We have the technology! – The Ukrainian drone attacks on Russian airfields

by Michael Winberg

Resumé

Den 1 juni spreds nyheten om drönarattacker mot ryska flygbaser för det strategiska bombflyget djupt inne i Ryssland. Den ukrainska säkerhetstjänsten SBU släppte relativt omgående filmer på attackerna som skett med hjälp av så kallade FPV-drönare. På sociala medier och olika nyhetssajter kablades det ut att attackerna möjliggjorts tack vare artificiell intelligens då avstånden mellan Ukraina och målen omöjliggjorde vanlig länkförbindelse. I efterhand har sanningen visat sig varit en annan och teknologin som möjliggjorde operationen betydligt enklare än vad många trott. Samtidigt är det ett budskap som fler kan lära sig av. Nämligen att vi redan idag har tillgång till teknik och mjukvara som kan möjliggöra den här typen av sofistikerade operationer, och att den finns tillgänglig att köpa till låg kostnad i elektronik- och hobbybutiker. Artikeln kommer att använda Ukrainas lyckade operation som fallstudie och argumentera för att även vi, med små medel kan lyckas med liknande operationer.

ON 1 JUNE, the news spread that Russian airbases deep inside Russian territory had been attacked. Although Russian airfields had been attacked before, this attack stood out as videos and imagery suggested the attack was carried out with first-person-view (FPV) drones—an incredible accomplishment when conducted as far as 4000 km away from Ukrainian soil.[1] And although the final count of destroyed aeroplanes is still debated, there is no denying the attack was a success. As the story began to spread on social media, some quickly attributed the successful attack to artificial intelligence (AI). However, as soon as the Ukrainian Security Service (SBU) began to release videos and details about the operation, named "Spider web", the facts told a different story. Instead of autonomous drones with AI targeting systems, we saw drones with pre-planned GPS-assisted flight routes and drone pilots steering the drones to hit valuable targets. While still an impressive display of cunning and strength, the execution of the drone phase was more simplistic than most had hoped for. However, in many ways, this made the operation more genius, daring, and worthy of appraisal now and in the future.

To be clear from the outset, this article does not aim to be yet another that points out that remotely piloted aerial platforms have existed since "forever" or that unmanned platforms are outdated technology. Neither will this article argue that drones are the key to successful warfare. Instead, it will say that we have at our fingertips today a lot of available technology in commercial stores that is waiting to be utilised in ways not originally intended when it was created. While we should strive towards the next technological breakthrough with AI-supported autonomous drone swarms and

similar innovations, we still have uncharted and underutilised areas of civilian technologies (often within the realm of hobbies) that can catalyse military innovations in the same way FPV drones have affected the battlefield in Ukraine. Instead of discussing history, let's discuss the opportunities of today.

> *The groundwork conducted by personnel on site was crucial for the operation even to be executed.*

With both Russian and Ukrainian units utilising community platforms like Discord, social media applications like Telegram, and open-source software like Betaflight and ExpressLRS (ELRS),[2] we have yet again been shown that a bottom-up process incentivised by the individuals' wish to survive and leave the battlefield victorious will use any tool that can aid them in achieving that goal. The attack on the Russian airfields and the strategic bombers is just another example confirming this.

Deconstructing the attacks on the airfields

This article will primarily focus on the technology used for the drones and how the Ukrainians can conduct their operations over such a great distance from home. The details about how SBU created a "front" with a truck company and managed to have covert operatives on site in Russia are outside the scope of this article. However, it must be said that drones alone could not have achieved the operation's goals. The drones are merely a means, a weapon, to be directed by humans, and the groundwork conducted by personnel on site was crucial for the operation even to be executed. As such, this article will not argue for drones (or open-source in general) as some "wunderwaffe," since drones have their fair share of problems;[3] it instead presents them as a tool that, with some clever thinking, has much potential when teamed up with other capable assets.

