Issue Brief

February 2026
No : 488

The Next War Starts Inside the Fence: Internally Launched Drone Threats to Air/ Critical Assets & Way Ahead

Col Dharmendra Yadav, SM

The Next War Starts Inside the Fence: Internally Launched Drone Threats to Air/ Critical Assets and Way Ahead

Col Dharmendra Yadav, SM

Abstract

Internally launched First Person View (FPV) drones now threaten air and strategic bases, previously considered as secure. Drawing on recent covert campaigns in Ukraine and Iran, this article analysis how low-cost, GPS-Independent FPVs and swarm tactics bypass perimetre defences, exploit intelligence gap and inflict disproportionate damage. It assesses threat vectors from China and Pakistan against India, examines vulnerabilities in detection, command and control, logistics and evaluates countermeasures including layered sensors, electronic warfare, directed-energy, kinetic interceptors and hardened infrastructure. The paper recommends integrated, intelligence-driven rear-area defence with regulatory, supply-chain and community measures to restore resilience of critical assets.

Keywords: Internally Launched FPV Drones, Asymmetric Drone Warfare, Counter-UAS Defence in Rear Areas, Airbase and Strategic Asset Protection, Hybrid Warfare, Rear-Area Security.

Why the Need to Raise the Red Flag Now Against Armed First Person View (FPV) Drones?

In an era wherein drone warfare is reshaping the contours of conflict, recent operations by Ukraine against Russia and by Israel against Iran have exposed the vulnerabilities of even the most hardened airbases / strategic bases deep inside their borders. Ukraine's '*Operation Spider Web'* demonstrated the devastating potential of low-cost FPV drones, inflicting unrecoverable damage on five Russian airbases using covertly launched FPVs from within Russian territory. Similarly, during '*Operation Rising Lion'*, Israel's Mossad orchestrated internal FPV drone strikes that crippled Iran's air defence grid, disabling over 800 missile launchers and blinding key radar systems, before conventional air raids started. These actions demonstrated our notion that, the enemy will strike from across the border does not hold good anymore and shattered our defensive concept of air / strategic bases. These events underlined

a sobering reality: "the next strike on airbases / critical bases, around the world, may not happen from the air, but from within". Thus, we need to re-examine the defence approach to depth assets and be prepared for this asymmetric drone threat within land borders.

Development in the Field of Drone Warfare

Over the past two decades, the role of Unmanned Aerial Systems (UAS) has evolved from just niche surveillance and standoff attack platform to central tools of attack in modern warfare. Initially deployed for Intelligence, Surveillance and Reconnaissance (ISR) and standoff attacks, as seen with US Predators over the Balkans, drones are now employed in close lethal roles with unprecedented versatility and lethality. This transition has been driven by rapid advances in battery technology, compact warhead design and GPS independent navigation, enabling First Person View (FPV) drones to loiter up to 20 kilometres or more, penetrate radar coverage and survive around electronic jamming (Molina, M. Z., Hunder, M., Rao, A., & Kiyada, S., 2024).

More critically, drones are being integrated at scale. AI-enabled swarm tactics allow dozens of drones to autonomously coordinate, reassign targets mid-flight and saturate air-defence systems. What makes this trend alarming is the ingenuity with which drones are now deployed. Covert smuggling in civilian trucks, Trojan-horse tactics using disassembled components and decentralised operator cells enable strikes from within national borders, thus the bypassing conventional perimeter defences altogether. From Yemen to Gaza to Donbas, drones are increasingly the weapon of choice in hybrid warfare: affordable, deniable and deeply destabilising. Their speed of integration into military doctrines worldwide suggests that drone-based asymmetry will not remain an exception, but the rule.

Recent Surprise Attacks Around the World

Ukraine's 'Operation Spider Web' (01 June 2025)

The ongoing conflict between Ukraine and Russia has rapidly evolved into a high-tech contest of unmanned systems. Today's coordinated drone swarms far outstrip the rudimentary reconnaissance UAVs and single-platform strikes seen in 2014–2015, thus underscoring as to how both sides are pushing the envelope of aerial autonomy and electronic warfare.

