Assessment of Ukraine's Operation 'Spider Web'

Introduction

In early Jun 2025, Ukraine targeted Russian military airbases located deep within Russian territory with a massive drone strike as a part of Operation 'Spider Web', which has been recorded as Ukraine's longest-range strike till date since the start of the conflict between the two countries. According to reports, Ukraine's coordinated attacks involving 117 First Person View (FPV) drones struck 41 Russian aircrafts, including A-50 aircrafts, nuclear-capable Tu-95, Tu-22, and Tu-160 strategic bombers, which were allegedly used to bomb Ukrainian cities.[1] This attack by Ukraine aptly demonstrates the changing nature of warfare in the contemporary times and the use of intelligence and covert operations to degrade an enemy's air-power capabilities. While the theatre of this attack was in Russia, it also has implications for other nations which rely on air power in current times.

Understanding Operation Spider Web

Either in spare parts or covertly assembled on various locations, 117 FPV drones were purportedly smuggled into Russia. Launches were conducted from concealed trailers, vehicles, or movable wooden huts or containers with retractable roofs that were placed close to targeted airbases. According to one report, drones were assembled at a Chelyabinsk warehouse that was hired for rent in Russia. A traditional special operations tactic that has been modified for this type of drone warfare is the employment of harmless civilian vehicles or structures for cover. By smuggling and launching FPV drones locally, this technique successfully produced a 'Trojan Horse'-like situation, circumventing perimeter defences intended to fend off outside attacks and posing a threat to the safety of vital assets situated well behind the front. Despite their small operational range, FPV drones are highly effective when launched from strategically placed and hidden sites close to the targets.[2]

Impact on Russia

Operation Spider Web exposed a loophole in Russia's defence preparedness in the present conflict. This has raised concerns and charges of carelessness, complacency, and corruption among Russian military elites. Questions are being raised about how it was possible for Ukrainian intelligence to transport the FPV drones within close proximity to various Russian air bases and then unleash them with disastrous results, while nuclear-capable bombers were left exposed and uncovered by hangars. There are reports of blatant irresponsibility and

negligence of the aerospace command head as there were plans to construct about 300 aeroplane shelters made of reinforced concrete, which had not been accomplished since 2021.[3]

From an operational perspective, this attack might compel the Russians to relocate their aircrafts farther away from Ukraine more frequently in order to evade detection. Additionally, it will compel Russia to perhaps re-allocate air defence resources from other locations. Depending on the exact number of aircrafts destroyed or damaged, fewer Russian bombers will be able to carry and deploy long-range missiles which are more accurate, more difficult to intercept, and carry a significantly larger warhead than any drone and, thus, achieve a higher rate of penetration against Ukrainian air defences.[4]

Evolution of Asymmetric Warfare

The Ukrainian morale was so high after this attack that they used underwater explosives to assault the Kerch Bridge in occupied Crimea as a follow-up to these airfield strikes.[5] Ukraine would also like to use this tactic in maritime sphere to take down Russia's naval assets as Ukraine is said to have transformed a few maritime drones into drone carriers capable of launching FPV drones. Russian Pantsir-S1 air defence systems were hit on land by FPV drones launched by Ukrainian Artificial Intelligence (AI)-enabled sea drones/carriers in the Black Sea early this year.[6]

Operation Spider Web demonstrates that strategic aircrafts valued at billions of dollars can be destroyed by FPV drones, which are constructed using low-cost parts and managed by open-source autopilot systems like ArduPilot, which provided advanced flight stabilisation, waypoint navigation, failsafe routines, and programmable mission profiles. Russian mobile telecommunications networks, including 4G and LTE connections, were used to remotely operate drones deployed in this operation. Ukrainian operators were able to control drone flights from outside of Russian territory, thanks to these networks which allowed for real-time video transmission and command inputs over great distances. This configuration eliminated the requirement for any local operators or physical ground control stations.[7]

