Spider Web: An Attack with Far-Reaching Implications

Major General Jagatbir Singh, VSM (Retd)[@]

Abstract

The article examines Operation 'Spider Web', a covert Ukrainian drone strike that penetrated deep into Russian territory, targeting strategic airbases with unprecedented precision. Blending elements of magical realism and cutting-edge warfare, the attack bypassed Russia's formidable air defence by launching first-person view drones from within its borders, employing smuggled commercial technology, remote control systems, and likely artificial intelligence-assisted targeting. This marked a tactical shift in modern conflict, demonstrating how low-cost, improvised systems can inflict high-value damage. The article details the operational ingenuity, including clandestine transport, remote launches, and use of open-source autopilot frameworks. It underscores broader implications for airspace management, the vulnerability of rear areas, and the necessity of adaptive defence strategies. Drawing lessons for India, the article calls for regulatory oversight of drone manufacturing, enhancement of counter-drone capabilities, and a whole-of-nation approach to emerging threats. Ultimately, the operation exemplifies how technological innovation, not just firepower, is redefining warfare.

[@]**Major General Jagatbir Singh, VSM (Retd)** is a Distinguished Fellow at the United Service Institution of India. Commissioned into 18 CAVALRY in Dec 1981, he has held varied appointments in different terrains including command of an Armoured Division. He has been an Instructor at the Indian Military Academy and has been an Instructor and Senior Instructor and Head of Training Team at the Defence Services Staff College. A prolific writer, his articles have been published in various newspapers and magazines.

Journal of the United Service Institution of India, Vol. CLV, No. 640, April-June 2025.

Introduction

Magical realism is a genre of writing that blends fantasy and reality in a way that feels natural and believable. On 01 Jun, drone-based operations on Russia launched by Ukraine striking five airbases deep inside Russian territory aligned both fantasy and reality, which prompted the Economist to rank it 'Among the greatest military raids in history'.[1] Soon after, the Russian Defence Ministry said in a statement, "Today, the Kyiv regime staged a terror attack with the use of First-Person View (FPV) drones on airfields in the Murmansk, Irkutsk, Ivanovo, Ryazan, and Amur Regions".[2] Ukraine, stated that at least 40 aircrafts had been damaged, specifying that these included nuclear capable Tu-95 and Tu-22 strategic bombers, earlier used to 'Bomb Ukrainian cities'. Russia's Defence Ministry only confirmed that "Several aircrafts caught fire".[3]

Two of the airbases struck, Olenya and Belaya, are around 1,900 kms and 4,300 kms from Ukraine. The first is in the Russian Arctic and the other in Eastern Siberia. The operation is another example of just how rapidly technology and innovative thinking are changing the battlefield. It marks a turning point in how low-cost, improvised unmanned systems can be employed with strategic impact deep behind enemy lines. To quote the Economist, "New technology deployed inventively can be lethal".[4]

The increasing and innovative drone deployment, concealment, and fusion with precision weapons undoubtedly shows the asymmetric power of low-cost high impact operations.

The Conduct

The Ukrainian media claimed that the large-scale special operation was conducted by *Sluzhba Bezpeky Ukrayiny* (SBU), Ukraine's Special Security Service. The planning and preparation started 18 months ago. Russia has highly capable Air Defence (AD) systems and so, it was impossible to strike it from Ukraine. Hence, a plan was made to hit Russia from within Russia, thereby, by-passing its AD wall. The operation has been launched under a special operation, code-named *Pavutyna* (Spider Web), aimed at degrading Russia's long-range strike capabilities. President Volodymyr Zelenskyy congratulated SBU head Vasyl Maliuk for the 'Absolutely brilliant result' of the operation.[5] Ukraine reportedly planned the attack for a year. The drones were packed onto pallets inside

wooden containers with remote-controlled lids and then loaded onto cargo trucks, with the crates being rigged to self-destruct after the drones were released, obliterating forensic evidence and preventing Russia from analysing the technology used. These cargo trucks then smuggled the drones into Russia, blending with normal Russian highway traffic. The trucks were camouflaged with wooden structures, likely posing their payload as cargo shipments, such as lumber or construction materials.[6] Some of these may also have had false license plates or forged documents to pass Russian checkpoints unnoticed. As an added advantage, Russia's vast road network and relatively porous internal transport system made it hard to monitor every vehicle. The trucks were then apparently driven to locations near airbases by drivers who were seemingly unaware of their cargo. Finally, the drones were launched and set upon their targets.

