection system

The "Strizh-3 UAV" detection and protection system is designed to detect unmanned aerial vehicles and block their control and navigation channels.

Parameter name	Meaning
Suppressible navigation systems	GPS, GLONASS
Suppressed communication frequencies, MHz	433, 868, 900, 1200, 2400, 5200, 5800
Range, m	Up to 2500
Built-in battery capacity, A/h	-
Dimensions, cm	35 x 35 x 170
Weight, kg	15

Portable complex "Taran-PRO"

The "Taran-PRO" portable complex is designed to disrupt the flight mission of a UAV by suppressing communication, control, and navigation channels.

Parameter name	Meaning
Suppressible navigation systems	GPS, GLONASS, Galileo, BeiDou
Suppressed communication frequencies, MHz	340 – 460; 824 – 980; 1200 – 1500; 2200 – 2458; 4000 – 5250
Autonomy, min	-
Range, m	Up to 2600
Suppression sector, hail	360
Weight, kg	-

Mobile electronic warfare station "Argus-Antifuria"

The mobile electronic warfare station "Argus-Antifuria" is designed to prevent the flight of unmanned aerial vehicles in the area of action by setting up high-power directional interference.

Parameter name	Meaning
Suppressible navigation systems	GPS, GLONASS, Galileo, BeiDou
Suppressed communication frequencies, MHz	400; 900; 1200; 1500; 2400; 5800
Autonomy, min	-
Range, m	2000
Suppression sector, hail	360
Dimensions, cm	150 x 120 x 120
Weight, kg	18

(Figure translated from General Staff of the Armed Forces of the Russian Federation, *Handbook: FPV Drones Used by the RF Armed Forces in the SMO* [2024])

Figure 9. Example of Four Types of Russian C-UAV Jammer Domes Available for Order from Suppliers to Frontline Units

The proliferation of lightweight jammers led to the evolution of the C-UAV doctrine. The Russian MOD could not keep up with the pace of battlefield innovations, so Russian volunteers codified counterdrone techniques into the *Handbook on Tactics of Using FPV Drones by the Enemy (in Diagrams) and Methods of Counteraction*. This manual emphasizes the importance of early detection of enemy drones, either visually or using drone detectors, and their electromagnetic suppression through portable C-UAV EW jamming domes or antidrone rifles [15]. Despite the increasing density of C-UAV EW equipment on the front line, the impact on reducing drone threats remains uncertain. Both sides are engaged in intense EW competition and are facing two significant challenges.

The first challenge is the rapid changes and extension of frequency bands used by drones' onboard radio-electronic equipment. For instance, when Russian C-UAV EW devices began jamming standard commercial radio frequencies and navigation signals, the AFU responded by switching to less commonly used frequencies with higher power. The AFU then began testing jammed frequencies by sending a single drone; if the frequency was jammed, they would change it and send another, and if the drone successfully passed through, they would then send the rest through the unjammed frequency [19]. This adaptation forced Russian EW spectrum analyzers to detect the new frequencies and update their C-UAV jammers accordingly. In response, the AFU began utilizing frequency hopping to evade suppression [24]. In certain instances, Russians reprogrammed their drones to the same frequencies, causing the AFU to inadvertently jam their drones when attempting to counter Russian drones [46]. Both sides have learned that C-UAV EW devices cannot be fixed to any single frequency and must be constantly updated based on electromagnetic detection results. Open-source evidence indicates that the AFRF is field-testing C-UAV equipment that uses artificial intelligence (AI) to detect and suppress frequencies used by the AFU [47].

The second challenge is using advanced electromagnetic protection devices and technologies by drones to prevent C-UAV

jamming. For example, both sides have begun encrypting drone radio frequencies, causing drones to ignore signals that do not match the encryption key [38]. Additionally, more expensive drones utilize preprogrammed routes, necessitating precise position-tracking methods [24]. Finally, Ukraine and Russia are both developing drones equipped with onboard AI systems capable of identifying and locking onto targets, which can navigate using AI with inertial gyroscopes, thereby eliminating the need for command-and-control signals from operators and rendering them impervious to jamming [18].

