CENJOWS

ISSUE BRIEF
IB/12/25

OPERATIONS SPIDERWEB: C-UAS LESSONS FOR INDIA

BRIGADIER ANSHUMAN NARANG (RETD)

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Operations Spiderweb: C-UAS Lessons for India

Brigadier Anshuman Narang (Retd) is an alumnus of the prestigious Rastriya Indian Military College. He holds the "Adani Defence Chair of Excellence" on UAS Warfare with special focus on Counter UAS at CENJOWS

Abstract

Two major operations within 25 days of each other- SINDOOR on Indian sub-continent and SPIDERWEB in Eurasian battlespace highlighted one same lesson that low-cost drones' threat is omnipresent today regardless of the depth, distance or nature of target. Counter-Unmanned Aerial Systems (C-UAS) grid is thus no more a display of niche technology but an absolute essential for any critical asset whether military, government or civilian / private. The C-UAS threat has magnified many times with the introduction of the easy to assemble First Person View (FPV) drones sometime in 2023 during the ongoing Russia-Ukraine war. The proponents of these literally home-made loitering munitions called FPV drones have been repeating one lesson since 2023 that "Big Isn't Beautiful Anymore". However, most militaries world over neither read nor were prepared to accept the complexity of this new threat. While the strategic Russian airbases were well prepared against larger aerial threat, all existing countermeasures were innovatively evaded by the Ukrainian low-cost small drones to strike the strategic bomber fleet which had been causing thousands of Ukrainian casualties for the last three years plus. This issue brief will thus examine the plan and execution of the most asymmetric and sophisticated technology enabled FPV drones-based precision strike cum raid titled "Operation Spiderweb" in detail to identify lessons learnt in general and draw out the implications for C-UAS grid in India. The detailed analysis of the Operation Spiderweb in this issue brief has been assisted by a C-UAS expert, Mr Pawan Kakkar, CEO and founder Jugapro and Geospatial Intelligence (GEOINT) team at Suhora Technologies.

Abstract

Two major operations within 25 days of each other- SINDOOR on Indian sub-continent and SPIDERWEB in Eurasian battlespace highlighted one same lesson that low-cost drones' threat is omnipresent today regardless of the depth, distance or nature of target. Counter-Unmanned Aerial Systems (C-UAS) grid is thus no more a display of niche technology but an absolute essential for any critical asset whether military, government or civilian / private. The C-UAS threat has magnified many times with the introduction of the easy to assemble First Person View (FPV) drones sometime in 2023 during the ongoing Russia-Ukraine war. The proponents of these literally home-made loitering munitions called FPV drones have been repeating one lesson since 2023 that "Big Isn't Beautiful Anymore". However, most militaries world over neither read nor were prepared to accept the complexity of this new threat. While the strategic Russian airbases were well prepared against larger aerial threat, all existing countermeasures were innovatively evaded by the Ukrainian low-cost small drones to strike the strategic bomber fleet which had been causing thousands of Ukrainian casualties for the last three years plus. This issue brief will thus examine the plan and execution of the most asymmetric and sophisticated technology enabled FPV drones-based precision strike cum raid titled "Operation Spiderweb" in detail to identify lessons learnt in general and draw out the implications for C-UAS grid in India. The detailed analysis of the Operation Spiderweb in this issue brief has been assisted by a C-UAS expert, Mr Pawan Kakkar, CEO and founder Jugapro and Geospatial Intelligence (GEOINT) team at Suhora Technologies.

Key Words

Counter-UAS (C-UAS), FPV Drones, Operation Spiderweb, Russia, Ukraine, Bomber aircrafts, Ukrainian Security Service's (SBU); Artificial Intelligence (AI); Manned-Unmanned Teaming (MUMT)

Introduction

"**Except for Ukrainians, Russians, and maybe the Chinese, not many people realize that it's happening right now**. And what people do realize, but people are not acting on it, not preparing for it by a lot of the equipment we have, a lot of the equipment we're investing in—is no longer useful—if we don't have the drones. This is what will be the big focus of the future. It's already part of any warfare. It's part of the present."

-Ukrainian perspective[1]

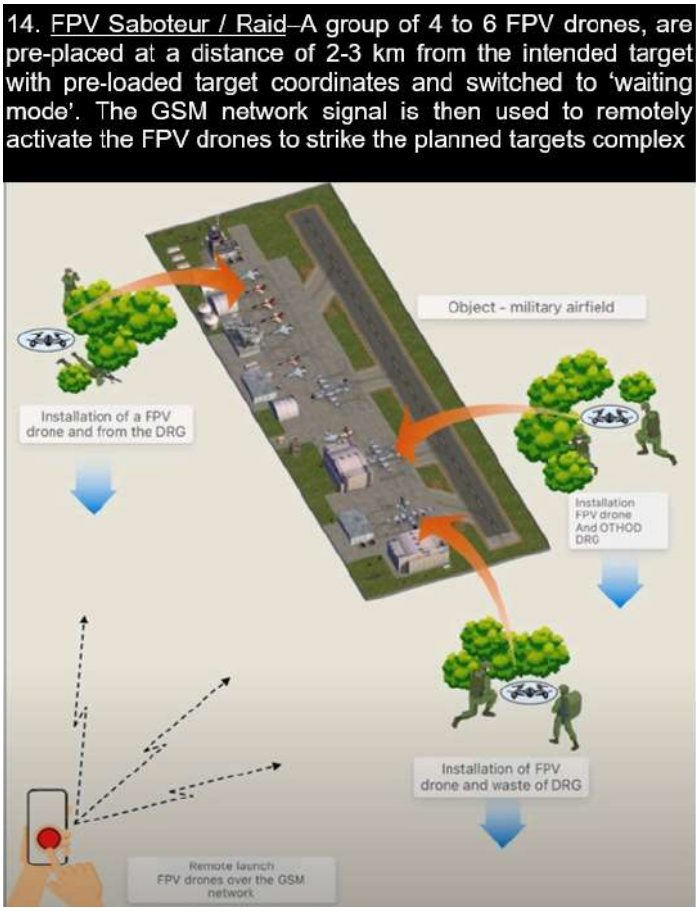
Indian Operation SINDOOR (punitive response to Pakistan's cowardly terrorist strike at Pahalgam on 22 April 2025) and Pakistan's retaliatory actions over four days from 07 to 10 May 2025 witnessed the extensive use of variety of drones and loitering munitions except the FPV drones. However, the Russia-Ukraine war has witnessed fast paced technological development of small drones particularly Artificial Intelligence (AI) enabled and Optical Fibre Cable (OFC) connected FPV drones. The precise execution of Ukrainian Security Service's (SBU) Operation Spiderweb involved the targeting of Russian Bombers fleet by truck-mounted AI-enabled FPV drones at the strategic depth of more than 4000 km away from Russo-Ukraine border. The timing of this operation was coincidentally unique as it came 24 hours after the largest Russian drones' strike on Ukraine but exactly 24 hours before the negotiations due at Istanbul, Türkiye on 02 June 2025. SBU successfully hit two bases where the bombers returned from their strikes on 26 and 31 May 2025.

In military, the operational planning basics taught to any young military officer are "Simultaneity, Non-linearity and Audacity". Operation "Spiderweb" displayed all three critical combat basics. The unprecedented asymmetricity of these strikes was an attempt to cover the vast expanse of Russian regions spanning three time zones and simultaneously strike five military airbases accounting for approximately 41 out of 127 bombers with Russian Air Force which is nearly 32%. Despite the open-source geospatial intelligence (GEOINT) analysis indicating only about 14 aircrafts damaged / destroyed at maximum, the drones clearly bypassed the Russian electronic warfare (EW) and traditional air defence (AD) countermeasures of its strategic airbases. The Ukrainian technological prowess was on display through a uniquely fused Manned-Unmanned Teaming (MUMT) by leveraging stealthy and deceptive deployment of FPV drones, autonomous cellular and inertial navigation, long-range internet-based

communication, and AI-enabled targeting[2]. The Russian FPV manual, issued in end 2024, described sabotage airport raid as one of the missions of Ukrainian FPV drones as shown in Figure 1 below and was covered in detail in the December 2024 Issue Brief by the author[3]. The Ukrainians executed the 14th anticipated task "FPV Saboteur / Raid" copybook style using the Russian mobile network. The numbers were multiplied minimum 25 times to strike at the maximum possible strategic depth while simultaneously hitting multiple airbases in a non-linear fashion. Russians should not be surprised as they had seemingly forgotten their own manual. The Russians had even covered the aircrafts with old tires which surely indicated that Russians had some evasive measures in place for such an attack.