Potential Future Vulnerabilities

The United States (US) could raise the alarm about American military installations susceptibility to this type of assault, but scholars believe it to be much likely and will not be a

surprise.[8] Security experts are concerned that many non-state entities have access to all the technology utilised in operation Spider Web, or at least copies of them. In order to attack both military and civilian infrastructure, they can be inspired by the operation and replicate certain aspects of it in new settings. Another aspect that could be imitated is the smuggling of drones on the back of trucks that are unintentionally operated by Russian drivers. Europe and the North Atlantic Treaty Organisation's (NATO) open, interdependent economies are susceptible to similarly disruptive threats. Checking every shipment that enters the ports of NATO countries for drones is not practical. The US has expressed worries in recent years about Chinese corporations buying land close to important US military installations; Finland forbade Russian citizens from doing the same in 2025 near its sensitive military installations. Concerns are raised by recent unexplained drone overflights close to bases and airports from Denmark and Germany to the US and the United Kingdom (UK).[9]

Global Military Lessons

In response to the possible threat posed by adversary drones to US soldiers, US Ambassador to NATO Matthew Whitaker stated that the country is taking lessons.[10] Similar to the concerns raised by the US military base overflights in recent years over their susceptibility to tiny drone attacks, Operation Spider Web demonstrates that vulnerabilities affect vital and military infrastructure more generally.[11] As seen in the operation, Pierre Vandier, Supreme Allied Commander Transformation of NATO, has admitted that the alliance can learn from Ukraine, especially in regards to its innovative approach to combat operations.[12]

Apart from Europe, Asian militaries will also take a few lessons from this asymmetric operation. Countries like Taiwan facing threat from China will get inspired to adopt drones and AI technology to counter China offensively in the event of an attack by them.[13] Similarly, Beijing will also look to guard itself against enemy forces infiltrating military bases in the event of a Taiwan conflict. Similar to Russia, China's strategic rear area, which includes the hilly southwest and northwest deserts, is thousands of kilometres deep and is remote from the east coast and the Taiwan Strait and houses a large number of military installations. Such drone attacks might also target China, particularly cross-shore important places; this would put a great deal of pressure on security personnel to protect military infrastructures.[14]

India also needs to assess its defence preparedness as future battles for India might not start with traditional cross-border force-on-force confrontations. Instead, the first rounds

might come in the shape of coordinated cyber-attacks against command networks, energy infrastructure, and transportation, or disguised civilian cargo laced with drones or harmful code inserted into software upgrades.[15]

Conclusion

Operation Spider Web demonstrated the ability of a weaker nation to cripple military assets inside a stronger enemy's territory at a nominal cost using technology, intelligence, and innovation. While the operation may not drastically alter the military balance of power between Russia and Ukraine, nor will it deter Russia in the near future, it psychologically impacts the Russian military as a large number of bombers were destroyed very easily and will take time to replenish. Going forward, every nation must protect its military strategy by identifying and detecting vulnerable assets not only during wartime, when they may remain dormant, but also in times of peace. Moreover, the covert and secret transportation and assembly of low-cost drones inside enemy territory will be a new challenge in the future.