In conclusion, the quick adaptation and widespread use of lightweight C-UAV EW devices by the AFRF highlight a significant change in the way of war, driven by the bottom-up battlefield realities in Ukraine. With the increasing threat from Ukrainian drones, especially the deadly FPV models, the AFRF has focused on enhancing electromagnetic protection at the company level. Initially reliant on large, vehicle-based EW systems, the AFRF faced critical vulnerabilities due to their high-value target status and limited coverage across a vast front line. In response, Russia bypassed traditional bureaucratic hurdles by dramatically accelerating the military innovation process of smaller, more flexible C-UAV solutions, including drone detectors, antidrone rifles, portable jamming domes, and vehicle-mounted jammers. After the diffusion of these technologies from Ukrainian forces, Russians implemented them through decentralized mass production and doctrinal integration.

The intense competition between Russia and Ukraine in countering drones highlights the need for continuous innovation to maintain an edge and has broader implications. The lessons learned from this war have shaped Russia's approach to warfare and influenced other countries like China to diffuse similar counterdrone technologies into their military [35].

Conclusions and Further Research

This article has demonstrated that the AFRF has successfully adapted its conduct of war based on lessons from the war in Ukraine, challenging previous assumptions about its rigidity. As argued in the introduction, the AFRF has effectively integrated new technologies and tactics—notably OWA Shahed drones, FPV drones, and lightweight C-UAV EW systems—to enhance combat effectiveness against the AFU, leading to demonstrable shifts in battlefield dynamics.

A Russian soldier carries an antidrone rifle. Since the beginning of the war in Ukraine, Russian soldiers have received improved antidrone rifles that are capable of drone detection at a distance of up to one kilometer. *Photo from the Russian Ministry of Defence*

Russia has successfully diffused and integrated Shahed drones, enabling cost-effective, long-range saturation attacks on Ukrainian critical infrastructure and population. By diffusing and implementing FPV drone warfare into its strategy, Russia has been able to carry out low-cost precision strikes that have significantly altered battlefield dynamics. Finally, the diffusion and use of lightweight C-UAV EW systems have enhanced Russia's ability to defend against the threat from Ukrainian drones at the company level.

Through the lens of military innovations theory, it is evident that Russia is adapting its tactics and technology based on lessons from Ukraine, institutionalizing changes within its doctrine, force structures, and the military-industrial complex. This ongoing process underscores the dynamic nature of modern warfare and the need for continuous advancements to maintain a strategic edge. Recognizing this, the Russian MOD announced the "Voentekh" project in February 2025 to accelerate the implementation of technological innovations by testing new products on the battlefield and introducing them to the AFRF [48].

Overall, the AFRF's ability to innovate and adapt through the integration of new technologies and tactics challenges conventional wisdom about its military capabilities and how Russia will reconstitute its military force following the war's conclusion in Ukraine [7]. The spread of these technologies to Russian allies highlights their broader impact on global security. These developments pose potential threats to the Baltic States and their NATO allies, in which they will need to address these challenges to be ready for future war. Further research could identify whether the Baltic States and their NATO allies need to change their legacy military strategies to enhance their AD systems to detect and counter the persistent threat of OWA drones like Shahed and invest in the development of lightweight C-UAV EW solutions to protect their combat vehicles and troops from the imminent threat of Russian FPV drones.

NATO's *2022 Strategic Concept* emphasizes the need to maintain technological superiority and invest in innovation [49]. Further research could also determine whether cheap and scalable OWA drones, FPV drones, and lightweight C-UAV EW solutions are mature enough innovations to be diffused and implemented into the Baltic States and their NATO allies' doctrine, force structures, and defense industries.