Much has been written about the attack and how it was conducted, particularly regarding the preparation of the operation, the transportation of all necessary equipment into Russia, and the assembly of the drones. To recap, it seems reasonably sure that all drones were smuggled into Russia in smaller parts, assembled in a warehouse and then placed into containers and small wooden houses to be transported to their target areas. The released imagery of the drones shows that every part has a number written on it, possibly to simplify the assembly process. When each truck reached its destination, which intelligence personnel may have overseen in some cases, the roof was removed, and the drones were activated remotely.[4] An activation that was likely done via the Russian cellular network. It is, however, possible that the activation was done according to a preset time, which could explain why some trucks never reached their destinations before exploding, although there could be several other reasons for that to happen. We can, however, be confident that the drones were remotely piloted through the cellular network, rather than through AI-assisted targeting, as shown in the videos released by the SBU. In later videos released on Russian telegram accounts, we are shown that inside the house, hidden in a cabinet, were communication modules mounted that use two SIM cards to connect to the internet and can act as a "hotspot" for other devices. The modules seem powered by batteries, or that the batteries were part of a reserve power system. The news reporting in the aftermath of the attack has not cov-

ered these details. Still, they are crucial to understanding how Ukraine could plan and execute this operation within the 18-month timeframe, given the distance that surpasses their conventional weapons.

> *Ukraine has been able to weaponise the drone hobby.*

Looking at the war, one could confidently state that Ukraine has been able to weaponise the drone hobby. We saw various DJI products used to reconnoitre Russian positions at the beginning of the Russian offensive in February 2022. In June that same year, we saw Ukrainian units use an FPV drone to strike a Russian position. Since then, various types of drones and associated (often free) software or hardware have been used to adapt to the ever-changing battlespace. The attack against the Russian airfields is no exception. It follows the same path as other successful Ukrainian ventures, such as integrating commercial Starlink on unmanned surface vessels (USVs) for added range and protection from jamming, or using Raspberry Pi[5] to build lightweight targeting systems.

The videos show clearly the graphical interface of the open-source software ArduPilot Mission Planner. ArduPilot is a popular open-source solution for autopilot functions for drones and hobby aircraft. It was founded in 2007, and the first compatible circuit board was released in 2009. The hardware required to use the autopilot function is commonly used in larger Ukrainian multicopters and has been in use since at least 2022; some sources indicate that it has been in use since the 2014 invasion of Ukraine. Ardupilot not only allows the operator to pre-plan a flight, but also enables them to define what the drone should do at every waypoint, allowing for the collection of imagery for an area without using radio or any other emitter. The software enables the operator to navigate using various sensors, such as LIDAR or "dead reckoning", when GPS is not available. For the price of free, the mission planner software is quite capable, even in a military setting when combined with cheap electronic components.

Looking at the videos from the operation, Ukraine did what the USA has been doing in the Middle East for a century when piloting their larger drones, like the Reaper, via satellite from Nevada, but with cheaper equipment and, instead of using SATCOM, relying on the Russian telecom system. The drones flew according to a previously defined path, and when they reached their final waypoint, they entered holding mode, waiting for the operator to take control. Judging from some of the videos, the drones flew more than six kilometres on their own, assisted by GPS. However, those drones that could not get a GPS fix were likely controlled from the start by a Ukrainian operator located inside Ukraine. The assigned pilot would then steer the drone towards an identified target, land on one of the identified weak spots on the airframes (either the wings of the Tu-95s or on top of the Tu-22s) and detonate the shaped charge housed in two cylinders on the drone.