Figure 1: Roles for FPV Drones from FPV Employment Manual Circulating on Russian Telegram Channels with Translation Available on LinkedIn

*(*Translated Diagrams by Curtis and Author's Issue Brief[4]*)*

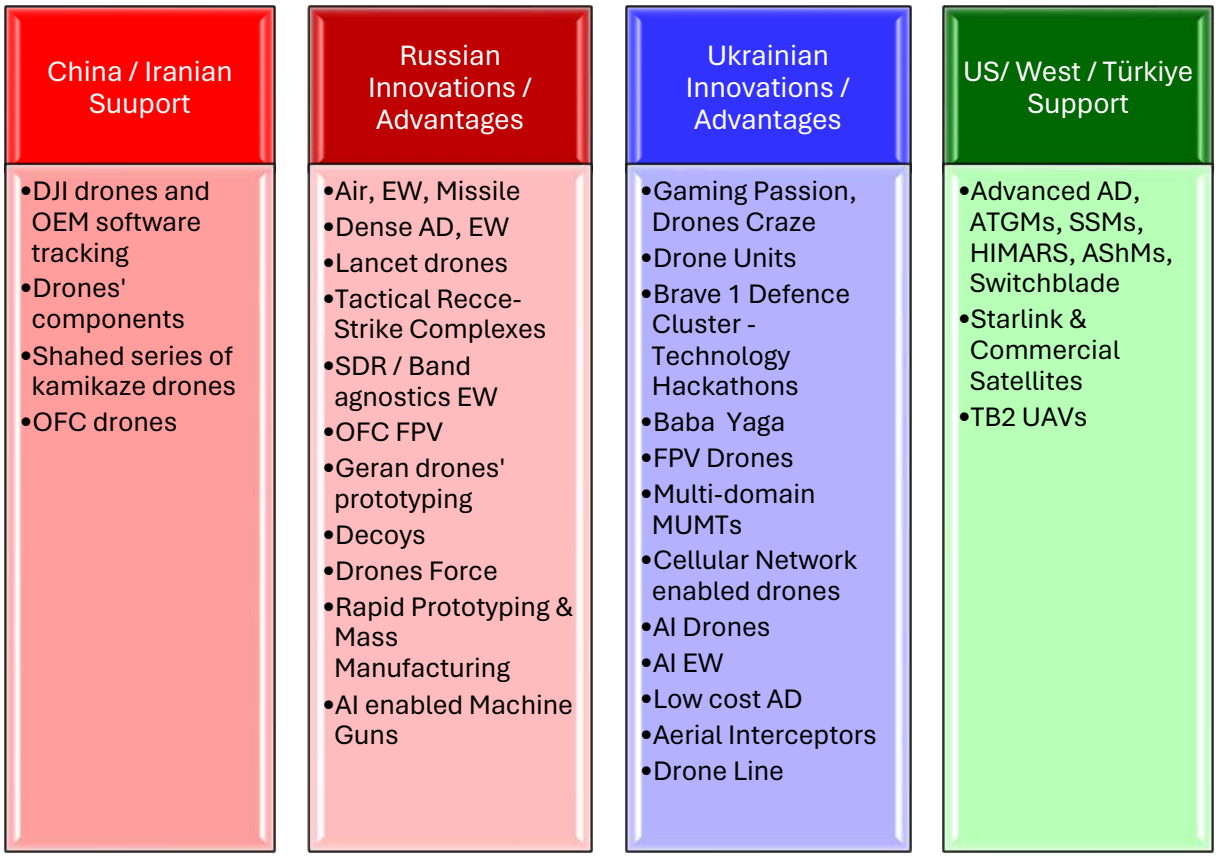


The Azerbaijan-Armenia war is considered the first dual-side drones' confrontation war and saw the evolution of drones' employment. However, the ongoing Russia-Ukraine war has shown a paradigm shift in the rapid pace evolution of drones' technologies

and platforms with or without external support, related organisational and doctrinal reforms as elucidated in the infographic below.

Figure 2: Evolution of Drones Platforms – Russo-Ukraine War

(Source-Author's Research)



Operation Spiderweb

In the age of propaganda and fake photographs and videos dominating internet and social media, it is very important to declutter validated information. This issue brief will apply common military knowledge, with GEOINT and OSINT to place together maximum possible confirmed information. The succeeding paragraphs will attempt to place the conduct and preparation sequentially and logically.

Plan. The SBU plan was to hit five Russian military airbases, across three time-zones from Finnish border to Siberia. The plan was conceptualised nearly 18 months earlier by SBU Chief Lieutenant General Vasyl Maliuk and his team and approved personally

by Ukraine's President Mr Volodymyr Zelenskyy, as per his X-post on 02 June 2025 at 2:19 am. The Ukrainian SBU planning office was supposedly located on Russian territory near the one of the Russian Federal Security Service (FSB) headquarters.[5]

Map 1: Targets of Ukraine's Operation Spiderweb

(Courtesy- Steven Simoni[6])

Aim. The possible singular aim was to target maximum Russian Tu22M3 and Tu-95MS aircrafts located at five military airbases as depicted in Map above- Belaya/ Irkutsk Oblast, Olenya/ Murmansk Oblast on the Arctic Kola Peninsula, Dyagilevo / Ryazan Oblast, Ivanovo and Ukrainka / Seryshevo Oblast. These bombers regularly launched Kh-101 cruise missiles on static Ukrainian targets. Keeping the high-cost factor of these Tu22M3 and Tu-95MS coupled with their irreplaceability and anticipated long repair time, Ukrainian military appreciated the damaged bombers to be out of the war for ever. Ukraine had surely monitored that six Tu-95MS bombers had returned to Belaya from Olenya airbase after participating in the largest ever drones strike by Russia on Ukraine on 31 May 2025. Additionally, few bombers had returned to Olenya after strikes on Ukraine on 26 May 2025.[7]

Russian Bomber Fleet. In view of the clear aim to target Russian bombers, it is important to assess the Russian Federation Aerospace Forces (RF VKS) bomber fleet before evaluating the execution methodology and results achieved. VKS's Long-

Range Aviation (DA) operates the bomber fleet. Repeated Ukrainian strike attempts at Engels Base had earlier forced VKS to shift its bomber fleet rearwards. [8] As per Military Balance 2025[9], Scramble website[10] and few social media accounts like AviVector on X[11], and Tom Cooper with account name Sarcastosaurus on substack[12], the Russian bomber fleet comprised maximum 127 bombers as tabulated-

Table 1: Russian Military Bomber Fleet

(Source- Military Balance 2025, Scramble website, AviVector, Tom Cooper)

Aircraft	Units	Numbers	Known Locations and Entities
Tu22M3	3 Regiments	56 (~ 27 fully mission capable in 2023)	**Belaya / Irkutsk** and Tiksi – 200th Guards Heavy Bomber Regiment / 326th Heavy Bomber Division; Olenegorsk / Vysokiy – 40th Composite Aviation Regiment / 22nd Guards Heavy Bomber Division; Shaykovka- 52nd Guards Heavy Bomber Regiment/ 22nd Guards Heavy Bomber Division; Ryazan / Dyagilevo- 43rd Guards Oryol Centre; Soltsy - 840th Heavy Bomber Aviation Regiment; Many Tu22M3s were repositioned to Shaykovka (7 aircrafts) while the donor Tu22M3s at **Olenya** airbase, as per AviVector, weren't actively used aircrafts[13]
Tu-95MS	3 Squadrons / Regiments	58	**Ukrainka/ Seryshevo**- 182nd Guards Heavy Bomber Regiment / 326th Heavy Bomber Division; Engels-2 – 121st Guards Heavy Bomber Regiment / 22nd Guards Heavy Bomber Division; **Ryazan / Dyagilevo**- 43rd Guards Oryol Centre; Engels-2 - 184th Guards Heavy Bomber Aviation Regiment
Tu-160	1 Squadron	13-16	Belaya, Engels-2 - – 121st Guards Heavy Bomber Regiment / 22nd Guards Heavy Bomber Division with 16 aircrafts

- **Tupolev Tu-95MS**. A four-engine turboprop plane with intercontinental range, it can carry 8 long-range cruise missiles which may be equipped with either conventional or nuclear warheads. As per various estimates, Russian military had nearly 55-60 Tu-95 bomber aircrafts.[14] As per Tom Cooper, Tu-95 bombers fleet has been maintained in mediocre condition with most of their airframes more than 30 years old. Post extensive employment in Syria, they have been the primary platform for Kh-101 and Kh-555 cruise missiles against Ukraine since 2022.[15]
- **Tupolev Tu-22M3**. A twin-engine supersonic bomber with lesser combat range than Tu-95, the latest version Tu-22M3 carries Kh-22 supersonic cruise missiles.

Russian military held anywhere between 50 to 60 Tu-22M3 as per estimates. [16] Due to absence of air refuelling capability, these are not considered as strategic bombers. As per Tom Cooper, these aircrafts have frequently caused massive Ukrainian civilian casualties due to low precision of Kh-32 supersonic air-to-ground missiles. Ukrainian intelligence estimated maximum 27 fully mission capable Tu-22M3s as of 2023. [17]

- The production of both these aircrafts was stopped in 1991 post collapse of the Soviet Union.

