Issue Brief

January 2026
No : 480

From Nadir Towards Zenith: The Rise of Russian Anti-drone Capability

Lt Gen (Dr.) VK Saxena,
PVSM, AVSM,VSM (Retd)

From Nadir Towards Zenith: The Rise of Russian Anti-drone Capability

Lt Gen (Dr.) VK Saxena, PVSM, AVSM, VSM, PhD (Retd)

Abstract

Russia is often known to be a mighty power when it comes to Ground Based Air Defence (GBAD) Weapon Systems. In the past, Russian GBAD arsenal has shown a 'chink in the armour' and that 'chink' is its conspicuous deficit of tailor-made anti-drone weaponry.

This work explores how this deficit has cost the Russians heavily in the past, in terms of disproportionate casualties at the hand of adversary's drone and missile power. The same was amply visible in the earlier months of the Russia-Ukraine War, till it was addressed in the years that followed.

Keywords: Ukrainian Drones, Russian Anti-drone Systems, Russia-Ukraine War

At the Nadir

Roll back to 2018, Russia had its Mediterranean footprint represented on the west Syrian coast at the Khmeimim Airbase and the Tartus Naval base. The former had a dominating presence of combat, air defence, electronic warfare (EW) and logistic aircrafts, while the latter had berths to secure as many as 11 warships! Ground based air defence (GBAD) was also played heavy. Khmeimim had the Pantsir S1 short to medium range (20-40 km) gun missile systems and the Igla series of MANPADs, while Tartus had an EW unit (Saxena, V.K. 2018).

Come 05 January 2025, and there was an attack on the above two bases by a mere 13 swarm drones (incidentally the first ever documented swarm drone attack). Result? Only 7 out of 13 drones could be destroyed by the mighty GBAD and EW systems, 6 still landed and caused significant damage at both bases.

The post-attack analysis revealed that the primary cause of swarm success was lack of tailor-made anti-drone weaponry in the Russian arsenal. The conventional air defence radars of the Pantsir system were unable to track small drones with very low Radar Cross Section (RCS) {a measure of visibility of an aerial object to radar}. Why so? Mainly because these radars are optimised for mainframe threat from such air threat vehicles like the combat strike aircrafts, attack

helicopters cruise missiles, anti-radiation missiles and more. These threat vehicles have much greater RCS.No radar detection meant no radar-controlled missile launch and resultantly, the 'little monsters' could cause significant damage on the two assets (Saxena, V.K. 2021).

A similar story unfolded in the initial phases of the Russia-Ukraine war wherein, the air defence weapons, of the Russian ground offensive force, pierced through the gut of Eastern Ukraine in the blitzkrieg mode and was typically deficit of anti-drone weaponry. The costs were punitive again. The Ukrainian, aware of this 'chink in the armour', struck successfully using the Bayraktar TB2 drones and the US switchblades, Aerorozvidka R18, Iranian Shahed 136 and Germanium -2 drones etc.).

Figure 1: Heavy Russian Tank Losses in the Initial Months of War

Source: https://www.google.com/search?q=Russian+tank+casualty+by+Ukraininan+drones

In the early months of the war, even the Russian ground-based EW punch, consisting of radar and communication jammers, did not carry the required punch. Reportedly, the entities that were supposed to be deployed centrally were split into penny packets and deployed on parallel thrust lines—not only they lost their cumulative punch, some EW networks became mutually interfering and were compelled to be pulled off air.

The Turnaround Begins

Faced with massive casualties of mechanizsd forces in the contact battle hit by drones and anti-tank missiles (according to one estimate some 1700 tanks and BMPs by June 2021) {RadioFreeEurope RadioLiberty, 2022}— the first sign of a turnaround started to appear towards

July-October 2022. This is when the Russians largely gave a pass to the headlong mechanised thrusts and made a switch to an old Russian tactics of large scale use of artillery to pulverise the targets before each troop contact. Big guns and rocket launchers boomed relentlessly across the Ukrainian battlefields (2S35 Koalitsiya-SV, SP Howitzers, 2S19 Msta-S Howitzers, 2A36 Giatsint towed and SP howitzers, rocket launchers - BM 21 GRAD P, BM30 Smerch, 9A 52-4 Tornado etc.(RadioFreeEurope RadioLiberty, 2022). Alongside this change, building of anti-drone muscle also started to pick up.

In the initial stages, Igla and Strela series of MANPADs were used to strike against the Ukrainian drone strikes. These proved ineffective against swarm done attacks which overwhelmed the defender's capabilities by sheer numbers.

