IIRF ISSUE BRIEF

UKRAINE'S OPERATION "SPIDER'S WEB": ASYMMETRIC WARFARE

Introduction

1. On 1st June, the Security Service of Ukraine (SSU) carried out a bold and unprecedented coordinated drone strike deep inside Russian territory. The operation targeted four strategic air bases and delivered a major blow to Moscow's long-range bomber fleet. Codenamed "Spider's Web"—or simply "Web"—the operation was named for its wide geographic coverage across remote Russian locations previously thought to be beyond the reach of Ukraine's long-range drone capabilities.

Using small striking drones covertly smuggled into Russia and launched from hidden compartments inside cargo trucks, the operation struck more than 40 high-value aircraft—including strategic bombers Tu-95MS, Tu-22M3, and A-50 planes used for launching and coordinating missile attacks on Ukrainian cities. The meticulously planned operation marks a significant milestone in Ukraine's evolving asymmetric warfare capabilities and signals a major vulnerability in Russia's rear defenses.

Key Targets

2. Operation Spider's Web targeted four key Russian military air bases that play pivotal roles in Russia's strategic aviation infrastructure. Notably, their locations span the entire breadth of Russian territory, an aspect that likely inspired the codename of the operation.

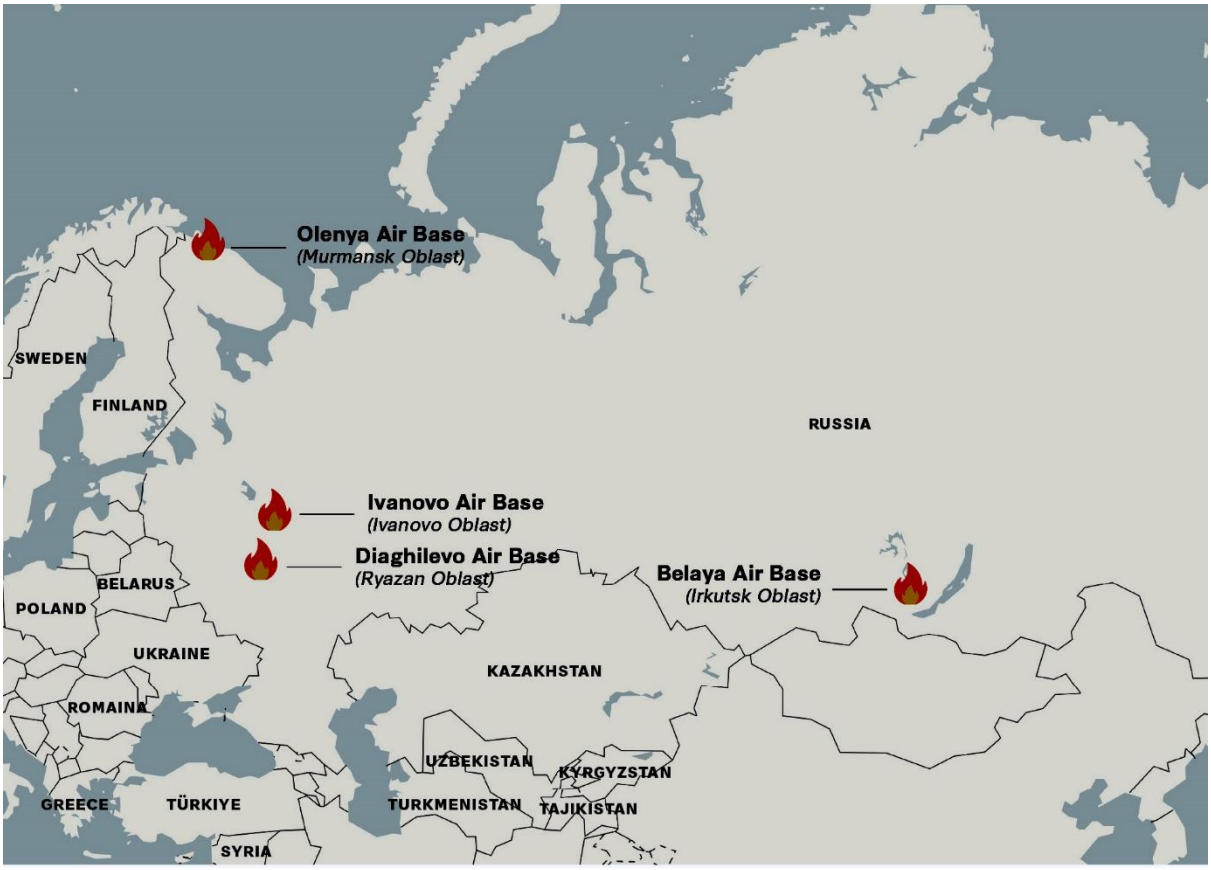
Olenya Air Base (Murmansk Oblast)