- **Tu-160**. 15 of these aircrafts, manufactured before 1992 were overhauled and upgraded in 2002-2006, as per Tom Cooper, to deploy Kh-555, Kh-101 and Kh-102 cruise missiles (maximum 12 in internal bomb bays). The 16th aircraft was assembled between 2014-2018. Most of these aircrafts have suffered lingering engine-related problems and lack of spares. The Tu160 bombers have been employed in Syria. Tom Cooper assesses that minimum 2 Tu160s have been kept on alert, while being armed with 'nuclear-tipped' cruise missiles. [18]

- **Belaya Airbase**. On 31 May 2025, the airbase had 7 Tu-160, 6 Tu-95MS, 2 Il-78M (Midas), 6 An-26, 2 An-12, 39 Tu-22M3 and 30 MiG-31. AviVector, in the X-post on 01 June 2025[19] at 2:23 AM, highlights: -

> "*Since the latest satellite imagery, 10 Tu-22M3s were repositioned from the upper-left to the central-right parking area. One more was likely training or relocated.* ***Six Tu-95MS bombers are once again present at the airfield, having arrived from Olenya Air Base after participating in the latest attack on Ukraine****. The presence of MiG-31 interceptors has grown from 25 to 30*.

Figure 3: Belaya Airbase 52.910283,103.570819

(Source-Google Earth – 24 April 2025)

Figure 4: Belaya Airbase on 31 May 2025

(Source-AviVector[20])

- **Olenya Airbase**. The airbase had most probably 1 Tu-160, 1 Il-76, 3 An-12 and 28 Tu-22M3 aircrafts on 03 June 2025. On 26 May 2025, it had 11 Tu-95MS, 5 An-12 and 40 Tu-22M3. Bombers from this base had participated in the Russian VBS strike on Ukraine on 26 May 2025. [21]
- **Dyagilevo Airbase**. The airbase had 3 Tu-95MS, 5 Tu-22M3, 14 Il-78M or Il-76MD and 2 Su-30SM.[22]

Figure 5: Dyagilevo Airbase on 02 June 2025

(Source-AviVector[23])

- **Engels-2 Airbase**. It had 2 Tu-95MS, 2 Tu-160 and 1 Il-76 as on 28 May 2025.

Execution. The operation involved sophisticated employment of 117 drones with as many controllers. The SBU personnel operated across numerous Russian Oblasts to

deploy the FPV drones. They were withdrawn to Ukraine before the commencement of the operation.[24] The methodology of execution is described in detail below as per inputs from various telegram posts and other social media sites[25]:

- **Drones' Stack**. As per the appreciation of Mr Pawan Kakkar, CEO Jugapro and a top-notch C-UAS expert, the FPV drone stack comprised STM32-based Flight Controllers (e.g., MatekF411); AI Module: Jetson Nano / RK3588; Camera: Caddx / Runcam / stripped GoPro; Control Link: ExpressLRS / Crossfire for nearby FPV operators and Power: 4S LiPo (1300–1800mAh), XT60 interface.
- **Drones' Spiderweb**. The launch rack most likely carried up to 36DJI Inspire 2-class quadcopters as shown in Figure 6. These quadcopters weigh 3.4 kg empty, can reach 94 km/h with 25 minutes endurance. Modified as FPV drones and carrying 1 kg warheads, each drone had the capability to fly 5–10 km from its covert mobile pad and strike any target with meter-level accuracy.[26] These drones' webs were hidden inside the wooden sheds' roofs which were later opened at opportune moment at the outer edge of Russian airbases to swarm the military bomber aircrafts parked in the open. [27]

Figure 6: Spiderweb Launch Rack

(Source- Mike Casey[28])

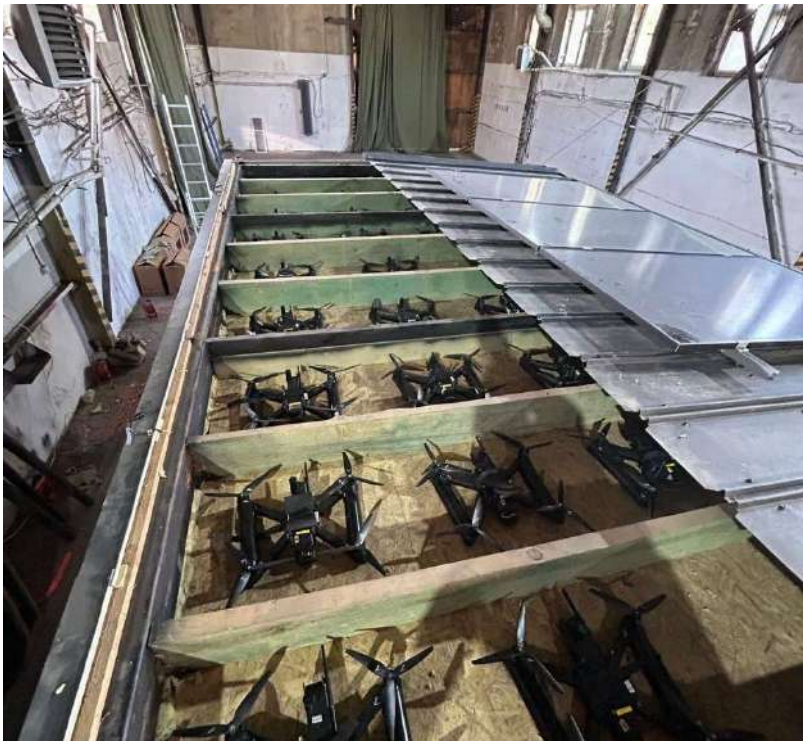
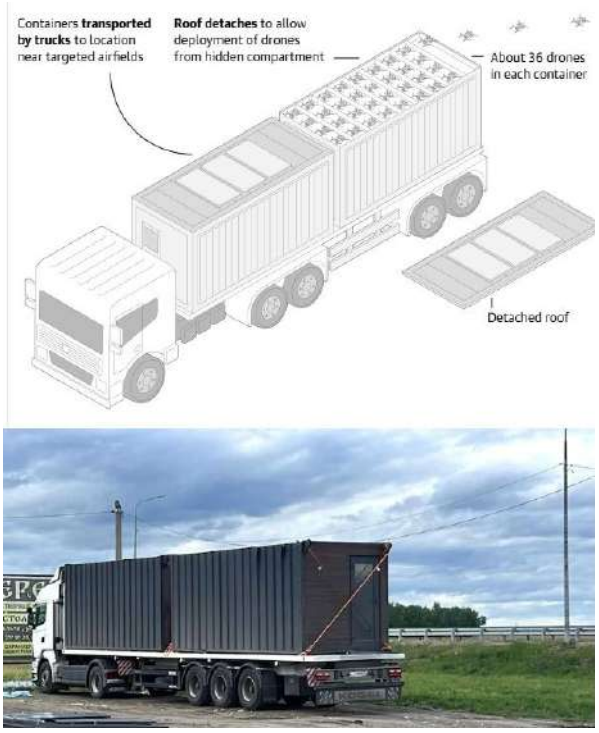


Figure 7: Truck Based Wooden Container

(Source- Riccardo Romani- C[29])



- **Placement in Russia**. The FPV drones were first smuggled deep in Russian territory in decoy mobile wooden structures. The drones were concealed under the roofs of various makeshift buildings in Chelyabinsk where they were mounted on cargo trucks. They were then driven by local Russian drivers to various different airbases. The truck drivers were most likely not aware of the consignment loads and only knew that they were carrying modular houses.
- **Proximity Positioning**. FPVs were launched from these trucks at the most opportune moment when they reached near the airbases. Without any ground control stations, these FPV drones were directly controlled by ARDUPILOT software through Russian 4G / Long Term Evolution (LTE) mobile network infrastructure with sufficient bandwidth to control them. This replicated the “Baba Yagas” drones launch model but with the Starlink communication terminal being replaced by an LTE modem with an ethernet modem.
- **Trigger Architecture**. As per Mr Kakkar, this included activation initiation via Real Time Clock (RTC triggers), optical sensors, or light-activated switch modules. The SIM card initialized LTE session to facilitate IP resolution and thereafter establishing MAVLink handshake and Autopilot Advanced RISC Machine (ARM) and ignition. As a backup option, manual piloting via LTE FPV relay or AI-guided visual classification and terminal homing was also ensured.

- **Guidance and Targeting**. AI-driven onboard inference was achieved using YOLOv5s/tiny. Target detection was done through visual classification of aircraft silhouettes. The kill command was executed via GPIO/MOSFET detonation or throttle threshold logic. The ARDUPILOT software used Universal Asynchronous Receiver / Transmitter (UART) channel to receive images from webcam and pass command instructions for controlling the drone through internet. Both Russians and Ukraine drone units have been regularly using internet for such tasks.
- **Shaped Charges**. The munition had redundant trigger mechanisms to ensure that the shaped warhead shall detonate in case of slow speed impact.
- **Self-Destruct Mechanism**. All the drones' trucks had a self-destruct mechanism thereby obviating any opportunity of intact capture by the Russians.