At around this time (December 22 –January 23) Russian drone guns started to appear on the front lines. The first lot of weapons that were spotted included the LPD 820, and LPD 801, drone guns. These were basically rifle-based systems with drone detection capability up to one km. The kill was affected by firing a Radio Frequency Jammer working in the commercial frequency range of 2.4 GHz to 5.8 GHz, in order to disable radio-communication on the drone (TADVISER, 2023). The above guns were entry level systems as 1 km detection meant very little. Also, as many of the Ukrainian drones operated outside the commercial frequency bands, these remained undetected.

Almost on the heels of LPD series, another drone gun viz. PARS-S Stepashka made an appearance. The surveillance range went up marginally to 1.5 km and the effectiveness envelop was claimed to include the entire spectrum of drone frequencies including effectiveness on First Person View (FPV) drones that were GPS independent and homed on to their targets by operators guiding them based on their on-board camera feeds (TASS, 2023).

By the end of 2022, relentless Russian artillery and rocket launchers (of the type as stated earlier) coupled with an array of missiles (Iskander, Kalibr OTR 21 Tochka and, very selectively, Kinzhal aero-ballistic hypersonic missiles) {Saxena, V.K. 2022} were plunging Ukraine into a dark and cold winter (HRW, 2022) and (Vatman, T. and Hart, C. 2024).

Into the initial months of the new year, reports of a possible Ukrainian counter offensive started rolling in and with that came the decision by Kremlin for a planned pull back and dig into

a solid multi-layered defensive line across Kupiansk-Kreminna, Bakhmut, Robotyne, Mariupol **(See Figure 2)** {{RadioFreeEuropeRadioLiberty,2022}.

Figure 2: Russia-Ukraine War Advanceline

Source: https://www.thehindu.com/news/international/explained-is-ukraines-counteroffensive-working

It was on these defensive lines that the Russian EW warfare muscle that performed sub-optimally in the initial months of war started to gain ground.

Russia is a very strong EW power with its diverse arsenal spanning multiple communication and non-communication domains. The major equipment includes radar jammers (truck-mounted mobile jammers viz. Krasukha 2 and Krasukha 4 capable of jamming drones, ground radars, AWACS and LEO Satellites), VHF/UHF jammers (RB341V Leer3- optimised for jamming GSM cellular networks used for radars), GPS and SATCOM jammers (RH 330 ZHITEL- optimised for jamming satellite communications used by drones), Long range HF commination jamming system (Murmansk-BN), airborne fire control radar jammers (SPN 2,3,4 X and KU band jammers optimised for ground-based radars) and anti-drone jammers (repellent—Patrul jammer optimised for jamming the communications on small sized UAVs etc.) {Saxena, V.K. 2024}.

Figure 3: Krasukha 2 Drone and Radar Jammer

Source: www.google.com/search?q=krasukha+ii+and+krasukha+4+jammers

Once the above arsenal was deployed tactically as part of the Russian defensive system, it started to assert and the Ukrainian drone casualties started to mount. As per an open source statement by an Ukrainian drone operator, the drone operation time at the front lines had shrunk to just 3-4 minutes before a Russian EW system took it on.

As the casualties of Russian helicopter fleet, at the hands of Ukrainian FPV drones mounted, Russia scrambled to put up a viable defence. In October 2024, Russia came up with Multic jamming pods capable of being mounted on attack helicopters. The jamming pod had twin channels that had the capability of disrupting video signals (camera feeds) by the FPV drone – lifeline for their navigation to target—Multic has a detection range of 1000 m and jamming range of 500m. Even the band coverage is very wide that is 700 MHz to 6000 MHz (Mykhailenko, D. 2025).

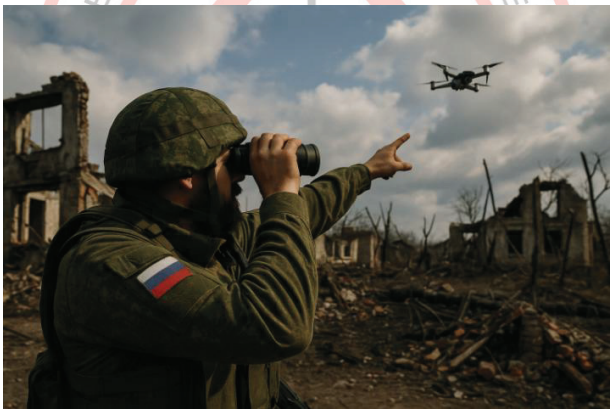
Besides the soft-kill RF guns, Russia also pressed into system kinetic Counter Unmanned Aerial Systems (C-UAS)— The most notable among them was the upgraded ZU 23-gun system. This 60s vintage Soviet-era weapon has been ageless; it has been upgraded with an electro-optical fire control system (EOFCS) comprising of a day CCD camera, night thermal camera based on forward looking infra-red(FLIR), a laser range-finder and a fire-control computing device. This system is capable of drone detection using the EO/IR resources and delivering effective guided fire on them at high volume (rate of fire of ZU 23 gun is 1600 rounds per minute per two barrels).