3. Olenya air base is located on the Kola Peninsula and approximately 1,900 km north of Ukraine. It is home to the 40th Composite Aviation Regiment, which includes a squadron of Tu-22M3 bombers. In addition, a significant number of Tu-95MS strategic bombers—previously stationed elsewhere—had been relocated to this base, making it a vital launch point for long-range missile strikes against Ukraine. The base's remote Arctic location was previously considered sufficient protection against Ukrainian attacks.

Diaghilevo Air Base (Ryazan Oblast)

4. Diaghilevo serves as Russia's central hub for the combat training of strategic aviation crews. It is located approximately 470 km from the Ukrainian border. The base also houses a major aircraft repair facility for all types of Russian strategic bombers, including the Tu-95, Tu-160, and Tu-22M3. Damage to this base not only affects active bomber units but also disrupts both pilot training pipelines and maintenance operations for Russia's long-range aviation fleet.

Targeted Russian airbases During Ukrainian Drone Operation



Belaya Air Base (Irkutsk Oblast)

5. Located deep in Siberia, more than 4,000 km from Ukraine, the Belaya air base was previously thought to be well beyond the reach of Ukrainian strikes—until now. The airfield hosts the 220th Heavy Bomber Aviation Regiment, which operates Tu-22M3 bombers capable of launching Kh-22 supersonic cruise missiles. The drone strike here marks the first documented Ukrainian attack on a military target in this region, demonstrating the unprecedented operational range and tactical ingenuity of the SSU's campaign.

Ivanovo Air Base (Ivanovo Oblast)

6. Located about 700 km from the Ukrainian border, Ivanovo air base is the primary station for Russia's A-50 AWACS (airborne warning and control system) aircraft, which are crucial to Russian air operations. These aircraft perform key functions such as detecting air defense systems, tracking airborne threats, and coordinating fighter jet activity. With Russia possessing fewer than ten A-50s in total, the loss or damage of even one significantly degrades its situational awareness and command-and-control capabilities.

7. The Russian Ministry of Defence also mentioned attacks in Amur Oblast, but no confirmed damage was reported.

8. Together, these four bases form the backbone of Russia's long-range strike and aerial surveillance capabilities. Their simultaneous targeting reflects a sophisticated and coordinated Ukrainian effort to undermine Russia's ability to project air power and sustain missile attacks across Ukraine.

9. Aviation Assets Destroyed

- During the SSU's special operation, Spider's Web, Ukraine targeted and destroyed more than 40 Russian aircraft stationed at four key air bases across Russian territory. The major losses include strategic bombing, aviation, and airborne early warning and control aircraft.

- **Tu-9** A Soviet-era strategic bomber equipped with turboprop engines, used by Russia to launch long-range cruise missiles such as the Kh-55, Kh-555, and the newer Kh-101/102. Each aircraft can carry up to 16 cruise missiles. Despite its age, the Tu-95 remains a critical asset in Russia's long-range strike capability.

- **Tu-22M3** A supersonic long-range bomber capable of carrying Kh-22 cruise missiles, which pose a severe challenge for Ukrainian air defenses due to their high speed. The Tu-22M3 forms part of Russia's conventional and nuclear strike forces.

- **A-50** An AWACS aircraft used by Russia to detect air defense systems, coordinate missile strikes, and guide fighter aircraft. Russia has fewer than ten operational A-50s, and each is estimated to cost around $350 million. Their loss severely limits Russia's situational awareness and air command capabilities.

- **Tu-160** A supersonic, variable-sweep wing strategic bomber and the largest combat aircraft in the world. Capable of carrying both nuclear and conventional cruise missiles, including the Kh-101 and Kh-102, the Tu-160 serves as a key component of Russia's long-range strike and nuclear deterrent force.

The majority of aircraft confirmed damaged or destroyed belong to the core platforms used by Russia for strategic bombing and battlefield coordination.