Russian Countermeasures. Mr Pawan Kakkar's assessment divides Russian countermeasures into AD and EW Systems.

- **AD Systems**. It probably included Pantsir-S1 which may have been overwhelmed by swarm saturation while its radar performance may have been ineffective against low RCS drones; S-350 Vityaz which would not have been triggered as it is designed for high-altitude threats; the Hand Held cUAS Systems were most probably bypassed by altitude and launch proximity; Anti-drone buggies most likely failed to respond in time.
- **EW Systems**. It spanned Pole-21 which was most probably ineffective due to RF silence; R-330Zh Zhitel which also obviously couldn't jam non-emitting drones; and finally, Krasukha-4 was not triggered since there were no uplink/SATCOM emissions. It is also very likely that SIM-IMEI randomness was ensured via MIC spoofing.

Results. Mr Zelensky claimed that "34% of the strategic cruise missile carriers stationed at air bases were hit". [30] While many Ukrainian social media handles, quoting SBU sources, have claimed up to successful strikes on five bomber bases as far east as Irkutsk and destroying or damaging 41 Russian aircrafts of the bomber variety comprising Tu-95, Tu-22M, and A-50 aircrafts. [31] SAR and electrooptical satellite images from all commercial space firms confirm that Olenya and Belaya airbases were very successfully struck. FPV strikes on these two airbases caused severe damage and destruction of nearly 14 bomber aircrafts which is 11% of VKS bomber fleet. The mostly validated and confirmed damage / destruction achieved is tabulated below:

Table 2: Evaluation of Damage / Destruction of Russian Bomber Fleet

(Source- Team Suhora's Detailed IMINT Analysis and Author's research from Multitude Sources and Satellite Imageries)

Base / Oblast	Destroyed	Damaged	Remarks
Olenya / Murmansk	4 Tu-95, 1 An-12	1 Tu-95	ICEYE (ex Suhora Technologies) and Umbra's 50 cm resolution SAR (5 looks) image; Ukrainian social media posts claimed 4 Tu-95MS destroyed, 5 Tu-22M3 & 5 AN-12 damaged at Olenya; 7 Tu-95MS & 7 Tu-22M3 damaged / destroyed at Belaya
Belaya / Irkustsk	3 Tu-95, 4-Tu22M3	1 Tu-95	
Ukrainka / Seryshevo	Trucks most probably prematurely detonated as the local alerts were reported. In case of Ivanovo, Russian Ministry of Defence claimed that attack was repelled. Ukrainian claims remain unconfirmed.		Claims of 1 Tu-95 damaged / destroyed
Ivanovo / Severnyy			Claims of 1 A-50 AEW destroyed & another 1 damaged.
Dyagilevo / Ryazan	No serious damage except traces of fire on right part of airfield.		
Total Aircraft Hit	14 aircraft damaged / destroyed – 9 Tu95MS; 4 Tu22M3; and 1 An-12		

Figure 8: Planet Image of Destroyed Tu-95 on Olenya Airbase

(Source- Marjin Markus[32])

Figure 9: Airbus Image of Destroyed Tu-95 on Olenya Airbase

(Source- Marjin Markus[33])

Figure 10: ICYEYE's SAR Images of Olenya Airbase ex Suhora Technologies

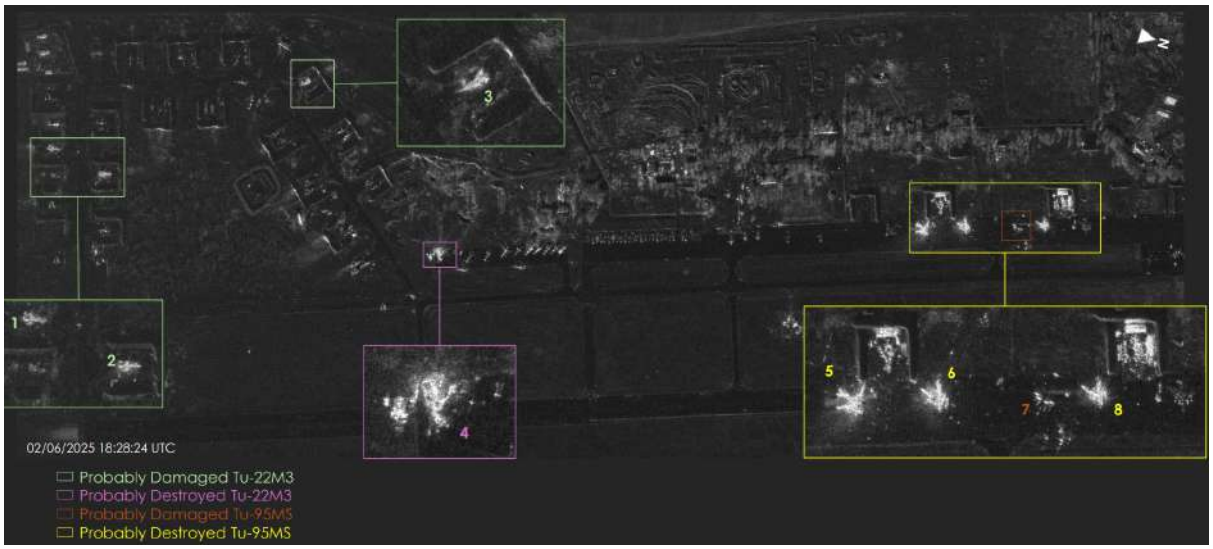
(Source- Suhora Technologies)

Figure 11: Planet Images of Strikes on Belaya Airbase

(Source- Marjin Markus[34])

Figure 12: ICYEYE's SAR Images of Strikes on Belaya Airbase

(Source- Suhora Technologies)



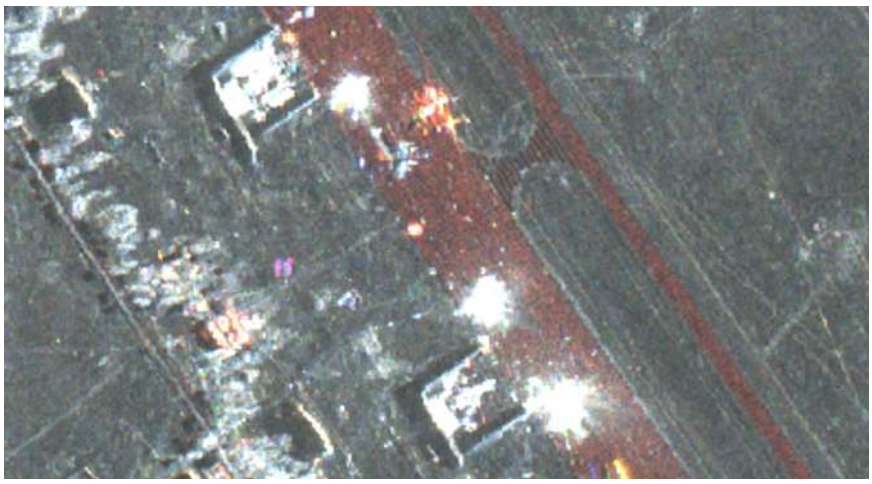


Figure 13: Umbra's SAR Image dated 01 June 2025

(Source- Umbra, X-post by Chris Biggers and Ukraine Battle Map @ukraine_map[35])

Figure 14: Burned Area at Dgagilevo Airbase, Ryazan Oblast

(Source: Emil Kastehelmi@emilkastehelmi[36])

Strikes' Success. With only about 27 fully mission capable Tu-22M3 bombers to Russian VBS, strike on 4 most likely operational types is nearly 15% destruction wherein cannibalisation will surely be a challenge keeping the spare parts' state in mind. While the Tu-160 fleet did not face any damage, damage / destruction caused to 9 Tu95MS out of maximum available 50-60 aircrafts in mediocre condition is significantly high. Thus, it's safe to assume that Russia will face severe problems in cannibalisation of parts now and it will take significant time for the bomber fleet to fully recoup.

Technology. The key technologies employed most probably to overcome various Russian C-UAS measures are listed below[37]: -

- **AI-Enablement**. The AI auto-homing model for the FPVs was trained to identify the most vulnerable spot on the bombers in case operators' control over drone through 4G was lost. In case of Olenya airbase, targeting of fuel tanks resulted in extensive fires.
- Russian 4G SIM-enabled microcontrollers for interface with flight control systems. This enabled transmission of MAVLink protocol via TCP/IP over cellular networks. Apropos, the communication modules were configured for temporal minimalism (<30s activation windows).