Even the ZU 23 ammunition has been reportedly modified to have the proximity fuse showing enhanced effects at target end.

For higher mobility and quick response, the guns have been mounted on High Mobility Vehicles (HMVs). Such vehicles also carry on-board multiple mounts of Rifles/LMGs (AK 12 and AK 74) to create mass anti-drone kinetic fire effect at close ranges in the visual domain. Recently, in October 2025, Russia displayed a robotic model of ZU 23 gun in the C-UAS role (Defence Express, 2025).

Another recent edition for very close quarter C- UAS role (100-150m) is the Izdelie 545 system that fires small projectile which interferes with the communication and the control system of the enemy drone. It is a low-cost small system mainly for front line soldiers and is operated in the visual domain of the Tactical Battle Area (Special Eurasia OSINT Team, 2025).

Figure 4: Izdelie 545 – Soldier lvel UAV defence



Source: https://www.specialeurasia.com/2025/10/05/russia-izdelie-545

There have also been reports of net cartridges that throw out a net to en-cage the drone or huge net fences to catch the incoming drones through entanglement (Unmanned Airspace, 2021).

Artificial intelligence is kicking in to power the latest generation of C-UAS systems. One such example in the Russian arsenal is the Gyurza drone detection and suppression system that is still in its prototype stage. All of 25 kg, the system powered by AI algorithms automatically detects the drones up to 1.5 km and generates dynamic suppression frequencies to cut/corrupt the

communication and video feed from the drone to its operator. The system is optimised for taking on the FPV drones and the swarm drones (RuAviation, 2024).

One other latest addition in the anti-drone arsenal is the Zont C-UAS system. It is a wearable device that resembles a bullet-proof jacket. True to its name ,meaning 'an umbrella', Zont, once operated, creates an umbrella of RF jamming frequencies ('bubbles') to cripple the FPV drones by interfering with their video streaming contact as well as the drone operator (Bisht, I.S. 2024).

In the kinetic kill suite, Russia, as of August 2025, has developed a family of interceptor drones that are capable of killing the Baba Yaga and Mavic category of Ukrainian drones. One such product is the Yolka drone— It is a catapult-launched fire-and-forget drone that is AI enabled (negative filtering algorithms) to detect enemy drones at a distance of 700-1000 m and kill it by a catastrophic collision with the same. Another variety of Yolka drones fire a kind of shotgun type of warhead to enhance the kill effect at the target end. Another is the Kinzhal Ovod PVD drone, that is based on the concept of kinetic kill either through catastrophic collision or by firing a small warhead.

To deal with sea-drones (Un-crewed Surface Vehicle or USV of the Black Sea fame) the Krestnik M drone can strike from air, land and sea platforms. All avenues of drone detection (and kill) are being exploited. 'Digital Patrol' is a network of acoustic sensors that can detect, classify and locate the drone based on their acoustic signatures. Also, the Granat 4 drone uses a laser-based drone detection system with a range capability from 100 m to 12 km (BCFA, 2025).

Another option, already being exploited for some time, is the use of very high rate of fire air defence weapons. These could be mainframe weapons such as the ZU23 gun (rate of fire 1600 rounds/min) ZSU23 4B1 Schilka weapon system (3400 rounds per minute) or small calibre anti-aircraft machine guns such as GShG gun (6000 rounds per minute). The target detection, especially in case of USV, is through thermal imaging system followed by the kinetic kill options as described above.

Another system in the trial phase is the Spider anti-drone device— this handheld weapon, when fired, sends out a projectile that expands into a net system upto 30 m (BCFA, 2025).