(The article was originally written as a research paper for the Baltic Defence College's Strategic Level Higher Command Studies Course. My thanks to Military Review*'s Beth Warrington, whose input significantly improved this article's clarity and overall quality.)*

Bibliography

1. Horowitz, M. C., Pindyck, S. What Is a Military Innovation and Why It Matters. *Journal of Strategic Studies* 46, 2023, No. 1. https://doi.org/10.1080/01402390.2022.2038572

2. Rubin, U. Russia's Iranian-Made UAVs: A Technical Profile. *RUSI*, 13 January 2023. https://www.rusi.org/explore-our-research/publications/commentary/russias-iranian-made-uavs-technical-profile

3. Armed Forces of Ukraine (AFU). Guidelines to Combined Arms Units to Combat Iranian-Made Strike UAVs "Shahed-136" ("Geran-2") and the Russian Federation "Lancet-2" (According to the Experience of the Russian-Ukrainian War of 2022–2023). Center for Operational Standards and Methods of Training of the AFU and Main Directorate of Doctrines and Training of the General Staff of the AFU, March 2023.

4. Starr, M. 'Demilitarization of Russia': Ukraine Says Russia Running Out of Missiles. *Jerusalem Post*, 16 October 2022. https://www.jpost.com/international/article-719795

5. Velikiy, A., Shorkin, N. Анализ развития БЛА типа «барражирующий боеприпас». Часть 1. *Арсенал Отечества*, 15 January 2025. https://arsenal-otechestva.ru/article/1910-analiz-razvitiya-bla-tipa-barrazhiruyushchij-boepripas-chast-1#

6. Hollenbeck, N. et al. Calculating the Cost-Effectiveness of Russia's Drone Strikes. *Center for Strategic and International Studies*, 19 February 2025. https://www.csis.org/analysis/calculating-cost-effectiveness-russias-drone-strikes

7. Grisé. M. et al., Russia's Military After Ukraine: Potential Pathways for the Russian Armed Forces. *RAND*, 16 January 2025. https://www.rand.org/pubs/research_reports/RRA2713-1.html

8. Albright, D. et al. Alabuga's Greatly Expanded Production Rate of Shahed 136 Drones. *Institute for Science and International Security*, 10 May 2024. https://isis-online.org/isis-reports/detail/alabugas-greatly-expanded-production-rate-of-shahed-136-drones/

9. Sebastian, C. et al., Russia Is Intensifying Its Air War in Ukraine. A Secretive Factory Is Ramping up Drone Production to Fuel the Offensive. *CNN*, updated 27 December 2024. https://edition.cnn.com/2024/12/27/europe/russia-ukraine-war-drones-alabuga-factory-intl-invs/index.html

10. Цветочки для ВСУ: как работают дроны «Герань-2» и «Гербера». *Izvestia*, 25 October 2024. https://iz.ru/1779810/2024-10-25/tcvetochki-dlia-vsu-kak-rabotaiut-drony-geran-2-i-gerbera

11. Cooper, T. Ukraine War, 29 December 2023: Start of the Winter Missile Campaign. *Sarcastosaurus Substack*, 29 December 2023. https://xxtomcooperxx.substack.com/p/ukraine-war-29-december-2023-start

12. Pokrova EW System Is a Real Game-Changer in the Ukrainian Fight Against Shahed-136 Drones and Cruise Missiles, That Renders GPS Receivers Useless. *Defense Express*, 4 November 2023. https://en.defence-ua.com/events/pokrova_ew_system_is_a_real_game_changer_in_ukrainian_fight_against_shahed_136_drones_and_cruise_missiles_that_renders_gps_receivers_useless-8462.html

13. Estonian Foreign Intelligence Service (EFIS), *International Security and Estonia 2025*. 20 December 2024, 14. https://raport.valisluureamet.ee/2025/upload/vla_eng-ra port_2025_WEB.pdf

14. Korshak, S. March 29—Day 1129—Belgorod in Focus, Defensive Drills with Drones, Balanced Attacks. *Medium*, 29 March 2025. https://medium.com/@Stefan.Korshak/march-29-day-1129-belgorod-in-focus-defensive-drills-with-drones-balanced-attacks-82fe7ecf6f8a

15. Добровольцы. Справочник. Тактика применения противником FPV-дронов (в схемах) и способы противодействия. Ministry of Defence of the Russian Federation, 2024, 3.