Roofs of the wooden cabins carried by the trucks were opened by remote control, with the drones being simultaneously launched to attack Russian airbases. Once launched, these aerial vehicles relied on Global Positioning System/inertial guidance systems to fly autonomously toward distant Russian airbases. The drones were adapted to FPV multirotor platforms, which allows the operator to get a first-person perspective from the aerial vehicle's onboard camera.

Apparently, Ukraine used North Atlantic Treaty Organization-supplied satellite data and Intelligence, Surveillance, and Reconnaissance (ISR) to identify the exact positions of Russian bombers, gaps in radar coverage, and safe launch zones deep inside Russia.[7]

Videos circulating online show the drones emerging from the roof of one of the vehicles involved. A lorry driver interviewed by Russian state outlet *Ria Novosti* claimed that he and other drivers tried to knock down drones flying out of a truck with rocks. "They were in the back of the truck, and we threw stones to keep them from flying up, to keep them pinned down", he said.[8]

Using 117 drones, Ukraine was able to reach regions thousands of kilometres from the front, compared to its previous attacks which generally focused on areas close to its borders. Once the drones were launched from within their territory, Russia's defences had very little time to react, as the aerial vehicles bypassed swiftly border surveillance.

The SBU stated that the strikes had managed to hit Russian aircrafts worth USD 7 bn at four airbases. The cost curve, using relatively cheap systems to destroy billions of dollars' worth of Russian combat power, has also been turned on its head.

As per reports regarding Operation Lion, Israel's Mossad had smuggled weapons into Iran ahead of the 13 Jun strikes, establishing a base of operations from which it remotely launched explosive-laden drones and positioning short-range, precision weapons near critical surface-to-air missile systems.[9]

This base played a pivotal role in the early stages of the operation, with Unmanned Aerial Vehicles (UAVs) launching overnight to neutralise surface-to-surface missile launchers, radar systems, and AD networks. These strikes from within were not high yield in firepower but strategically designed to create temporary blind spots in radar coverage and confuse ground coordination during the critical opening moments of the Israeli air campaign. The base was established through gradual smuggling of drones, surveillance gear, and command modules via Mossad intelligence networks, and is believed to have operated with local assistance from sleeper cells or sympathetic insiders. This is similar to what was witnessed in the Ukrainian drone strike on Russian strategic assets.

Use of Commercial Technology

Ukraine demonstrated a hybrid approach to drone warfare that combined remote human control with elements of autonomy and potentially Artificial Intelligence (AI)-assisted functionality. While the operation was not fully autonomous, the available evidence suggests that AI likely played a supporting role in both flight stability and targeting, particularly in enabling precise strikes on vulnerable components of high-value aircraft.[10]

Apparently, the FPV drones were controlled through Russian mobile telecommunications networks, including 4G and Long Term Evolution (LTE) connections. These networks provided sufficient bandwidth to support real-time video transmission and command inputs across vast distances, allowing Ukrainian operators to manage drone flights from outside Russian territory. This avoided the need for any physical ground control stations or nearby operators. As per reports, the drones relied on a software-hardware system built around ArduPilot, a widely used, open-source autopilot framework designed

for UAVs. In this case, each drone was integrated with a compact onboard computer, connected to a webcam and an LTE modem via Ethernet. The camera feed was used for visual navigation, while control signals were routed through ArduPilot.

In addition, AI-assisted targeting appears to have been integrated into the drones' attack logic. According to open-source intelligence, SBU teams studied construction and visual profiles of the targeted aircraft to identify precise weak points which enabled rapid and precise final-stage manoeuvring during the dive attack.

Ubiquitous Role of Drones

Drones first came to the fore during the Azerbaijan-Armenian Conflict, and these were the Turkish TB2 Bayraktar. However, the Russia-Ukraine War has seen the rise of an array of military capabilities including the use of drones en-masse as one-way attack systems previously only used in small quantities.

Prior to the war, drones were associated with remotely piloted platforms, such as the MQ-9 Reaper—a High-Altitude Long-Endurance (HALE) system—and the Heron, a Medium-Altitude Long-Endurance (MALE) system. These were essentially large platforms capable of loitering thousands of feet in the air for days to conduct surveillance missions and/or launch precision Hellfire missiles against potential targets.