Operation 'Spider Web' was a covert Ukrainian special-operations campaign aimed at striking deep inside Russian territory with low-cost FPV drones, hence demonstrating a new paradigm of stand-off precision attacks. Launched in early June 2025, it marked one of the most audacious long-range drone raids by Ukraine during the war.

Objective. Cripple Russia's long-range strike capability by hitting strategic bomber bases deep inside Russian territory (Meyn, C. 2025).

Planning and Execution. Over several months, Ukrainian special-operation teams smuggled in disassembled FPV drones and shaped-charge warheads by concealing them inside camouflaged truck-mounted cabins. On the dawn of 01 June 2025, 117 custom quadcopters launched simultaneously, from pre-planned sites near five airfields viz. Belaya, Dyagilevo, Ivanovo-Severny, Olenya and Ukrainka. Exploiting known gaps in S-300 and Pantsir coverage, operators guided their drones to strike fuel tanks, avionics bays as well as parked Tu-95MS and Tu-22M3 bombers (Fenbert, A. 2025).

Likely Reasons for Success. Russian tactical radars struggle with tracking low-RCS quadcopters, allowing FPV drones to slip through until it's too late. Russia's electronic-warfare countermeasures were either offline or poorly calibrated. No active jamming was engaged to disrupt drone navigation, hence enabling unimpeded guidance to key assets. Layered S-300 / Pantsir defences left coverage gaps at certain approach vectors, which planners meticulously exploited. Operational complacency and the assumption that remote airfields were beyond reach meant that no additional patrols or mobile air-defence groups were deployed around bomber shelters (Марущак, О. 2025). Moreover, concealing drones and warheads inside camouflaged truck-mounted cabins prevented any on-site surveillance or electronic signatures from revealing the operation until launch.

Impact. The assault destroyed or disabled upto 41 long-range bombers, thus inflicting multi-billion-dollar losses and grounding Russia's deep-strike strategic air fleet (Fenbert, A. 2025). Beyond material damage, the 'operation sowed doubt in Russian rear-area defences', proving that low-cost drones, when expertly coordinated, can penetrate even advanced air-defence networks.

Israel's Internal Drone Strikes in 'Operation Rising Lion' (June 2025)

Why Israel Opted for Drones on the First Night before Airstrikes during 'Operation Rising Lion'. Neutralising Iran's integrated air-defence grid before manned aircraft arrived was critical to avoid heavy IAF losses. Drones offered pinpoint precision against radar arrays and SAM batteries, thus reducing the need for large bomber formations that could trigger overlapping Iranian fire zones. Their small radar cross-section made early detection unlikely and autonomous dead-reckoning navigation ensured resilience against jamming. By deploying explosive-tipped drones first, Israel could blind key terrain and create corridors for follow-on strikes, hence maximising surprise and minimising collateral risk to pilots and civilian populations.

Objective. Blind Iran's integrated air-defence grid, SAM batteries and radar array, to secure air superiority for subsequent Israeli Air Force raids on nuclear and missile sites (Doornbos, C., McEntyre, N., and Crane, E. 2025).

Execution. Mossad staged a covert logistics campaign, siphoning drone components into Iran and assembling explosive-tipped quadcopters near the Esfajabad complex. In the early hours of 13–14 June 2025, these UAVs lifted off from clandestine launch points inside Iran—stealthily neutralising over 800 missile launchers and radar nodes (Doornbos, C., McEntyre, N., and Crane, E. 2025).

Likely Reasons for Success. The operation's success stemmed from exhaustive intelligence gathering, stealth logistics, and synchronised electronic-warfare planning. Mossad's months-long smuggling of drone units into Iran allowed for a rapid, covert launch without attracting attention. The UAVs' small radar signatures slipped past air defence batteries. Local human intelligence pinpointed vulnerabilities in Iran's S-300 umbrella, thus enabling a timed strike sequence that caused a system collapse (Berman, L., & Fabian, E. 2025). Iran's failure to patrol likely launch zones, coupled with overconfidence in static air-defence deployment and inadequate counter-UAV measures, left its SAM sites exposed and unable to repel the assault.