16. Orlova, A. Rethinking Warfare—Key Takeaways from Zaluzhny's CNN Column. *Kyiv Post*, 2 February 2024. https://www.kyivpost.com/post/27504

17. Farrell, F. Deadly Drone Arms Race Intensifies as Ukraine,

Russia Embrace the Future of War. *Kyiv Independent*, 13 September 2023. https://kyivindependent.com/head-first-into-the-future-inside-the-race-to-win-the-drone-war-in-ukraine/

18. Zafra, M. et al. How Drone Combat in Ukraine Is Changing Warfare. *Reuters*, 26 March 2024. https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/

19. FPV-революция: как дроны-камикадзе изменили ситуацию на фронте. Posted 6 June 2024 by Редакция. *YouTube*, 51 min. 51 sec. https://www.youtube.com/watch?v=qSP258qGYjU

20. Institute for the Study of War (ISW) Press, *Russian Offensive Campaign Assessment.* April 23 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-23-2024

21. Plamenev, I. Белоусов объяснил необходимость создания нового рода войск. *RBC*, 21 December 2024. https://www.rbc.ru/politics/21/12/2024/6766de049a79475899cc6ebb

22. General Staff of the Armed Forces of the Russian Federation. *Справочник. FPV-дроны применяемые ВС РФ в СВО.* 2024.

23. Hill, D. Don's Weekly, 6 January 2025: Part 3. *Sarcastosaurus Substack*, 6 January 2025. https://xxtomcooperxx.substack.com/p/dons-weekly-6-january-2025-part-3

24. Watling, J., Reynolds, N. Tactical Developments During the Third Year of the Russo-Ukrainian War. *RUSI*, 14 February 2025. https://www.rusi.org/explore-our-research/publications/special-resources/tactical-developments-during-third-year-russo-ukrainian-war

25. Hill, D. Don's Weekly, 19 February 2024: Part 1. *Sarcastosaurus Substack*, 19 February 2024. https://xxtomcooperxx.substack.com/p/dons-weekly-19-february-2024-part

26. Hill, D. Don's Weekly, 10 February 2025: Part 2. *Sarcastosaurus Substack*, 10 February 2025. https://xxtomcooperxx.substack.com/p/dons-weekly-10-february-2025-part-82d

27. ВУНЦ, ВВС. Эксплуатация и применение беспилотных летательных аппаратов (FPV-дронов). 2023.

28. Добровольцы. Применение ракет, гранат и инженерных

боеприпасов в качестве боевой части для различных типов БПЛА. Ministry of Defence of the Russian Federation, 2023.

29. В составе группировки войск «Запад» сформировали роту БПЛА. *TASS*, 26 January 2024. https://tass.ru/armiya-i-opk/19832741

30. Минобороны России. Андрей Белоусов проинспектировал работу нового Центра перспективных беспилотных технологий Минобороны. *Telegram*, 11 October 2024. https://t.me/mod_russia/44389

31. Белоусов: в ВС РФ сформируют «войска беспилотных систем». *TASS*, 16 December 2024. https://tass.ru/armiya-i-opk/22682103

32. ISW Press. Russian Offensive Campaign Assessment. January 28, 2025. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-28-2025

33. Trevithick, J., Rogoway, T. Russia Now Looks to Be Using Wire-Guided Kamikaze Drones in Ukraine. *TWZ*, 8 March 2024. https://www.twz.com/air/russia-now-looks-to-be-using-wire-guided-kamikaze-drones-in-ukraine