Endnotes

[1] Nikita Sharma, "Drones Hidden in Trucks: How Ukraine Carried out Operation Spider's Web in Russia", *Hindustan Times*, 02 Jun 2025, accessed 05 Jun 2025 https://www.hindustantimes.com/world-news/drones-hidden-in-trucks-how-ukraine-carried-out-operation-spider-s-web-against-russia-101748813348698.html
[2] Joël-François Dumont, "Operation Spider Web: Strategic Analysis", *European Security*, 03 Jun 2025, accessed 06 Jun 2025 https://european-security.com/operation-spider-web/
[3] Mark Trevelyan, "Russian War Bloggers Blame Military Command for Stunning Ukrainian Attack on Bomber Fleet", *Reuters*, 04 Jun 2025, accessed 07 Jun 2025 https://www.reuters.com/business/aerospace-defense/russian-war-bloggers-blame-military-command-stunning-ukrainian-attack-bomber-2025-06-04/
[4] Mick Ryan, "The Three Punch Combo behind Ukraine's Spectacular Drone Strike on Russia", *Lowy Institute*, 02 Jun 2025, accessed 08 Jun 2025 https://www.lowyinstitute.org/the-interpreter/three-punch-combo-behind-ukraine-s-spectacular-drone-strike-russia
[5] Christian Edwards, Svitlana Vlasova, and Anna Chernova, "Ukraine Strikes Bridge Connecting Russia to Crimea with Underwater Explosives", *CNN News*, 03 Jun 2025, 07 Jun 2025 https://edition.cnn.com/2025/06/03/europe/ukraine-crimea-bridge-russia-underwater-intl
[6] David Kirichenko, "Ukraine's Cheap Robot Drones Extract a Heavy Price from Russia", *Lowy Institute*, 05 Jun 2025, accessed 08 Jun 2025 https://www.lowyinstitute.org/the-interpreter/ukraine-s-cheap-robot-drones-extract-heavy-price-russia
[7] Kateryna Bondar, "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare", *Center for Strategic and International Studies*, 02 Jun 2025, 10 Jun 2025 https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare
[8] Harlan Ullman, "What the US Can Learn from Ukraine's Remarkable Operation Spider Web", *The Hill*, 09 Jun 2025, accessed 10 Jun 2025 https://thehill.com/opinion/national-security/5337452-spider-web-ukrainian-drone-attack-russia/
[9] Katja Bego, "Ukraine's Operation Spider's Web Is a Game-Changer for Modern Drone Warfare. NATO Should Pay Attention", *Chatham House*, 06 Jun 2025, accessed 10 Jun 2025 https://www.chathamhouse.org/2025/06/ukraines-operation-spiders-web-game-changer-modern-drone-warfare-nato-should-pay-attention
[10] Khrystyna Bondarieva, "Operation Spider's Web: US Learning Lessons from Russo-Ukrainian War, Says Ambassador", *Ukrainska Pravda*, 04 Jun 2025, accessed 10 Jun 2025 https://www.pravda.com.ua/eng/news/2025/06/4/7515634/

[11] Michael C Horowitz, “Ukraine’s Operation Spider’s Web Shows Future of Drone Warfare”, *Council on Foreign Relations*, 03 Jun 2025, accessed 10 Jun 2025 https://www.cfr.org/expert-brief/ukraines-operation-spiders-web-shows-future-drone-warfare
[12] Ulyana Krychkovska, “NATO Admiral Says That Operation Spider’s Web Is Example of Creativity Worth Learning From”, *European Pravda*, 09 Jun 2025, accessed 10 Jun 2025 https://www.eurointegration.com.ua/eng/news/2025/06/9/7213350/
[13] Derek Grossman, “Ukraine’s Audacious Asymmetric Attack on Russia Inspires Taiwan”, *Nikkei Asia*, 13 Jun 2025, accessed 15 Jun 2025 https://asia.nikkei.com/Opinion/Ukraine-s-audacious-asymmetric-attack-on-Russia-inspires-Taiwan
[14] Liu Zhen, Seong Hyeon Choi, and Yuanyue Dang, “How Ukraine’s Operation Spider’s Web Attack on Russia Holds Important Lessons for China”, *South China Morning Post*, 07 Jun 2025, accessed 10 Jun 2025 https://www.scmp.com/news/china/military/article/3313436/how-ukraines-operation-spiders-web-attack-russia-holds-important-lessons-china
[15] BK Sharma, “The Trojan Horse Returns: Lessons from Ukraine’s Operation Spiderweb for India’s Strategic Security”, *The Week*, 09 Jun 2025, accessed 10 Jun 2025 https://www.theweek.in/news/defence/2025/06/09/the-trojan-horse-returns-lessons-from-ukraines-operation-spiderweb-for-indias-strategic-security.html

Ajay Kumar Das is a Independent Scholar of International Affairs & Security Studies

Uploaded on : 23-06-2025