Impact. By neutralising the bulk of Iran's air-defence systems on 13–14 June 2025, the strikes slashed Iran's retaliatory missile capacity by roughly 80% and cleared the way for precision airstrikes with minimal interception (Berman, L., & Fabian, E. 2025).

Key Reasons for the Success of Asymmetric Attacks

Operation 'Spider Web' shattered the illusion of invulnerability of rear bases and Israel's internal drone operation underscored the perils of insider-launched UAV attacks. These operations may serve as 'blueprints for both state and non-state actors aiming to disrupt adversary airpower / strategic asset power without deploying a single conventional aircraft'. As we analyse, there are three key reasons that Ukraine and Israel succeeded in the strike: -

- All focussed on the front line.
- Intelligence failure of an impending attack.
- Areas around depth Airbases / Critical Bases did not sanitise.
- No systems in depth to identify and engage/ destroy the FPVs during the attack.

Therefore, there is an urgent need to 're-evaluate rear/ depth base security, particularly the need for intelligence-driven early warning systems, multi-layered defences, integration of counter-UAS technologies and active participation of Police/ CAPFs'.

Potential Threats from China and Pakistan

China

China is leader in new age drone production and poses a rapidly evolving drone-based threat to India's strategic infrastructure. The People's Liberation Army (PLA) has made unmanned systems a cornerstone of its future warfare doctrine. By 2026, it aims to field over one million AI-driven drones, ranging from tactical reconnaissance units to fully autonomous kamikaze, swarms capable of conducting coordinated saturation attacks lasting up to eight hours (QQ News, 2024). China's indigenous drone ecosystem, featuring the Wing Loong II, CH-5 and stealth GJ-11, has matured to global export levels. In the recent Ukraine-Russia conflict, Chinese DJI drone software was subverted by Russians to pinpoint Ukrainian operators and attack them (Skove, S. 2022). These drones can operate in concert with J-16D electronic warfare aircraft, which are designed to blind radar coverage and paralyse C-UAS networks during stand-off strikes, particularly near the Line of Actual Control (LAC) {Moneycontrol, 2023}.

Even more concerning is the possibility of covertly launched drone strikes from Indian soil. Given the porous terrain and connectivity near border zones, Chinese operatives can

smuggle in FPV drones, conceal them in safehouses or disguised vehicles and launch precision attacks from within the Indian territory. Airbases, hardened shelters, radar stations, missile batteries and Command & Control (C2) nodes are all vulnerable to such asymmetric tactics, especially in peacetime, when alert thresholds are lower.

Pakistan

Pakistan's drone capability has also expanded significantly through partnerships with Turkey and China, enabling a mix of imported and indigenously assembled systems. It now operates Turkish Bayraktar TB2 drones— the Songar armed quadcopter and Shahed-derived loitering munitions, some of which were tested during the May 2025 'Op Sindoor', wherein Pakistan deployed hundreds of drones to probe Indian air defences (Dimitra, S. 2025). In addition, cross-LoC drone incursions— often low-flying, radar-evading quadcopters— have dropped munitions, surveyed military infrastructure and conducted electronic intelligence (ELINT) runs in the Punjab, Jammu and Rajouri sectors.

What elevates the risk is "Pakistan's potential to exploit sleeper networks and cross-border infiltration routes to insert compact FPV drones" or launch cells into the Indian territory. Like Ukraine's Spider Web model, such teams could launch low-signature attacks on forward airbases, strategic fuel depots, satellite communication hubs, missile bases and C2 infrastructure. Pakistan's past record of using deniable, proxy tactics only adds to this possibility.