34. Hambling, D. New Drone Tactics Sealed Russian Victory in Kursk. *Forbes*, updated 20 March 2025. https://www.forbes.com/sites/davidhambling/2025/03/17/new-drone-tactics-sealed-russian-victory-in-kursk/

35. Cheung, S., McReynolds, J. Autonomous Battlefield: PLA Lessons from Russia's Invasion of Ukraine. *China Brief,* 28 March 2025, No. 6. https://jamestown.org/program/autonomous-battlefield-pla-lessons-from-russias-invasion-of-ukraine/

36. Martyniuk, Y. NHK: North Korea Built a Drone with Russian Help, Mass Production Starts This Year. *Euromaidan Press*, 8 February 2025. https://euromaidanpress.com/2025/02/08/nhk-north-korea-built-a-drone-with-russian-help-mass-production-starts-this-year/

37. Shumlianskyi, D. Serbian Army Begins Using Serbian-Made FPV Drones. *Militarnyi*, 29 December 2024. https://mil.in.ua/en/news/serbian-army-begins-using-serbian-made-fpv-drones/

38. Withington, T. Clear Channels. *Armada International*, 13 March 2024. https://www.armadainternational.com/2024/03/secure-drone-communications-milcom/

39. AFU Довідник військового зв'язківця. Засоби радіоелектронної боротьби та розвідки, які використовуються Російською федерацією. Command of the Signal and Cybersecurity Forces of the Armed Forces of Ukraine and Military Institute of Telecommunication and Information Technologies Named After the Heroes of Kruty, 2024.

40. Минобороны России. ПАМЯТКА по защите и противодействию БпЛА противника. Main Directorate of Combat Training.

41. Loh, M., Video Shows Ukraine's 'Hornet' Drones Following Russia's Tanks and Plopping Grenades on Top of Them. *Business Insider*, 26 September 2023. https://www.businessinsider.com/video-shows-ukraine-drones-following-russian-tanks-dropping-grenades-2023-9

42. New Saniya EW System Seeks to Protect Russian Tanks from FPV Drones, but Where's Overhyped Volnorez? *Defense Express*, 14 January 2024. https://en.defence-ua.com/weapon_and_tech/new_saniya_ew_system_seeks_to_protect_russian_tanks_from_fpv_drones_but_wheres_overhyped_volnorez-9181.html

43. Минобороны России. Методические рекомендации по обеспечению защиты БТР от FPV дронов. Main Armored Directorate of the Ministry of Defense of the Russian Federation, 2023.

44. Russian Troops Successfully Use Harpoon-3 Anti-Drone Systems in Ukraine. *Army Recognition*, 18 October 2022. https://www.armyrecognition.com/news/army-news/2022/russian-troops-successfully-use-harpoon-3-anti-drone-systems-in-ukraine

45. AFU. Довідник малі РЕБ ворога. Command of the Signal and Cybersecurity Forces of the Armed Forces of Ukraine and Military Institute of Telecommunication and Information Technologies Named After the Heroes of Kruty, 2023.

46. Withington, T. Check the Manual. *Armada International*, 14 March 2024. https://www.armadainternational.com/2024/03/

russian-fpv-drone-manual-milcom/

47. Van Brugen, I. Russia Deploying New AI-Powered Anti-Drone Devices. *Newsweek*, 30 April 2024. https://www.newsweek.com/russia-artificial-intelligence-ai-drones-ukraine-1895424

48. В Минобороны создали новую систему внедрения инноваций «Воентех». *TASS*, 18 February 2025. https://tass.ru/armiya-i-opk/23173057

49. NATO. NATO 2022 Strategic Concept. 2022, 8. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/ 290622-strategic-concept.pdf

50. Tuzov, B. ANALYSIS: Russia's Electronic Warfare Equipment. *Kyiv Post*, 11 May 2024. https://www.kyivpost.com/analysis/32435