Some reflections

Following points are made:-

- In the wars of the recent past, Russia has paid heavily by taking disproportionate casualties, primarily owing to a clear deficit of tailor-made anti-drone weaponry in in its air defence arsenal.
- This 'chink in the armour' first came to light when a mere 13 drones caused significant damage at the Khmeimim air base and Tartus naval base, even when there were mighty air defence weapons deployed — the kind of Pantsir SI SRSAM, Igla series of MANPADs and one EW unit.
- The above deficit came out more loud and clear during the initial months of the Russia-Ukraine war. This was compounded by a volley of tactical mistakes done by the attacking force. These included not tactically deploying their ground-based air defence arsenal in a leap-frog mode and carrying them as convoy serials. Also, not making optimal use of the tremendous might of the Russian EW muscle as stated earlier.
- As if that was enough, Russia started to turn back by starting to revamp its anti-drone arsenal sometime in the later months of 2022.
- First, to make the appearance in the frontline were the simple hand-held drone guns, firing RF pulses on the incoming drones with a view to interfere with their electronics or GPS based communications.
- On a fast pace, the Russian war machine addressed all the drone detection and kill avenues and translated them into effective C-UAS systems. For detection, diverse means to include RF, EO, IR, Laser and acoustic were pressed in. Similarly, for the kill, multiple and diverse options were chosen. These, in the soft-kill domain, included RF jamming, EW attacks (hacking, phishing and more), laser-based burn outs, directed-energy weapons such as the high-power microwave. In the kinetic sphere as well, every avenue was put to use starting from high-rate- of-fire anti-aircraft machine guns or the mainframe air defence gun systems, micro drones in catastrophic kills, net-based capture and autonomous weapons.
- A new challenge was faced when the Ukrainians came up with the FPV drones and USVs. Sooner than latter C –UAS weapons started to appear to address this threat as well.

- Most noteworthy was the revamping of EW suite by the Russian war machine. Putting their earlier mistakes aside, the diverse inventory of the EW systems was deployed properly. This included centralisation and concentration of EW means and execution of EW operations in a co-ordinated manner.

On Co-ordination and Control

When such a diverse range of C-UAS weapons involving multiple detection and kill get concentrated in the Tactical Battle Area (TBA), there is a live problem of their networking in a layered and tiered C-UAS grid.

Normally, an altogether separate grid comprising of control Nodes communications and connectivity is required that can knit various functions related to drone-counter drone operations in the Tactical Battle Space (TBS).

TBS will actually mean the 2D construct of the TBA and the third dimension of the immediate airspace over it (say up to 10,000 ft) in which the drone-anti-drone operations unfold from the terminal range to around 12-15 km.

This TBS grid will be mainly responsible for the following:-

- Networking all the drone-detection sensors (RF, EO, IR, laser and radar) as well as, their associated kill means (normally configured on each completed C-UAS system) into one common grid.
- Have the AI-driven capability been able to fuse the detection inputs of multiple sensors into one common Air Unmanned Situation Picture (AUSP).
- Using negative-filter (taking out own) algorithms to convert the AUSP into Recognised AUSP (RAUSP) by classifying the drone threat into being friendly and hostile.
- Prioritising the threat in RAUSP based on immediacy and comparative lethality (in most of the small over-the-hill type drones there will be no time for any deliberate classification).
- Directing the fire of drone kill weapons on the threat in near real time.

- On the other side of the fence, maintaining a treasure-trove of drone- intelligence generated by own drones in the TBS and sharing the same on cloud for use by all stakeholders.
- Maintaining a plug-and-play coordination of air space and air defence engagement control with the air defence battle management command and control system (called the ADCRS) which is responsible to tackle the mainframe threat —from aircrafts, attack helicopters, cruise missiles, SSMs, ARMs, PGMs and more.

All this coordination is a huge task-vertical by itself and would call for a separate and independent grid for the TBS.

Keeping in mind the co-ordinated nature of drone and anti-drone operations underway by Russia, it will be fair to assume that such a grid is in place.

Incidentally, India on 09 October 2025 has also issued a Request for Proposal (RFI) for a C-UAS grid for the TBS— it is called SAKSHAM (Situational Awareness For Kinetic Soft and Hard Kill Asset management) {CENJOWS,2025}.

Figure 5: SAKSHAM

Source: https://www.google.com/search?q=SAKSHAM+C+UAS+grid+RFI+by+India

On the macro front, Russia has put together a dedicated branch for command, control and co-ordination of all drone warfare (drone as well as anti-drone). Such a force was reportedly created on 12 Nov 2025. It is designated as Unmanned System Force or USF.

The purpose of USF is to be a doctrine-owner for drone warfare and oversee the issue of planning, procurement, training, maintenance, tactics, future force development and logistic aspects related to drone warfare (Eruygur, B. and Aktas, A. 2025).

That is the story of the Russian anti-drone capability— indeed from nadir and now headed towards zenith!

Works Cited

Bisht, I. S. (2024, July 12). Russia develops counter drone umbrella system. *The DefensePost*. https://thedefensepost.com/2024/07/12/russia-counter-drone-system-2/. Accessed on 23 December 2025.