In sum, "both China and Pakistan possesses the capability, intent and opportunity to launch disruptive drone attacks on India". The targets they are most likely to strike, such as airbases, missile bases, air defence systems and C2 centres, are not just tactical but strategic assets essential to India's warfighting capability. Hence, addressing this threat will require a 'layered mix of technology, intelligence and doctrinal adaptation' and more so, very urgently.

Way Forward: Multi-Layered Defence Framework for India

A truly resilient defence base needs to 'weave together detection, denial, hardening, intelligence gathering, physical security and organisational cohesion, preferably under a unified tri-service command'. Each layer adds depth and redundancy, ensuring that if one fails,

others will still protect critical assets. Some of the urgently needed actions to protect rear / depth bases are suggested in subsequent paragraphs.

Detection and Early Warning

- **Enhanced Radar and Sensors**
    - ***Low-Radar Cross Section (RCS) Detecting Radars:*** Retrofit existing 3D radars with low-RCS detection modes and high-angle tracking to spot small, fast FPV drones at 15–25 km ranges (Griffin, B., Balleri, A., Baker, C., Jahangir, M., & Harman, S. 2022).
    - ***Mobile Low-Level Transportable Radar (LLTR) 'Ashwini' Units:*** Place mobile low-frequency radars such as 'Ashwini' on high grounds to detect swarm ingress from unexpected vectors (Deshpande, S. 2025).
- **Passive and Unconventional Sensors**
    - ***Acoustic Arrays and Infrared Towers:*** Install distributed microphone clusters and EO/IR (Electro-Optical/Infrared) cueing masts to triangulate drone swarms before they enter radar coverage (Maneice, C. 2016, March 11).
    - ***LiDAR (Light Detection and Ranging) Fencing:*** Erect LiDAR-based perimeter 'tripwires' that flag objects < 0.5 m² in size, day or night (Senstar, 2025).
- **AI Fusion C2 Node**
    - ***Multi-Source Data Fusion:*** Integrate satellite Electro Optical (EO) / Infrared (IR), ground radar, passive sensors and air-traffic feeds into an AI-driven command node (Tennant, A. 2024).
    - ***Real-Time Swarm Clustering:*** Use machine-learning algorithms to identify hostile drone formations and cue intercept assets automatically (Ashush, N., Greenberg, S., Manor, E., & Ben-Shimol, Y. 2023).

- **Active Denial and Interdiction**

- **Electronic Warfare (EW)**

    - ***FrequencyAgile Jammers:*** Deploy vehicle-mounted and rooftop jamming pods that dynamically sweep common FPV control bands.

    - ***Global Navigation Satellite System (GNSS)-Spoofers & Link Disruptors:*** Position net-disruptor towers around perimetres to sever GPS and video-feed links, forcing drones into 'fail-safe' hover or return modes (RoboticsBiz , 2024).

    - ***OFC Cutter Tech:*** OFC is increasingly used in advanced drones to resist electronic warfare tactics like jamming and spoofing, and ensuring secure, high-speed data transmission. To counter this, Quick Reaction Teams (QRTs) must be equipped with specialised OFC cutter technology (Sabbagh, D. 2025).

- **Directed-Energy Weapons (DEW)**

    - ***High-Power Laser Systems:*** Install truck-mounted HEL batteries (e.g., DRDO prototypes) capable of engaging drones at 500–1000 metres (Tennant, A. 2024).

    - ***Microwave Emitters:*** Integrate short-range microwave cannons to fry drone electronics in flight (Sherman, J. 2024).

- **Kinetic Interceptors**

    - ***C-RAM (Counter Rocket, Artillery and Mortar) Guns & Counter-Drone Artillery:*** Adapt 35 mm twin-barrel systems with airburst ammunition optimised for small-UAS swarms (IDRW, 2025).

    - ***Short-Range Man-Portable Air Defence Systems (MANPADS):*** Emplace infrared and radar-guided point-defence missile systems such as VSHORAD (Very Short-Range Air-Defence) system, at key choke points around the apron (Mittal, V. 2025).