Conduct of Operation

10. Planning for the operation reportedly began over 18 months prior to its execution. Ukrainian operatives smuggled around 150 small strike drones, modular launch systems, and 300 explosive payloads into Russia through covert logistical routes. The drones were concealed inside wooden modular cabins, which were then loaded onto standard cargo trucks.

11. An integral component of the operation was its use of covert logistics conducted through Russian territory, involving unwitting Russian civilian participants. As part of the operation's deception strategy, the SSU reportedly recruited Russian truck drivers to deliver the mobile drone launchers camouflaged as standard cargo loads. These drivers were instructed to arrive at specific times and park at predesignated locations in the vicinity of Russian strategic air bases, including fuel stations and isolated roadside areas.

12. At the designated time, the roofs of the cabins were remotely opened, and the drones launched directly from within the trucks. This minimized the distance between launch and impact, allowing the drones to bypass Russia's layered air defense systems—including Pantsir and S-300 units—before they could react. Notably, Russian sources confirmed the drones were launched from positions just outside the airfields, including from fuel stations and roadside laybys. After all the drones were launched, the trucks exploded, indicating that they were equipped with a self-destruction mechanism.

13. Altogether, 117 drones were launched, with over 40 aircraft struck, amounting to what Ukrainian sources estimate as 34 percent of Russia's strategic cruise missile delivery platforms. This includes some of the few remaining A-50 airborne early warning and control aircraft, which are vital to Russia's airspace surveillance and targeting operations.

14. Importantly, all personnel involved in the operation were successfully moved from Russian territory to Ukraine prior to drone launch. Ukrainian leadership, including President Zelensky and SSU chief Vasyl Maliuk, was reportedly closely involved in the planning and real-time coordination of the strike.

15. The success of Spider's Web highlights a dramatic shift in the balance of initiative. Ukraine demonstrated the ability to execute a coordinated, multi-theater deep-strike operation, far beyond its borders, using fully indigenous systems and asymmetric tactics—blending deception, precision, and strategic surprise.

Role of AI in Spider's Web Drone Operation

16. In Operation Spider's Web, Ukraine demonstrated a hybrid approach to drone warfare that combined remote human control with elements of autonomy and potentially AI-assisted functionality. While the operation was not fully autonomous, the available evidence suggests that artificial intelligence likely played a supporting role in both flight stability and targeting, particularly in enabling precise strikes on vulnerable components of high-value aircraft.

17. The first-person-view (FPV) drones used in the operation were remotely controlled through Russian mobile telecommunications networks, including 4G and 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 setup avoided the need for any physical ground control stations or nearby operators.

18. To enable stable long-distance control over mobile networks, the drones relied on a software-hardware system built around ArduPilot—a widely used, open-source autopilot framework designed for unmanned aerial vehicles. ArduPilot provides advanced flight stabilization, waypoint navigation, failsafe routines, and programmable mission profiles. In this case, each drone was integrated with a compact onboard computer (such as a Raspberry Pi), 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's UART interface, allowing operators to pilot the drone remotely with stabilized, responsive input—even when faced with significant signal latency.

19. ArduPilot's flexibility makes it well-suited for missions operating over unstable or high-latency links, such as mobile internet, as it can independently manage the drone's orientation, heading, and altitude, ensuring flight stability while awaiting operator commands. This made it the ideal choice for long-range, internet-based FPV control—especially when using improvised mobile launch platforms deep inside Russian territory.

20. In addition to manual control, AI-assisted targeting appears to have been integrated into the drones' attack logic. According to open-source intelligence and reporting, SSU teams studied construction and visual profiles of the targeted aircraft—including Tu-95MS, Tu-22M3, and A-50 models, which are preserved in Ukrainian aviation museums like the Poltava Museum of Long-Range and Strategic Aviation—to identify precise weak points.

21. These profiles likely served as training data for machine vision models that were then embedded into the drones' onboard computers. Such models could assist operators by identifying key structural weak points, such as underwing missile pylons and fuel tank seams, enabling rapid and precise final-stage maneuvering during the dive attack. The images released by the SSU confirm that the specific structural points, as shown in Figure 3, were identified as targets during the preparation phase, and later, official footage shows drones striking precisely at those designated areas.