Military drones, also known as unmanned aerial vehicles, are broadly categorised by their size, mission, and capabilities. These include micro/nano drones, tactical drones, MALE drones, HALE drones, and unmanned combat aerial vehicles. They are used for reconnaissance, surveillance, strikes, and logistics.

There is also the tactical use of quadcopters for small-unit surveillance, FPV one-way attack systems flown in short ranges into targets, and longer-range one-way attack systems like the Iranian-built Shahed-136, which can go hundreds or thousands of kilometres and it has been used regularly by Russia in this conflict.[11] The use of these drones for attack has become a new, ubiquitous form of conventional warfare. Many are based on commercially-available technology, and they are relatively cheap—from as little as a few hundred dollars to tens of thousands of dollars. They are easy to produce and often have open architectures, which means the software is easy to update in response to jamming or other defensive

countermeasures. AI is being increasingly used to enhance the capabilities of military drones, such as autonomous navigation and target recognition. In addition, there is an increasing employment of smaller drones in swarms working together to achieve a common goal. One-way attack drones of different sizes and ranges at speed and scale have transformed the battlefield. Operation Spider Web also appears to show the growing use of AI in one-way attack drones. AI, in this context, does not mean the most advanced and expensive large language models, but often simple algorithms trained on very specific datasets.

Evaluation

The idea behind Operation Spider Web was to transport small, FPV drones close enough to Russian airfields to render traditional AD systems useless. President Zelenskyy said the attack "Had an absolutely brilliant outcome" and dubbed it as 'Russia's Pearl Harbour', one that demonstrated Ukraine's capability to hit high-value targets anywhere on enemy turf, dealing a significant and humiliating blow to the Kremlin's stature and Moscow's war machine.[12]

"Our people operated across several Russian regions in three different time zones. And the people who assisted us were withdrawn from Russian territory before the operation, they are now safe", the Ukrainian President stated.[13]

Dr Steve Wright, a United Kingdom-based drone expert, told the BBC that the drones used were simple quadcopters carrying relatively heavy payloads.[14] However, in his view, what made this attack 'Quite Extraordinary' was the ability to smuggle them into Russia, and then launch and command them remotely. This, he concluded, had been potentially achieved through a link relayed through a satellite or the internet. Although the full extent of the damage from these Ukrainian strikes is unknown, the attacks showed that Kyiv was adapting and evolving in the face of a larger military with deeper resources. As per Justin Bronk of the Royal United Services Institute, "If even half the total claim of 41 aircrafts damaged/destroyed is confirmed, it will have a significant impact on the capacity of the Russian long-range aviation force to keep up its regular large-scale cruise missile salvos against Ukrainian cities and infrastructure".

Lessons Regarding Air Space

Nations treat their airspace as sovereign, a controlled environment that is mapped, regulated, and watched over. AD systems are built on the assumption that threats come from above and from beyond national borders. Yet, Operation Spider Web exposed what happens when countries are attacked from within. The drones flew low, through unmonitored gaps, exploiting assumptions about what kind of threat was faced and from where. In low-level airspace, responsibility fragments and detection tools evidently lose their edge.

As per Lieutenant General Ashok Shivane, former Director General Mechanised Forces, "AD grids are designed to track ballistic arcs, intercept radar signatures, counter drones, and maintain exclusion zones. None of those countermeasures apply when the threat is pre-assembled behind the lines, activated by remote control, and flown by handheld devices. Russia's vast AD network was not breached; it was bypassed. And that distinction is fatal". [15]

Spider Web worked, not because of what each drone could do individually, but how the operation was designed. The cost of each drone was low, but the overall effect was high. This is not just asymmetric warfare, it is a different kind of offensive capability for which nations need to adapt. Beyond the battlefield, the impact of this operation is perhaps even more significant. What Spider Web confirms is that the gaps in airspace can be used by an adversary with enough planning and the right technology. They can be exploited not just by states and not just in war. The technology is not rare, and the tactics are not complicated. What Ukraine did was to combine them in a way that existing systems could not see the attack coming. It also shattered the illusion that distance ensures safety. This is now a universal vulnerability and a defining governance challenge of drones in the low-level airspace. This means that airspace is widely accessible. It is also difficult to keep out drones with unpredictable flightpaths. It showed how little the margin for error is in an airspace where cheap systems can be used with precision. As demonstrated, the cost of failure can be strategic.[16]

Lessons for India

The ability to use precise mass capabilities at speed and scale especially when fused with advancing AI for guidance places enormous pressure on defensive measures. The technology, which used to be available only with the armed forces of nations are now highly adaptable by non-state actors. An example that comes to mind is the targeting of commercial shipping in the Red Sea by the Houthis. But what is more concerning is the use of sleeper cells or local support to facilitate use of this technology which now renders even areas in depth as vulnerable. Anyone who can smuggle, hide, and pilot small drones can cause destruction with surprise and creativity. The attacks, both in Russia and Iran, therefore, clearly are a case of failure of intelligence.