- **Drone-On-Drone Tactics**

    - ***Camouflaged Interceptor Fleets:*** Station disguised 'friendly' FPV drones on early-warning nets; once hostile drones approach, they swarm in pairs to net or ram them (Deshpande, S. 2025).

    - ***Automated 'Drone Traps':*** Hang lightweight, spring-loaded nets around static assets that deploy when a radar cue is triggered.

Passive Denial and Interdiction Measures

- **Hardening & Dispersal**

    - **Next-Gen Hardened Shelters**

        - ***Modular Blast-Resistant Units:*** Rapidly deployable shelters rated for shaped-charge and tandem warhead penetration. This would incur heavy cost and hence needs to be done on selective bases as per priority.

        - ***Integrated C-UAS Jamming:*** Embed EW nodes within shelter roofs to counter drones targeting parked aircraft. These would be effective against a drone working on RF communication (Lykou, G., Moustakas, D., Gritzalis, D , 2020).

- **Apron Dispersal and Alternate Strips**

    - ***Staggered Run-Around Pads:*** Construct multiple pad networks with mobile revetments to avoid concentration of aircraft.

    - ***Highway Strip Operations:*** Regularly exercise sorties from designated Highway strips to complicate enemy targeting.

- **Camouflage / Protective Nets**

    - ***Temporary Camouflage Nets:*** Keep the aircrafts and strategic assets concealed under multispectral camouflage nets to reduce detection across visible, infrared and radar spectrums (The Indian Express, 2022).

This would deny visibility as well as work as a shield against small FPVs.

- ***Protective Nets:*** Have simple protective nets around Hangars, boundary walls and parking bays to prevent the enemy's small quadcopters or FPVs from striking own assets.

- **Physical and Human Security**

  - **Perimeter Patrol and Surveillance**

    - ***Integrated Patrol Routes:*** Combine foot, vehicle and UAV patrols in randomised schedules in suspected areas to deter insider launch teams from operating.

    - ***Watchtowers and Observation Posts with Anti-Drone Guns:*** Elevated posts equipped with EO/IR binoculars and Anti-Drone Guns (Deshpande, S. 2025) to observe and take immediate measures with rapid-reaction teams on standby.

- **Rapid-Response Teams**

  - ***Quick Reaction Teams (QRTs):*** Train dedicated C-UAS teams with man-portable interceptors to sweep suspicious areas during heightened alert situations.

  - ***Explosives / Bomb Disposal (ED/ BD) Units:*** Position ED/ BD teams within the base to be ready to safely neutralise any drone if found with live ordnance attached.

- **Community and Personnel Vigilance**

    - ***Civilian Drone Spotter Network:*** Engage and train locals to immediately inform of any suspicious persons or activities happening around the military bases. A social media group/hotline can be made to facilitate quick reporting.

- ***Insider Threat Mitigation:*** Conduct regular surprise background checks with Police, rotate duty assignments and employ biometric access controls at the entry gates.

- **Intelligence and Security Measures**

  - **HUMINT/SIGINT Fusion**

    - ***Adversary Network Penetration:*** Task joint intelligence teams to infiltrate the adversary's drone supply chains and disrupt logistics nodes before components cross the border.

    - ***Social Media Monitoring:*** Intercept the planning chatter on known encrypted channels like Telegram, Whatsapp, Signal, feeding real-time alerts to C2 nodes.

- **Supply-Chain and Cyber Integrity**

  - ***Vendor Vetting and Audits***: Mandate government certification for all drone-component suppliers, conduct unannounced inspections of factories and warehouses.

- **Legal and Regulatory Controls**

  - ***Drone Registration and Geo-fencing:*** Expand mandatory UAV registration to all cities within 300 km of key bases; enforce no-fly zones with 'geo-fencing software' on commercial drones (Sabbagh, D. 2025).

  - ***Import/ Export Licensing:*** Tighten scrutiny on cross-border drone parts trade, and leverage customs data analytics to flag suspicious shipments.