- **AltHold Mode**. This mode facilitated altitude maintenance through barometer and accelerometer.
- **ARDUPILOT**. The flight controllers ran the ARDUPILOT firmware. It was optimally employed for controlling FPV drones through internet medium thereby requiring flight stabilisation and maximum flight control autonomy, particularly when communication delays are likely between the drone and the operator.
- **Inertial Navigation System (INS)**. INS was most probably used to overcome Global Navigation Satellite System (GNSS) dependencies.
- **Command and Control (C2)**. As per Mr Kakkar, telecom-driven C2 chain was ensured by

  "*command-and-control (C2) continuity was possibly maintained via MAVLink over LTE channels—a tactic invisible to legacy RF-dependent defence mechanisms*…utilized civilian 4G/5G infrastructure with network-resident authentication evasion…possibly might have used burner SIMs or even cloned IMEIs…Data telemetry might have been cloaked to emulate common smartphone usage profiles, evading heuristic filters if any."
- **Miscellaneous** High Quality Video Stream, RTC (Real-Time Clock) triggers, GSM-triggered pulse (SIM800L modules), Infrared or low-power RF bursts and Photodiode-based sunset triggers.

Analysis

Although the operation aimed to target 41 Russian bomber aircrafts, it could adversely impact 14 aircrafts which by itself is a big success. The innovativeness of strike execution was in organising logistics deep inside Russian territory which in turn got facilitated by low effectiveness of Russian security in the areas where they were not expecting any such targeting. The plausible reasons for success are: -

- **Precise Target Selection**. Selected air bases operated the main bomber aircrafts responsible for maximum damage on Ukrainian civil targets. Real time GEOINT of the targets was maintained through commercial satellite images.
- **Strike Timing and Precise Intelligence**. SBU had the precise intelligence to target the airbases when they had large number of strategic bomber aircrafts in the open. Coincidentally, the asymmetrical strike took place exactly one

day after the single heaviest Russian strike on Ukraine comprising 472 drones and 8 missiles. It was also exactly one day before the US mediated Russia-Ukraine negotiations at Istanbul.[38]

- **Tactical and Technological Innovations**. Ukraine's tactical innovations managed to evade most Russian surveillance options and counter measures. While concealed sheds for drone stacks inside logistics trucks facilitated deep infiltration in Russia, complete RF silence, before launch, facilitated evasion of all Russian SIGINT platforms. AI-enabled guidance provided autonomy while swarm saturation was ensured by multi-wave multi-time-zone drone launches. GNSS independence was ensured via onboard Inertial Measurement Units and barometric correction algorithms. Any possible FPV drones video uplink was suppressed until the FPV drones were airborne. The payload video bandwidth was minimized sufficiently to evade Deep Packet Inspection (DPI) and EW filtering [39]

Image Forensics. Image Forensics, undertaken by Mr Kakkar, indicated the following[40]

- Hardware most probably included STM32-based flight controllers; Jetson Nano AI boards; BLHeli_32 4-in-1 Electronic Speed Controllers; XT60 power connectors; Heatshield foam and conformal coating with organized and industrial-grade wiring.
- Blast analysis showed Tu-95s having burn patterns near wings and engines. The flash-burn circles indicated possibility of LiPo or directed charge detonation.

Impact on Russia. The operation has surely impacted Russia adversely but would have also strengthened the resolve of Russian populace to defeat Ukraine in the ongoing war. The key issues which merit attention are: -

- **Drones' Floods**. Ukraine's attempts to flood the length and breadth of Russia with low-cost drones is now finally 'Revolution in Military Affairs' impacting the psyche of complete national populace, way of functioning by requiring to protect every single critical asset in routine peacetime drill and most importantly the helpless feeling of a small drone flying in from anywhere.
- **Security Paranoia**. The Russian security agencies and locals will now suspect anyone and greater distrust amongst the locals will be a major fallout. The enhanced implementation of security measures will undoubtedly cause inconvenience to the local populace already impacted by the war.

- **Reduction in Bombers Fleet**. Disruption of approximately 10% strategic bomber fleet is significant. The non-availability of spare parts and replacement bombers will undoubtedly adversely impact the long-range strikes on Ukraine or overall Russian VKS deterrence.

- **Olenya Airbase**. Russian VKS relocated 11 Tu-22M3 bombers to Ukrainka airbase on 02 June 2025.

Figure 15: Olenya Airbase on 03 June 2025

(Source-AviVector[41])

- **Enegels-2 Airbase**. The airbase, although not targeted on 01 June 2025, had 2 Tu-95MS, 2 Tu-160, 1 An-12 and 1 An-148 on 03 June 2025. 2 Tu-95MS bombers were relocated to the Ukrainka airbase on 01 June 2025, post Ukrainian strike. This base otherwise has been subject to regular Ukrainian strike attempts.

Figure 16: Engels-2 Airbase on 03 June 2025

(Source-AviVector[42])

Impact on Ukraine. The numbers of aircrafts would not be of that much significance to the Ukrainian populace. The capability to strike 4000 km deep inside Russian territory and impact the Russian populace across the length and depth of the invading nation itself is a major morale booster for Ukrainian military and population at large. SBU has asymmetrically implemented a well-planned, coordinated and precise sabotage strike on minimum two Russian strategic air bases causing significant irreplaceable damages. Russians will respond more violently but as Mr Zelensky points out that they are already being hit every day. The violence scale of Russian retaliatory response may even be beyond imagination but Ukraine has managed to show that it has many cards up its sleeves. Ukrainian ambassador to the United States Oksana Markarova, summed up the attack[43] as a

> "*very successful defensive operation in Russia against Russian aircraft that, on a daily basis, bomb our hospitals and schools and kill our kids… the best example of how innovation can and should work in defence*."

Ukraine has undoubtedly displayed continued strategic resolve both within the political and senior military leadership to stand up against the mighty Russians despite all the odds. The success of this strike was undoubtedly the product of the dogged determination to strategically surprise the Russians at their maximum depth despite knowing very well that Russia will hit back harder.

The nuclear capable Tu-160 bombers, intentionally or unintentionally, were not targeted. Hence, from an unbiased perspective, Ukraine military had the rights to target the very bomber fleet which was causing immense civilian casualties as recent as 26 and 31 May 2025. With Tu160 bombers escaping any damage during the sabotage strikes, nuclear escalation should be out of the response matrix. However, this operation has surely disrupted the conventional strategic deterrence of Russian VKS bomber fleet.

Key Lessons

While the next section shall focus on C-UAS lessons, there are many other key lessons for India which must be kept in mind.

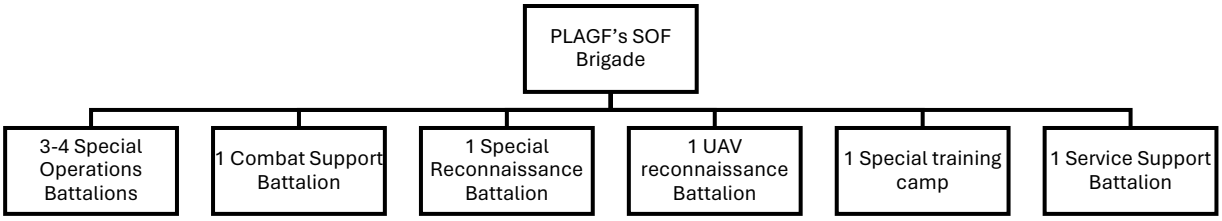
Depth of Special Forces' Operations – Manned Unmanned Teaming. The depth achieved by SBU would be the most achieved by any special operations force (SOF) historically during war. By ensuring the SBU operatives crossed back into their own territory, this is the ideal example of **strategic Manned-Unmanned Teaming (MUMT) at the largest possible distance optimally exploiting communication technology**. It would usher in a new era of MUMT. With similar demographic profiles amongst adversaries, such an operation may get replicated in India-Pakistan scenario. **A multi-domain team of robots and drones may just be the next strike.** It could simply be achieved through dropping of robots at strategic depth by Mother drone with robots themselves being capable of launching loitering munitions with the man appearing only on the loop to confirm the timing and exact target.

Long-Range Sabotage. PLA, in its official pamphlets like Science of Military Strategy 2020, plans sabotage missions for its SOF. In a Taiwan scenario, such long distance MUMT operations do open the floodgates for PLA's planning for sabotage operations in conjunction with amphibious operations for its Taiwan contingency.

SOF and Drones. Ukrainian SBU has revolutionised the paradigm of integrated application of drones, AI and SOF to evade the complete Russian security apparatus in wartime. However, PLA already has a UAV battalion and a special recce battalion in every PLAGF SOF Brigade as illustrated at Figure below. Every PLAGF Corps / Group Army has one SOF Brigade equalling 15 SOF brigades including Tibet and Xinjiang Military Districts. Additionally, PLA has SOF brigades within its Air Force Airborne Corps, Rocket Force and Navy's Marine Corps. PAPF has its own SOF detachments particularly Xinjiang PAP Corps. Hence, SOF's employment of advanced technologies at strategic depth will become the new normal in conduct of sabotage raids by SOF troops.