Eruygur, B. and Aktas, A. (2025, November 12). "Russia announces unmanned systems forces as new branch of military. *AA*. https://www.aa.com.tr/en/world/russia-announces-unmanned-systems-forces-as-new-branch-of-military/3741843#. Accessed on 25 December 2025.

Geran specialists have created Gyurza drone suppressor with artificial intelligence (2024, May 5). *RuAviation*. https://ruavia.su/geran-specialists-have-created-the-gyurza-drone-suppressor-with-artificial-intelligence/. Accessed on 22 December 2025.

Institute for Study of war: Russia develops new anti-drone interceptor that uses kinetic force only. (2025, August 25). *BCFA*. https://bcfausa.org/institute-for-the-study-of-war-russia-develops-new-anti-drone-interceptor-that-uses-kinetic-force-only/. Accessed on 23 Dec 2025.

LPD 820. *TAdviser*. Accessed on 19 December 2025.

Mykhailenko, D. (2025, October 17). Russia Deploys "Multik" EW Pods to Shield Helicopters From $500 Ukrainian Drones . *UNITED24 MEDIA*. https://united24media.com/latest-news/russia-deploys-multik-ew-pods-to-shield-helicopters-from-500-ukrainian-drones-12588. Accessed on 21 December 2025.

Revamping capabilities in the Tactical battle Space. *CENJOWS*. Accessed on 25 December 2025.

Russia Has Lost 50,000 Soldiers In Ukraine, U.K. Military Chief Says. (2022, July 17). *RadioFreeEurope:RadioLiberty*.https://www.rferl.org/a/russia-50000-casualties-ukraine/31947401.html. Accessed on 18 December 2025.

Russia's latest anti-drone gun capable of stunning FPV drones — design firm. (2023, April 21). *TASS*. https://tass.com/defense/1607883. Accessed on 19 December 2025.

Russia federal nuclear center develops missile based net capture C- UAS system (2021, April 5). *Unmanned Airspace*. https://www.unmannedairspace.info/counter-uas-systems-and-policies/russias-federal-nuclear-center-develops-missile-based-net-capture-c-uas-system/. Accessed on 22 December 2025.

Russian Kinetic Anti Drone "Izdelie 545" and Implications for Forward UAV Defence. (2025, October 5). *Special Eurasia*. https://www.specialeurasia.com/2025/10/05/russia-izdelie-545-uav-defence/. Accessed on 21 December 2025.

Russia Unveils Robotic ZU-23-2 Air Defense System — Yet Western Systems Still Outshine It (2025, October 19). *Defense Express*. https://en.defence-ua.com/news/russia_unveils_robotic_zu_23_2_air_defense_system_yet_western_systems_still_outshine_it-16195.html. Accessed on 21 December 2025.

Saxena, V.K. (2018, January 19). Commentary: First Ever Swarm Attack has Happened. *Vivekananda International Foundation (VIF)*. https://www.vifindia.org/print/4392?via=Azure. Accessed on 18 December 2025.

Saxena, V.K. (2021, July 14). Drone Threat– The Big Picture. *Vivekananda International Foundation (VIF)*. https://www.vifindia.org/article/2021/july/14/drone-threat-the-big-picture. Accessed on 18 December 2025.

Saxena, V.K. (2022, July 27). The Power of the 'God of War': Assessing the Russian advantage in Artillery in the Russo-Ukrainian War. *VIF*. https://www.vifindia.org/article/2022/july/27/the-power-of-the-god-of-war. Accessed on 20 December 2025.

Saxena, V.K. (2024, February 20). A Full Circle by Second Anniversary of Russia-Ukraine Conflict. *VIF*. https://www.vifindia.org/article/2024/february/20/A-Full-Circle-by-Second-Anniversary-of-Russia-Ukraine-Conflict. Accessed on 21 December 2025.

Ukraine: Russian attacks on Energy Grid Threatens Civilians (2025, December 6). *Human Rights Watch (HRW)*. https://www.hrw.org/news/2022/12/06/ukraine-russian-attacks-energy-grid-threaten-civilians. Accessed on 20 December 2025.

Vatman, T. and Hart, C. (2024, January 17). Russia's attacks on Ukraine's energy sector have escalated again as winter sets in. *IEA*. https://www.iea.org/commentaries/russias-attacks-on-ukraines-energy-sector-have-escalated-again-as-winter-sets-in. Accessed on 20 December 2025.

About the Author

Lt Gen (Dr) V K Saxena is the former Director General of the Corps of Army Air Defence. He is the Distinguished Fellow at VIF and a Visiting Fellow at CLAWS besides being a UN and a Law scholar. The General is a prolific writer who has authored five books and is regularly published by the Defence media of the country. He is also a regular at TV shows contributing on many a defence issues.