- **Organisational and Doctrinal Reforms**

  - **Tri-Service Counter-UAS Command**

    - ***Unified Task Force:*** Create a single chain of command under the Chief of Defence Staff that oversees all drone offence and defence planning,

thus ensuring seamless ISR sharing, joint targeting and resource allocation.

- **Standard Operating Procedures (SOPs)**
  - ***Airbase Defence Manual:*** Publish an integrated doctrine covering sensor-shooter hand-offs, QRT activation and escalation-of-force guidelines tailored for UAS threats. This should be done at each base level by Base Commanders.
- **Joint Exercises and Wargames**
  - ***Live-Fly Swarm Drills:*** Conduct annual large-scale exercises simulating multi-axis drone swarm attacks, with red-team evaluation and after-action review.
  - ***Tabletop Wargames:*** Integrate C-UAS scenarios into service-wide wargames and staff college curriculum to engrain decision cycles.

Conclusion

Operation Spider Web and Israel's internal drone strikes during Operation Rising Lion demonstrates that 'no rear-area security zone is invulnerable to low-cost, asymmetric UAS threats. India, sandwiched between two peer adversaries capable of fielding kamikaze swarms from inside own territory, must adopt a "layered, integrated defence posture" from cutting-edge detection to kinetic and non-kinetic denial: from hardened infrastructure to unified tri-service command and intelligence fusion. Only through coordinated action across technology, infrastructure, doctrine and policy can Indian air/ strategic bases remain shielded from the next 'Spider Web' looming on its horizon.

Works Cited

腾讯网. (2024, December 23). 美媒:解放军采购百万无人机,2026年交付,提前为战争做准备 _ 腾讯新闻. Copyright 1998 - 2025 *Tencent*. All Rights Reserved. https://news.qq.com/rain/a/20241223A09FTE00.

Admin. (2025, May 23). India's urgent need for a C-RAM-Type system to counter Pakistani drone threats - Indian Defence Research Wing. *Indian Defence Research Wing*. https://idrw.org/indias-urgent-need-for-a-c-ram-type-system-to-counter-pakistani-drone-threats/.

Ashush, N., Greenberg, S., Manor, E., & Ben-Shimol, Y. (2023). Unsupervised drones swarm characterization using RF signals analysis and machine learning methods. *Sensors*, 23(3), 1589. https://doi.org/10.3390/s23031589.

Berman, L., & Fabian, E. (2025, June 13). Mossad set up drone base in Iran, UAVs took out missile launchers overnight. *The Times of Israel*. https://www.timesofisrael.com/mossad-set-up-drone-base-in-iran-uavs-took-out-missile-launchers-overnight/.

China's expanding military drone ecosystem is a menace for the likes of Taiwan and India. (2023, October 17). *Moneycontrol*. https://www.moneycontrol.com/news/opinion/chinas-expanding-military-drone-ecosystem-is-a-menace-for-the-likes-of-taiwan-and-india-11544611.html.

Deshpande, S.(2025, March 13). How indigenous transportable radar Ashwini can boost India's air defence capabilities. *The Print*. https://theprint.in/defence/how-indigenous-transportable-radar-ashwini-can-boost-indias-air-defence-capabilities/2546731/.

Dimitra, S. (2025, May 16). Poor performance of Turkish and Chinese drones puts Pakistani army in difficult position – OPEd. *Eurasia Review*. https://www.eurasiareview.com/16052025-poor-performance-of-turkish-and-chinese-drones-puts-pakistani-army-in-difficult-position-oped/.

Doornbos, C., McEntyre, N., & Crane, E. (2025, June 13). How Israel's Mossad covertly infiltrated Iran to launch unprecedented attack: Fake meetings, secret drones, smuggled missiles. *New York Post*. https://nypost.com/2025/06/13/world-news/israel-mossad-infiltrated-iran-to-damage-air-defence-systems-during-operation-rising-lion-airstrikes/.