Figure 18: Author's Appreciation of Composition of PLAGF SOF Brigade

(Source- Author's research)



Precision. Precise delivery of less lethal payload at the most vulnerable spot of the target can give disproportionate results as shown in Figure 17. Low-cost drones struck at the most vulnerable point of adversary's strategic and expensive platforms thereby delivering out of proportion benefits.

Low-Cost Miniaturisation. Russo-Ukraine war has repeatedly proven that "Big isn't beautiful anymore". There is a gradual transformation towards miniaturisation of combat platforms and systems across all domains particularly drones and space. Since low-cost targeting requires imagination to be freed from bureaucratic hurdles, there is an inescapable need to flatten organisations and cultivate Innovators. The Maxar satellite image below aptly elucidates as to how sub-tactical low-cost FPV drones can simply destroy much-larger and expensive strategic bombers with asymmetric technological advancements and out-of-the-box innovative combat application.

Figure 17: Ashes of Three Tu-95 Bombers at Olenya Airbase

(Source- Damien Symon[44])

Ingenuity. Human imagination and innovation have no caste, creed, or nationality. Battlespace innovative solutions are the real cards in the modern combat battlefield. Near real time GEOINT with innovative AI enabled Drones have no boundaries and no limitations to strategic depth. Innovative low-cost solutions can asymmetrically obviate the requirement of many times expensive longer range standoff weapons and platforms. The most apt quote is “Become Innovators, Not Buyers”.

Talent. Niche technologies require cultivation of domain specialists. Technical breakthroughs on modern battlefield are as relevant as bravery and courage of the boots on grounds. Hence, Team BHARAT must ensure that such innovative technological talent is identified, harnessed and trusted to create miracles.

Indigenisation. The provision of quality SAR images by both UMBRA and ICEYE on one hand proved the success of Ukrainian strikes on two Russian airbases while simultaneously lowered their claim from 41 aircrafts to nearly 14. When we compare the scenario with Operation SINDOOR and delayed provision of images to substantiate the immensely high precision achieved by Indian military, it becomes amply evident that "Indigenous AI-enabled real time Satellite IMINT / GEOINT should be PRIORITY 1 focus for Indian Military". Anyways, indigenous commercialisation of drones and space domain is extremely important for any country in the modern battlefield particularly India.

Indigenous real time satellite imaging, spanning hyper spectral, Radio Frequency (RF), Synthetic Aperture Radar (SAR) / Ground Moving Target Indicator (GMTI), Electro-optical (EO), Automatic Identification System (AIS), Infrared (IR) is a must. China has already initiated steps to transform from “Image in Space, Analyse on Ground” to “Image in Space, Analyse in Space”. Availability of such indigenous capabilities during Operation SINDOOR would have ensured that ADG PI released successful strike SAR images within two hours of strikes and high-resolution EO images latest by 0800 hr on 07 May or 10 May. Pakistan's ISPR would have had minimal opportunity to deny the strikes’ success. Despite the attempts of Pakistan’s bots’ army or Chinese 50 cent-army to amplify disinformation / propaganda through fake videos. Exploiting Indian internet mass as media, Indian military would have

positively filled the information vacuum in the minds of millions of Indians and security analysts' world over before our adversaries occupied that space.

Escalation Amidst Negotiations. The largest drones' strike by the Russians on 31 May 2025 was coincidentally followed up by most devastating Ukrainian strike on Russia. The ongoing negotiations did get disrupted with the negotiations finishing within one hour. The violent scale of Russian response may alter the scenario though Ukrainians were already facing heavy barrages of Russian missile-drones strikes daily.

Local Sympathisers / Honey-Trapped Moles. Every country, despite being closed, strongest, or even wealthiest, will have local sympathisers / moles who will facilitate sabotage actions in their own country's rear areas. Although the Russian truck drivers seem innocent till now having been fooled by Ukrainian SBU operatives, Pakistan has a network of Pakistani Intelligence Operatives (PIOs) across India through honey traps and other espionage activities.

FSB Failure. Russian FSB failed to detect a sabotage operation being planned for the last 18 months on its own soil most probably very close to one of its own units. More details may emerge once detailed investigations are undertaken.

Key C-UAS Lessons for India

C-UAS is not an imagination or just a niche technology anymore. It's an essential operational imperative equally for military and civil which must transform from the bureaucratic drawing boards to a gap-free grid on ground. Since the operation was facilitated by local sympathisers / innocent civilians, its occurrence in India has high possibility. The operation highlights numerous C-UAS lessons for India as elucidated below in succeeding paragraphs.

Doctrine. The decoupling of drones' standard command and control protocols from conventional fixed RF or even frequency hopping and GPS dependency has rendered the existing C-UAS doctrines and organisational structures obsolete. There is an urgent inescapable need to rework the whole C-UAS doctrine, platforms, organisational structures and grid architecture.

Drones' Revolution and Sophistication of Technology. When studied in conjunction with Operation SINDOOR, drones' strikes can occur at any depth, from outside borders or by anti-national elements with or without enemy nation support inside India too. While the requirement of drones in all fields is diversifying including agriculture, Air Mobility etc, the security challenges are magnifying too. The sophistication of technology as witnessed in Operation SINDOOR can be extremely dangerous when in the hands of terrorists and applied on rogue drones. The absolute inadequacy of Russian C-UAS grid to handle such innovative employment of latest drones' technological toolkit should be taken as a serious wake-up call by all Indian security installations.

Easy Availability of Chinese Drones' Components. Unchecked easy availability of cheap Chinese drones' components has accentuated the rogue-drones threat through the ease of assembly on Indian soil.

Rogue Drones' Threat. Every asset, whatever size, mobile or static, tactical and strategic, is vulnerable to low-cost drone strikes unless well protected in a covered and concealed location. Any rogue drone strike can cause escalation of tensions which sometimes can spiral out of control.

Innovative Attacks – Steady Defence. While advancements in drones' technologies allow large innovation space in offensive operations, there is no scope of error in counter-drones defence. All the trials, errors and innovative ideas in C-UAS need to be practised under realistically simulated conditions. **There must be a separate innovative and advanced red drones' team, with latest adversary drones, for every indigenous C-UAS platform / system / architecture being tested before deployment**. **Since there would be no second chance, a steady C-UAS grid needs to be combat ready 24x7 to withstand any type of rogue drone threat as of yesterday**. Indian military, paramilitary, and police forces need to jointly collaborate with our civil industry to look for best fused solutions rather than individual L1 options.

Low Altitude Defence. As the AD systems of most strategic airbases focus on long-range defences, the low-altitude defence against rogue drones can sometimes be missed out. While low altitude is generally considered from 100 to 1000 metres

above ground, altitude lesser than 100m cause more significant problems. The propaganda videos coming lately from People's Liberation Army (PLA) indicate that the pilots from PLA Ground Forces (PLAGF) and People's Armed Police (PAPF) have been rehearsing flying of FPV drones extremely close to the ground. Thus, Indian security establishments need to be prepared to detect and engage small drones flying close to ground or "Spiderweb" type raid / sabotage situations.

Survivability. The key pillars of C-UAS are Detection, C2, Tracking and Engagement through both hard and soft kill methods. Whenever any of these steps gets missed **assured survivability** remains the only option to face the drones' attacks. Thus, survivability of all critical assets, whether military, government or private is most important. Rogue drones' threat is omnidirectional as they can fly in from anywhere. The most relevant survivability options against small drones include deployment in a tunnel / underground bunker / covered blast pen; mesh nets over mobile assets / roads; cope cages; and most importantly reduction of multi-domain signatures profile to minimise detection as much as possible.

Sanitisation of Neighbouring Areas. The Indian Drones regulations 2021 need to be revisited to ensure sanitisation of neighbouring areas around sensitive locations, redefine policies of usage of mobile networks and control on the numbers of drones held and prevent illegal assembly of drones' parts.

Multi-Domain MUMT. While Operation Spiderweb involved launch of FPV drones from trucks, Ukrainians have effectively also launched FPVs from Unmanned Surface Vehicles (USVs) on Sea to target Russian naval assets in black sea. Chinese have just tested one of the largest mother drones capable of launching many FPV drones. They are also mass-producing their own Baba Yaga variety of bomber drones. Hence, a multi-domain C-UAS grid must look at all possible cross-domain MUMT contingencies.

Balanced C-UAS Grid. While Akashteer and IACCCS ensured AD against Pakistan retaliatory strikes from 07 to 09 May 2025, Pakistani drones managed to infiltrate 100-120 km inside Indian territory. Hence, there is an inescapable urgency to strengthen Akashteer at tactical level with balanced C-UAS grid as illustrated below at

figure. There is a need to have multi-tiered multi-disciplinary AI enabled detection grid comprising an array of acoustic, visual, RF, EO/IR sensors, and passive / active radars.