Rear areas are now increasingly vulnerable. This will necessitate for hardening of shelters to protect assets from attacks, dispersal of critical assets to avoid putting them all at risk in case of an attack, and countermeasures to defeat such drone attacks. Rear-echelon installations and critical infrastructure must now need to be accorded similar security as frontline positions. Anti-drone measures must be put in place to defend high-value targets. There may also be a need develop new tactics and anti-drone capabilities akin to an AD umbrella used to protect an offensive formation.

This strike also represents a widening cost to kill ratio with cheap drones targeting and damaging expensive aerial assets, heralding a new norm in modern warfare which reemphases the impact of drones and non-contact kinetic attacks. This necessitates a re-examination of inventories with expensive weapon platforms needing to be balanced by many cheaper capabilities.

The former Chief of the Army Staff General Manoj Mukund Naravane has also flagged the lack of accountability in India's growing drone ecosystem. "It must be made mandatory for all such companies to register themselves and provide details of their manufacturing or assembly capacities, with a record of sales and verified end-users. An underground market for drones cannot be allowed to flourish", he said.[17] He recommended that all drones be registered at local police stations, including their technical parameters. "Unauthorised possession or sale of drones needs to be made an offence through suitable legislation, on the lines of the Arms Act. All agencies need to work seamlessly to deal with this emerging threat".[18]

As per Major General BK Sharma (Retd), "Defence innovation must be agile, anticipatory, and synergistic to accelerate procurement cycles. The Defence Research and Development Organisation, the armed forces, and industry partners must be galvanised to develop indigenous capabilities, including drone swarms, autonomous intelligence, surveillance, and ISR systems, Electronic Warfare (EW) systems, AI, anti-drone systems, and smart logistics. Operation Spider Web underscores that national security is no longer solely a function of defence forces but merits a whole-of-nation approach".

Solutions can range from low-cost options such as overhead protection and camouflage to EW and jamming, engagement by AD weapon systems and by looking at developing new methods to track and disable drones on approach.

Conclusion

This will undoubtedly go down as one of the most sophisticated covert operations of the Russo-Ukrainian War so far. Ukraine, though outgunned by Russia, has responded by developing a cheap and sizeable inventory of attack drones. The innovative use of these drones has now been clearly exhibited, showcasing the strategic value of this asset.

Though the consequences of the attacks on Russian military capabilities are difficult to estimate at this stage, their symbolic significance is important for Ukraine, as it has been facing setbacks on the battlefront. Kiev, which has banked on expanding the use of domestically produced drones during the ongoing conflict, has now surprised Russia and the world with this new approach. From critical military infrastructure to civilian sites, the vulnerability to small, precise, and hard-to-detect systems is growing. Conventional AD is often ill-suited for this new threat landscape, prompting an urgent call for innovation in early detection, EW, and layered physical defences. Together, these trends point to a future where technological agility, not just industrial scale, determines strategic advantage.

To quote Major General Sharma, "The operation succeeded not through firepower but through a convergence of innovation, decentralised execution, and rapid decision-making. It was a testament to the weaponisation of software and the integration of civilian technology into the fabric of national defence".[19]

There is no doubt that this attack will go down as one of the finest out-of-the-box ideas of this conflict, executed with amazing ingenuity, rendering the entire AD system sterile and raising huge questions regarding the management of airspace with repercussions far beyond the conflict.