Highlights

22. While there is no public confirmation that the drones executed AI-assisted autonomous strikes, the integration of AI-based object recognition into the control architecture likely augmented the operators' ability to strike specific aircraft vulnerabilities. In effect, the drones acted as precision weapons—remotely flown, but potentially capable of executing final targeting actions with computational assistance.

23. The success of the mission did not hinge on technological novelty alone, but rather on the organizational ingenuity, deep reconnaissance, and logistical mastery that enabled Ukraine to strike at the core of Russia's strategic aviation assets—far beyond the frontline.

Estimated Cost of Losses

24. The SSU has estimated cost of the equipment destroyed as a result of Operation Spider's Web is over US$7 billion. A senior NATO official called the operation the most successful one yet. The Alliance estimated that at least 40 aircraft were damaged and between 10 and 13 aircrafts were completely destroyed.

25. **Relocation of Russian Assets** Russia has relocated dozens of its strategic bombers to more remote airbases across the country in the wake of this month's sweeping Ukrainian drone assault on Moscow's military aircraft, satellite imagery suggests.

26. Ukrainian security services conducted a massive drone attack against Russian military airbases on June 1, striking thousands of kilometres from the front line in what President Volodymyr Zelensky said was their longest-range operation ever. The attack, named "Operation Spider's Web," targeted multiple airbases deep inside Russia, including in the Murmansk, Irkutsk, Ryazan and Ivanovo regions.

27. Beyond the battlefield, Operation Spiderweb reshapes strategic assumptions, diplomatic dynamics, and the very nature of deterrence. It reaffirms the principle that innovation and resolve can compensate for size and scale, and it establishes Ukraine as a formidable actor capable of transforming adversity into strategic advantage.

28. This operation was not just about damage—it was about declaring that in the 21st century, even a smaller power can strike at the heart of a larger one, provided it has the ingenuity, the intelligence, and the will. As nations around the world take note, the lessons of Operation Spiderweb may well define the next generation of military and hybrid conflict.

Analysis of the attack

29. Operation Spiderweb stands as a turning point in the war between Ukraine and Russia, not only because of its bold execution and technical precision but because of what it symbolizes. It represents a shift from traditional, attrition-based warfare to a form of conflict that is smart, asymmetric, and deeply integrated with civilian and commercial technology. With relatively inexpensive means, Ukraine demonstrated the capacity to disrupt some of the most secure and critical infrastructure within the Russian Federation.

30. **Role of AI** One of the most important questions here is how an attack of this scale was successful. The AI-powered drones used in the attack infiltrated Russia from various regions in specially designed trucks. The attack was carried out semi-autonomously, with hundreds of drones taking off from areas very close to air bases. The drones operated remotely via the Russian mobile telecommunications network. This network has sufficient bandwidth to transmit images instantaneously to operators in Ukraine. Additionally, the drones, which targeted specific bombers, were provided with information about the aircraft's weaknesses through artificial intelligence before the attack. This increased the accuracy of the attack.

31. **Asymmetric Attack** This is an asymmetric attack. It can be said that the strategically important airport is not adequately protected, or at least not protected against current threats. While areas of such importance are protected against large-scale attacks, they are vulnerable to smaller, simpler yet effective ones. No matter how advanced old technology is, it is vulnerable to new, simpler technology. The ability of a low-cost RPG to overcome a tank is a similar example. The Spider Web operation demonstrates the vital importance of advanced counter-unmanned aircraft defence systems for such strategic bases.

32. These aircraft are designed to travel long distances and deliver heavy payloads deep inside target countries. We have also seen some bombers launch ballistic missile attacks in Ukraine. The exact impact of Kyiv's high-profile operation on Russia's long-range strike capabilities, as well as its reconnaissance and surveillance activities, is unclear. However, this operation will partially disrupt future attacks, not only in Ukraine but also in any locations where Russia has a military footprint.

33. **Future Prediction** One reason these weapons are strategic is the cost of the aircraft's nuclear capability. They are no longer in mass production, and it would take a long time to rebuild them. Moscow might even consider scrapping the entire fleet. Nevertheless, this attack would not undermine Russia's vast inventory, especially its nuclear capabilities. Nevertheless, Russia should reassess the vulnerability of its strategically important air and naval bases, which house nuclear-capable submarines. Ukraine is very likely to carry out similar attacks more frequently, given its failure to achieve success on the main fronts and its increased deep strike capabilities.