Figure 19: Balanced C-UAS Toolkit

(Source-Author's Research and Analysis)

Detect	C2 / Tracking	Soft Kill	Hard Kill
• Acoustics • RF sensors • Electro-optical / PTZ camera • Active (AESA) radars • Passive radars • Mobile network usage	• Identification Friend or Foe (IFF) system • AI enablement – Auto Capture / Auto Homing	• Jamming (Noise, Follower, Tone, Smart, Swept) • GNSS Denial • Signal Spoofing • Sensor / Video Spoofing • Cyber Takeover • Net Capture • OFC cutting • OEM Software exploitation • AIS / SAR Jamming	• Shotguns / AI enabled machine guns • AD weapons / guns • Lasers/ DEWs • Microwave – HPM • Aerial/ Swarms Interception • Target Crew-RTH, Flight Data • Robot Dogs – Machine vs Machine

Mobile Intelligence. AI enabled detection of mobile network enabled flying of drones needs to be ensured timely by incorporating telecom operators, enhancing cellular traffic monitoring mechanism particularly for video uplinks data usage being undertaken apart from the whitelisted users. Thus, Telecom SIGINT layer integration is absolutely essential with IACCCS, Akashteer and Indian military's EW and C-UAS grid. India's national security apparatus must urgently design an integrated, telecom-literate counter-drone doctrine focussing on real-time surveillance of SIM activation across defence perimeters. This necessitates Integration of customs, telecom and defence intelligence databases including AI-enablement for predictive analytics and pattern-based interdiction protocols

LTE Coverage of Drones. Operation "Spiderweb" has demonstrated the evolving drones' threat landscape and the technology advancements wherein national telecom infrastructure can be actively exploited to bypass hardened AD / drones' defence

perimeters. Hence, Telecom Regulatory Authority of India must suitably address the illegal usage of telecom network by drones through both technological solutions as well as policy implementation. Additionally, the LTE coverage from India's border spillover regions needs to be unmonitored. Chinese mobile coverage on own side may also be exploited by PLA during operations. Mr Kakkar aptly points out that import of telemetry-capable modules, which may be concealed under generalized harmonized system codes, must be strictly monitored.

Aerial Interception. With increased sophistication of drones' technology in a cat and mouse game to evade advanced C-UAS measures, an establishment of a permanent standby interceptor drone may work out as the cheapest solution. With slightest doubt of a rogue drone detection by acoustic / visual / RF / radar means, a sentry pilot (with good FPV drone skills) must launch a FPV drone to engage the intruding rogue drone. Even every critical civilian entity like a data centre, defence production factory, religious site, oil rig, space data centre etc or even a big mall, must have adequately trained FPV drone pilots to bring down an intruding drone as a last resort.

C-UAS Awareness and Drills. While Operation SINDOOR ensured Indian government machinery right up to all Western Districts rehearsed blackout drills aimed at air alert, C-UAS drills would require few unique skills and procedures. There is no shortage of gamers' talent in India. Gaming and drones' racing skills and passion of such talented persons must be identified, harnessed and exploited during such emergencies.

Quantum AI Enabled and OFC Drones. While Operation Spiderweb showed an amalgamation of most advanced drones' technologies to evade C-UAS grid, it is important to look at what are the possible future advancements. Militaries world over are already looking at Quantum AI (QAI) enabled drones which can evade most EW counter-measures and even cyber-hacking attempts. At the same time, countering OFC drones has been a major challenge for both Russian and Ukrainian militaries during the ongoing war. Hence, Indian C-UAS grid must prepare for OFC as well as post QAI drones' era.

Multi-Layered C-UAS Grid. Mr Pawan Kakkar, has aptly described the layers of the C-UAS grid, with the recommended technology and the strategic objectives, as elucidated in figure below.

Figure 20: Recommended Drones Countermeasures Architecture

(Source- Mr Pawan Kakkar, Jugapro)

Layer	Technology	Strategic Objective
Passive RF Surveillance	SDR arrays + TDOA triangulation	Real-time mapping of SIM-initiated drone uplinks
Customs AI Pipelines	Machine-learned import profiling	Flag telemetry-capable hardware misclassification
Telecom-SIGINT Fusion	Real-time IMSI/IMEI correlation	Block dynamic LTE-based drone control networks
HUMINT-Support Layer	Civil-police vector education	Enable beat-level interdiction at drone staging nodes
Kinetic C-UAS Systems	AI-guided EO/IR + RF interceptors	Terminal-phase drone neutralization in layered envelope

Conclusion

Ukraine's SBU operation to strike five Russian airbases, holding the VKS bombers' fleet showcased precise orchestration of low-visibility FPV drones. It can also be taken as a revenge against those very bombers from Olenya and Belaya which struck Ukraine very hard on 26 and 31 May 2025. While attacks on three other bases generally failed, Ukraine's multi-axis sophisticated technology and sabotage precision strikes were successful on Belaya and Olenya airbases destroying and damaging more than 10% of Russian bomber fleet. The percentage is much higher for the active / fully mission capable bombers. Amongst all the strategic drone strikes world over till now, this will count as the most innovative, ambitious, sophisticated technology orchestration, low-cost but undoubtedly extremely complex logistically. The asymmetric audacity which incapacitated or evaded Russian AD on its strategic airbases is praiseworthy and admirable. However, with a large Pakistan's PIO network in India and advanced technology backup by China and Turkey, we would have to be extremely concerned about such emulations on Indian soil. The use of Chinese ultra

sets (exported to Pakistan Army) by terrorists in Pahalgam is an ideal example of how Chinese latest technology finds its way with terrosrists.

No single domain can create miracles alone and provide decisive victory. However, one vulnerability if optimally exploited by the enemy can surely lead towards defeat. **Indian security apparatus cannot afford to allow C-UAS to be that one vulnerability**. Operation Spiderweb was a balanced mixture of strategic resolve and steadfast politico-military will, quality GEOINT, HUMINT, innovative special forces operations, complex logistics, AI technology, local sympathisers / innocent persons (or moles if proven later) in Adversary nation, and low-cost FPV drones. The success of this operation will allow military thinkers to innovate new MUMT methodologies across all levels and depths of modern battlespace. **Indian bureaucracy, military, para-military, police, academia and most importantly industry partners need to sit together to establish a foolproof multi-domain C-UAS grid.**

About the Author

Brigadier Anshuman Narang, Retired, is an alumnus of prestigious Rastriya Indian Military College. He holds the “Adani Defence Chair of Excellence" on UAS Warfare with Special Focus on Counter-UAS at CENJOWS, is the Founder and Director of an independent Think-Tank "Atma Nirbhar Soch" and Advisor at Suhora Technologies. A keen China watcher and author of three books, his PhD topic is "Chinese RMA and Centennial Goals - Implications for India". His fourth book "PLA's ORBAT Compendium" is under publishing. As a gunner, he has the unique distinction of having been Brigade GSO-1 and Colonel GS of key armoured formations and has served across the complete India’s Western front from Siachen to South in both offensive and defensive formations. He has attended courses in all quad countries- American Artillery's Captain Career Course, Australian Joint Warfare Course and Japanese National Institute of Defence Studies Course. He took voluntarily retirement after commanding a prestigious Composite Artillery Brigade in October 2024 to pursue in-depth research of India’s adversaries.

Disclaimer

The views expressed in this monograph are solely those of the author and do not necessarily reflect the opinions or policies of CENJOWS. The author affirms that this work is an original piece of scholarly research, has not been published or submitted for publication elsewhere (in print or online), and that all data, facts, and figures cited are appropriately referenced and believed to be accurate to the best of the author's knowledge.

---

[1] Dr Oleksandra Molloy, Australian Army Research Centre, "Drones in Modern Warfare: Lessons Learnt from the War in Ukraine", 04 November 2024, available at https://researchcentre.army.gov.au/library/occasional-papers/drones-modern-warfare, accessed on 10 November 2024.

[2] Mr Pawan Kakkar, Jugapro, "Intelligence Dossier: Operation Spiderweb".

[3] Anshuman Narang, CENJOWS, "Employment of FPV Drones: A New Paradigm in Drones' Warfare", December 2024, available at https://cenjows.in/pdf-view/?url=2024/12/Brig_Anshuman_Narang_IB_Dec_2024_CENJOWS.pdf&pID=25888.

[4] Ibid; Curtis S, Control Room Supervisor at the Ukrainian Houses of Parliament, LinkedIn posts from 07 to 09 December 2024, available at https://www.linkedin.com/in/curtis-c-0695292a1?utm_source=share&utm_campaign=share_via&utm_content=profile&utm_medium=android,app, accessed on 09 November 2024.