Endnotes

[1] "Lessons from Ukraine", *The Economist*, 03 Jun 2025, accessed on 10 Jun 2025 https://www.economist.com/leaders/2025/06/03/the-west-is-rethinking-how-to-fight-wars

[2] Justin Bronk, "Justin Bronk Comments on the Latest Deep Strikes on Russia", *Rusi.org*, 02 Jun 2025, accessed 11 Jun 2025 https://www.rusi.org/in-the-news/justin-bronk-comments-latest-deep-strikes-russia

[3] Jagatbir Singh, "Russia's Pearl Harbor? Ukraine's Operation Spider Web an Attack of Astonishing Ingenuity", *The New Indian Express*, 05 Jun 2025, accessed 12 Jun 2025 https://www.newindianexpress.com/web-only/2025/Jun/05/russias-pearl-harbor-ukraines-operation-spider-web-an-attack-of-astonishing-ingenuity

[4] "Lessons from Ukraine", *The Economist*, 03 Jun 2025, accessed 10 Jun 2025, https://www.economist.com/leaders/2025/06/03/the-west-is-rethinking-how-to-fight-wars

[5] Anil Chopra, "Lessons Ukraine's Operation Spider Web Has for India", *Firstpost*, 07 Jun 2025, accessed 12 Jun 2025 https://www.firstpost.com/opinion/lessons-ukraines-operation-spider-web-has-for-india-13895164.html

[6] Singh, "Russia's Pearl Harbour?"

[7] V K Singh and Jagatbir Singh, "Spiderweb: An Attack with Far Reaching Implications", *CS Conversations*, 07 Jun 2025, accessed 11 Jun 2025 https://www.csconversations.in/spiderweb-an-attack-with-far-reaching-implications/

[8] Laura Gozzi and BBC Verify, "How Ukraine carried out daring 'Spider Web' attack on Russian bombers", 03 Jun 2025, accessed 13 Jun 2025 https://www.bbc.com/news/articles/cq69qnvj6nlo#:~:text=One%20lorry%20driver%20interviewed%20by,pinned%20down%2C%22%20he%20said

[9] Doug Livermore, "By fusing intelligence and special operations, Israel's strikes on Iran are a lesson in strategic surprise", 14 Jun 2025, accessed 16 Jun 2025 https://www.atlanticcouncil.org/blogs/new-atlanticist/by-fusing-intelligence-and-special-operations-israels-strikes-on-iran-are-a-lesson-in-strategic-surprise/

[10] Kateryna Bondar, "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare", *CSIS*, 02 Jun 2025, accessed 10 Jun 2025 https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

[11] Michael C Horowitz, "Ukraine's Operation Spider's Web Shows Future of Drone Warfare", *Council on Foreign Relations*, 03 Jun 2025, accessed 12 Jun 2025 https://www.cfr.org/expert-brief/ukraines-operation-spiders-web-shows-future-drone-warfare

[12] Singh, "Russia's Pearl Harbour?"

[13] Ukrainian World Congress, "Ukraine Destroys 40 Russian Strategic Bombers in Audacious 'Spider Web' Drone Operation", *Ukrainian World Congress*, 02 Jun 2025, accessed 06 Jun 2025 https://www.ukrainianworldcongress.org/ukraine-destroys-40-russian-strategic-bombers-in-audacious-spider-web-drone-operation/

[14] "A Brilliant Operation Was Carried out on Enemy Territory, Aimed Exclusively at Military Targets–Address by the President", *Official website of the President of Ukraine*, 01 Jun 2025, accessed 07 Jun 2025 https://www.president.gov.ua/en/news/provedena-bliskucha-operaciya-na-teritoriyi-voroga-viklyuchn-98193

[15] The Conversation, "How Ukraine Drone Strikes Deep inside Russia Serve as a Lesson for Other Countries", *Firstpost*, 04 Jun 2025, accessed 10 Jun 2026 https://www.firstpost.com/explainers/how-ukraine-drone-strikes-deep-inside-russia-serves-as-a-lesson-for-other-countries-13894068.html

[16] Singh, "Russia's Pearl Harbour?"

[17] Saurabh Sharma, "'Track All Drone Firms, Declare No-Fly Zones Near...': Former Army Chief Says Entire Country Is Now the Battlefield", *Business Today*, 09 Jun 2025, accessed 15 Jun 2025 https://www.businesstoday.in/india/story/track-all-drone-firms-declare-no-fly-zones-near-former-army-chief-says-entire-country-is-now-the-battlefield-479640-2025-06-09

[18] Ibid.

[19] B.K Sharma, "The Trojan Horse Returns: Lessons from Ukraine's Operation Spiderweb for India's Strategic Security", *The Week*, 09 Jun 2025, accessed 11 Jun 2025 https://www.theweek.in/news/defence/2025/06/09/the-trojan-horse-returns-lessons-from-ukraines-operation-spiderweb-for-indias-strategic-security.amp.html