Russian Punitive Strike

34. Russia launched a massive punitive bombing attack against Kyiv's daring **Spider's web** drone assault. Friday's massive bombing was Putin's biggest attack since Kyiv's daring drone assault took out dozens of strategic bombers at Russian airfields.

- KYIV — Russia launched a huge barrage of missiles and drones against a broad swath of Ukrainian territory early Friday, killing at least three people and injuring more than 40 others that took out dozens of strategic bombers at Russian airfields on June 1.

- In total, over 400 drones and more than 40 missiles — including ballistic missiles — were used in this attack. Almost all of Ukraine were targeted in this attack — Volyn, Lviv, Ternopil, Kyiv, Sumy, Poltava, Khmelnytskyi, Cherkasy, and Chernihiv regions.

- The attack was described as one of the largest since the beginning of the war. Russia also targeted other areas in Ukraine including it's largest city, Kharkiv.

- **Ukraine's air force said 452 drones and missiles were launched against the country, with airstrikes recorded in 13 locations, in an attack that lasted more than four hours. More than 400 of the drones and missiles were shot down or otherwise neutralized, the air force said.**

Comments

35. It is pertinent to examine whether Operation Spider Web, a Ukrainian drone attack targeting Russian airbases, was likely a worthwhile strategic and psychological victory for Ukraine, despite the subsequent Russian retaliation.

36. While Russia did respond with increased aerial attacks, the operation inflicted significant damage on Russian military assets, including nuclear-capable bombers, and demonstrated Ukraine's ability to strike deep inside Russian territory. This raised the cost of the war for Russia and potentially influenced the calculus of future negotiations.

- **Significant Damage** Operation Spider Web resulted in the destruction or damage of over 40 Russian military aircraft, including strategic bombers, causing an estimated $7 billion in losses. This included the disruption of early warning radar systems.

- **Strategic Impact** The attack targeted Russian airbases far from the front lines, demonstrating that even seemingly secure locations were vulnerable to Ukrainian strikes. This forced Russia to reassess its defensive posture and potentially divert resources to protect its rear areas.

- **Psychological Effect** The operation boosted Ukrainian morale and served as a powerful message that Ukraine could inflict significant damage on Russia, potentially influencing the trajectory of the war.

- **Retaliation** Russia responded with increased aerial attacks on Ukrainian infrastructure and military targets. However, the scale and nature of the Ukrainian attack, particularly its targeting of strategic assets, likely forced Russia to reassess its strategy.

- **Potential for Diplomacy** Some analysts suggested that the attack, while not immediately altering Putin's goals, could push Russia towards diplomacy by demonstrating the cost of continuing the war.

Conclusion

37. Operation Spider's Web not only showcased Ukraine's tactical ingenuity but also illuminated the broader technological and strategic shifts reshaping modern warfare. As unmanned systems become more sophisticated, accessible, and effective, there are three critical trends that military and political leaders around the world can no longer afford to ignore.

38. **First,** the proliferation of cheap, attritable technologies—both in hardware and software—is accelerating. Cheap off-the-shelf FPV drones, open-source software platforms, and AI models, once designed for hobbyists, are now weaponized with devastating results. The accessibility and adaptability of such systems make them an attractive tool for state and non-state actors alike, demanding urgent efforts to anticipate, regulate, and counter their militarized use in both conflict zones and domestic settings.

39. **Second,** the steady advance of autonomy is reshaping how these systems operate. While current drones often separate navigation, targeting, and execution into distinct semiautonomous functions, future iterations will likely merge them into unified, fully autonomous platforms capable of conducting missions independently, across vast distances, and with minimal human oversight. This progression will challenge existing doctrines, oversight mechanisms, and ethical boundaries.

40. **Third,** the operation demonstrated the growing need for robust physical protection and dedicated countermeasures against drone threats. From critical military infrastructure to civilian sites, the vulnerability to small, precise, and hard-to-detect systems is growing. Conventional air defenses are often ill-suited for this new threat landscape, prompting an urgent call for innovation in early detection, electronic warfare, and layered physical defenses.

41. Together, these trends point to a future where technological agility, not just industrial scale, determines strategic advantage. The militaries that adapt early—by investing in resilience, countermeasures, and adaptive doctrine—will be best positioned to meet the challenges of a rapidly evolving battlefield.