[5] Mr Volodymyr Zelenskyy, **Володимир Зеленський** @ZelenskyyUa, x-post 02 June 2025, available at https://x.com/ZelenskyyUa/status/1929279052147265990, accessed on 02 June 2025.

[6] Steven Simoni, LinkedIn post, 04 June 2024, available at https://www.linkedin.com/posts/stevensimoni_a-few-trucks-117-drones-7-billion-of-russian-activity-7336055594748952576-xqVg/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxll4, accessed on 04 June 2024.

[7] X-post by AviVector@avivector, 01 June 2025 at 2:23 AM, available at https://x.com/avivector/status/1928917683937976352, accessed on 01 June 2025.

[8] Associated Press, "Ukraine's drone attack on Russian warplanes was a serious blow to the Kremlin's strategic arsenal", PBS News, 02 June 2025, available at https://www.pbs.org/newshour/world/ukraines-drone-attack-on-russian-warplanes-was-a-serious-blow-to-the-kremlins-strategic-arsenal, accessed on 03 June 2025.

[9] The International Institute for Strategic Studie (IISS), "The Military Balance 2025", Routledge Taylor Francis, Page 223.

[10] Scramble webpage for Russian Federation Air Force, available at https://scramble.nl/planning/orbats/russian-federation, accessed on 02 June 2025.

[11] Profile available at https://x.com/avivector.

[12] Tom Cooper, Sarcastosaurus on Substack, "A quick Review of the Russian Bomber-Fleet", 04 June 2024, available at https://xxtomcooperxx.substack.com/p/a-quick-review-of-the-russian-bomber?r=1xrkiw&triedRedirect=true, accessed on 04 June 2024.

[13] X-post by AviVector@avivector, 29 May 2025 at 9:43 PM, available at https://x.com/avivector/status/1928122657205059721, accessed on 01 June 2025.

[14] Associated Press, "Ukraine's drone attack on Russian warplanes was a serious blow to the Kremlin's strategic arsenal", PBS News, 02 June 2025, available at https://www.pbs.org/newshour/world/ukraines-drone-attack-on-russian-warplanes-was-a-serious-blow-to-the-kremlins-strategic-arsenal, accessed on 03 June 2025.

[15] Tom Cooper, Sarcastosaurus on Substack, "A quick Review of the Russian Bomber-Fleet", 04 June 2024, available at https://xxtomcooperxx.substack.com/p/a-quick-review-of-the-russian-bomber?r=1xrkiw&triedRedirect=true, accessed on 04 June 2024.

[16] Associated Press, "Ukraine's drone attack on Russian warplanes was a serious blow to the Kremlin's strategic arsenal", PBS News, 02 June 2025, available at https://www.pbs.org/newshour/world/ukraines-drone-attack-on-russian-warplanes-was-a-serious-blow-to-the-kremlins-strategic-arsenal, accessed on 03 June 2025.

[17] Tom Cooper, Sarcastosaurus on Substack, “A quick Review of the Russian Bomber-Fleet”, 04 June 2024, available at https://xxtomcooperxx.substack.com/p/a-quick-review-of-the-russian-bomber?r=1xrkiw&triedRedirect=true, accessed on 04 June 2024.
[18] Tom Cooper, Sarcastosaurus on Substack, “A quick Review of the Russian Bomber-Fleet”, 04 June 2024, available at https://xxtomcooperxx.substack.com/p/a-quick-review-of-the-russian-bomber?r=1xrkiw&triedRedirect=true, accessed on 04 June 2024.
[19] X-post by AviVector@avivector, 01 June 2025 at 2:23 AM, available at https://x.com/avivector/status/1928917683937976352, accessed on 01 June 2025.
[20] X-post by AviVector@avivector, 01 June 2025 at 2:23 AM, available at https://x.com/avivector/status/1928917683937976352, accessed on 01 June 2025.
[21] X-post by AviVector@avivector, 03 June 2025 at 7:45 PM, available at https://x.com/avivector/status/1929904849027490216, accessed on 03 June 2025.
[22] X-post by AviVector@avivector, 02 June 2025 at 11:39 PM, available at https://x.com/avivector/status/1929601187348729911, accessed on 03 June 2025.
[23] X-post by AviVector@avivector, 02 June 2025 at 11:39 PM, available at https://x.com/avivector/status/1929601187348729911, accessed on 03 June 2025.
[24] Mr Volodymyr Zelenskyy, **Володимир Зеленський** @ZelenskyyUa, x-post 02 June 2025, available at https://x.com/ZelenskyyUa/status/1929279052147265990, accessed on 02 June 2025.
[25] Telegram posts at https://t.me/ZarodinuVmesteZOV/20905, https://t.me/ZarodinuVmesteZOV/20905; Mr Pawan Kakkar, Jugapro, “Intelligence Dossier: Operation Spiderweb”.
[26] Mike Casey, “Quick Turn: Ukraine's "Spider Web" Strike”, 02 June 2025, available at https://substack.com/home/post/p-164960568, accessed on 02 June 2025.
[27] Cybele Mayes-Osterman, USA Today, “Russia's 'Pearl Harbor': What to know about Ukraine's audacious drone strike”, 02 June 2025, available at https://www.usatoday.com/story/news/world/2025/06/02/ukraine-drone-strike-attack-russia-pearl-harbor/83987304007/, accessed on 03 June 2025.
[28] Mike Casey, “Quick Turn: Ukraine's "Spider Web" Strike”, 02 June 2025, available at https://substack.com/home/post/p-164960568, accessed on 02 June 2025.
[29] LinkedIn post by Riccardo Romani, 02 June 2025, available at https://www.linkedin.com/feed/update/urn:li:activity:7335491187815919616?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEnsP2oBmwwXa-ctZBR93FVX62E0KCbGS2A, accessed on 02 June 2025.
[30] Mr Volodymyr Zelenskyy, **Володимир Зеленський** @ZelenskyyUa, x-post 02 June 2025, available at https://x.com/ZelenskyyUa/status/1929279052147265990, accessed on 02 June 2025.
[31] Mike Casey, “Quick Turn: Ukraine's "Spider Web" Strike”, 02 June 2025, available at https://substack.com/home/post/p-164960568, accessed on 02 June 2025.
[32] Marjin Markus, LinkedIn post on 04 June 2025, available at https://www.linkedin.com/posts/marijnmarkus_ukraine-activity-7336034335537459201-oKNI/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxII4, accessed on 04 June 2025.
[33] Marjin Markus, LinkedIn post on 04 June 2025, available at https://www.linkedin.com/posts/marijnmarkus_ukraine-activity-7336034335537459201-oKNI/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxII4, accessed on 04 June 2025.
[34] Marjin Markus, LinkedIn post on 04 June 2025, available at https://www.linkedin.com/posts/marijnmarkus_ukraine-activity-7336034335537459201-oKNI/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxII4, accessed on 04 June 2025.
[35] X-post at 3:40 am on 03 June 2025 by Ukraine Battle Map@ukraine_map, available at https://x.com/ukraine_map/status/1929661928395182242, accessed on 03 June 2025.
[36] X-post by Emil Kastehelmi@emilkastehelmi, on 03 June 2025 at 1:49 AM, available at https://x.com/emilkastehelmi/status/1929633971991990456, accessed on 03 June 2025.
[37] Telegram posts at https://t.me/ZarodinuVmesteZOV/20905, https://t.me/ZarodinuVmesteZOV/20905; Mr Pawan Kakkar, Jugapro, “Intelligence Dossier: Operation Spiderweb”.
[38] Cybele Mayes-Osterman, USA Today, “Russia's 'Pearl Harbor': What to know about Ukraine's audacious drone strike”, 02 June 2025, available at https://www.usatoday.com/story/news/world/2025/06/02/ukraine-drone-strike-attack-russia-pearl-harbor/83987304007/, accessed on 03 June 2025.
[39] Mr Pawan Kakkar, Jugapro, “Intelligence Dossier: Operation Spiderweb”.
[40] Mr Pawan Kakkar, Jugapro, “Intelligence Dossier: Operation Spiderweb”.

[41] X-post by AviVector@avivector, 03 June 2025 at 7:45 PM, available at https://x.com/avivector/status/1929904849027490216, accessed on 03 June 2025.
[42] X-post by AviVector@avivector, 04 June 2025 at 12:19 AM, available at https://x.com/avivector/status/1929973635953111475, accessed on 04 June 2025.
[43] Cybele Mayes-Osterman, USA Today, “Russia's 'Pearl Harbor': What to know about Ukraine's audacious drone strike”, 02 June 2025, available at https://www.usatoday.com/story/news/world/2025/06/02/ukraine-drone-strike-attack-russia-pearl-harbor/83987304007/, accessed on 03 June 2025.
[44] X-post by Damien Symon, 04 June 2025 at 10:54 PM, available at https://x.com/detresfa_/status/1930314714527019423, accessed on 05 June 2025.