Editorial. (2024, June 13). Top 15 most effective anti-drone technologies (C-UAS). *RoboticsBiz*. https://roboticsbiz.com/top-15-most-effective-anti-drone-technologies/.

Express News Service. (2022, August 25). IAF procures 6,000 Multi-Spectral Camouflage Nets for enhanced protection of its strategic installations. *The Indian Express*. https://indianexpress.com/article/cities/pune/iaf-procures-6000-multi-spectral-camouflage-nets-for-enhanced-protection-of-its-strategic-installations-8110921/.

Fenbert, A. (2025, June 10). Ukraine's SBU releases new footage of Operation Spiderweb drone strike on Russian Tu-22 bomber. *The Kyiv Independent*. https://kyivindependent.com/ukrainian-drone-strikes-russian-tu-22m3-bomber-new-footage-of-operation-spiderweb-from-sbu/.

Griffin, B., Balleri, A., Baker, C., Jahangir, M., & Harman, S. (2022). Development of a passive dual channel receiver at L-Band for the detection of drones. 2021 18th *European Radar Conference* (EuRAD), 106–109. https://doi.org/10.23919/eurad50154.2022.9784465.

Lykou, G., Moustakas, D., Gritzalis, D., & Department of Informatics, Athens University of Economics & Business (AUEB). (2020). Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. *Sensors*, 20, 3537–3537. https://doi.org/10.3390/s20123537.

Maneice, C. (2016, March 11). Department of Justice uses Army equipment to locate shooters.

www.army.mil.
https://www.army.mil/article/163939/department_of_justice_uses_army_equipment_to_locate_shooters.

Mittal, V. (2025, February 11). The Indian military is developing domestic Counter-Drone capabilities. *Forbes*. https://www.forbes.com/sites/vikrammittal/2025/02/11/the-indian-military-is-developing-domestic-counter-drone-capabilities/.

Molina, M. Z., Hunder, M., Rao, A., & Kiyada, S. (2024, March 26). How drone combat in Ukraine is changing warfare. *Reuters*. https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/.

Марущак, О. (2025, June 3). Помста від Путіна за літаки: військовий експерт попередив про загрозу найближчими днями. *ТСН.Ua*. https://tsn.ua/exclusive/pomsta-vid-putina-za-litaky-viyskovyy-ekspert-poperedyv-pro-zahrozu-u-nayblyzchi-dni-2841533.html.

Meyn, C. (2025, June 2). Ukraine hits Russian bombers in major drone strike: What to know. *The Hill*. https://thehill.com/policy/defence/5328715-ukraine-strikes-russian-airbases/.

Sabbagh, D. (2025, April 23). 'They cannot be jammed': fibre optic drones pose new threat in Ukraine. *The Guardian*. https://www.theguardian.com/world/2025/apr/23/they-cannot-be-jammed-fibre-optic-drones-pose-new-threat-in-ukraine.

Sherman, J. (2024, February 20). New Microwave Weapons Could Defend against Swarms of Combat Drones. *Scientific American*. https://www.scientificamerican.com/article/new-microwave-weapons-could-defend-against-swarms-of-combat-drones/.

Skove, S. (2022, October 17). How Ukraine learned to cloak its drones from Russian surveillance. *C4ISRNet*. https://www.c4isrnet.com/battlefield-tech/2022/10/17/how-ukraine-learned-to-cloak-its-drones-from-russian-surveillance/.

Surya Valliappan Krishna, Ashima Singh (2023, July 10). Drone intrusions along the India-Pakistan international Border: Countering an emerging threat. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/posts/2023/07/drone-intrusions-along-the-india-pakistan-international-border-countering-an-emerging-threat.

Tennant, A. (2024, January 29). Speedy UAV Swarms Detection, Identification, and Tracking using Deep Learning. https://www.linkedin.com/pulse/speedy-uav-swarms-detection-identification-tracking-using-tennant-hmxye.

3D LiDAR and Perimeter Security (2025, March 11). *Senstar*. https://senstar.com/senstarpedia/3d-lidar/.