> *If the Russians had denied access to GPS, that would not have been enough to stop the attack since the drones could operate without a GPS fix.*

By using available components on the market, specifically built for use with ArduPilot, Ukrainian operators could control their drones via the Internet and 4G/LTE,

exploiting a gap in the Russian airbase defence that was not prepared to jam mobile communications. Each truck likely acted as a relay, equipped to transmit video and commands through routers and modules specifically designed for industrial use.[6] Thus, if the Russians had denied access to GPS, that would not have been enough to stop the attack since the drones could operate without a GPS fix. Examining the antennas on the drone, it is possible that all drones used multiband GNSS antennas, which further complicates the challenge of effectively jamming all frequencies for all drones during the attack. This is a cautionary tale for others not to rely solely on jamming GNSS and radio frequencies when protecting infrastructure against drones, and highlights the need for airbases to quickly block all emitters in the vicinity of the base, including cell phone towers.

It should be noted that Russia has been experimenting with controlling small FPV drones in Ukraine from Moscow. In a video first published by Russian RIA Novosti in April, Russian operators in civilian clothes are shown controlling a drone in Ukraine through the "Orbita" system from a skyscraper in Moscow city. Although the video was later removed from the website, it was spread on social media and criticised by Russian bloggers for giving Ukraine a valid reason to target the skyscrapers in the city. Even if it was demonstrated to be used with FPV, it is plausible that the same solution could be applied to control other types of platforms remotely across all domains. Therefore, should this be considered a credible threat against us and our allies tomorrow, especially when the trend as of now seems to be to distance drone operators from the battlefield as a means to protect them since they have become high-value targets, at least by the Ukrainian point system that now awards 25 points for every killed Russian drone pilot. That can be compared to a tank that only awards the unit 8 points. Since 2022, drone operators have had to continuously adapt to the threat of being targeted, from disabling geotracking in DJI drones to digging themselves in and constructing antennas placed at a distance from their position. Antennas that are built to be harder to find both visually and in the electromagnetic spectrum. Utilising alternative communication protocols like 4G becomes one way of blending into the background noise in a war, where signals that stand out get hit by ordnance. Thus, systems like "Orbita" will likely become a standard capability.

> *Ukraine has been forced to find solutions outside of conventional thinking.*

Keeping it simple

Comparing the Ukrainian and the Russian solutions is probably not entirely correct. However, one must acknowledge the different approach to solving technological problems. Russia has a large military-industrial complex, which appears to influence the solutions it creates. On the other hand, Ukraine did not have a large military industry and, as such, has been forced to find solutions outside of conventional thinking. This author would argue that this is one of the key differences that Ukraine have been able to turn to their advantage in this war. While Russian units still can't be fully supplied with smaller drones through their logistics chain, having to rely on volunteers, Ukrainian units now have an official points system that enables them to obtain what they need or want to continue the fight in their designated area of

operations. This again is a lesson identified for other countries when adapting to a rapidly changing battlefield. It seems unlikely that the military-industrial complex will be agile enough to keep pace with the changes throughout the front. Instead, there is a need for a balance where the industry prioritises larger systems in the long term, while simultaneously allowing for rapid changes and experimentation with available commercial products in the short term.

> *It was, simultaneously, not simple because they had to gather over 100 pilots and ensure they could connect to their assigned drone, which was assembled in another location.*

It is also interesting to note that, long before the attack on the Russian airfields, Russian information existed about the Ukrainian tactic of activating pre-positioned drones with the help of cellular phones. It appears that the Russian security apparatus fell into the cognitive trap of believing the enemy could not conduct such an operation, based on how the Russians perceived their own capabilities. One could argue that the Russians fell into the same thinking as the democratic world when a Russian offensive into Ukraine in 2022 was ruled less likely to occur. It also shows that information warfare about the Ukrainians' capabilities and characteristics not only affects the Ukrainians, but also the Russians and how they perceive their enemy's ability to conduct sophisticated operations. Suppose you say your enemy is incompetent and unable to succeed in operations, and you never recognise them as having any success. In that case, given enough time, a cognitive anchor may hinder you from objectively assessing their real capabilities. The same is true when overestimating military power.

"Everything in war is very simple, but the simplest thing is difficult"[7] is a quote that is probably not unknown to the reader. The attack on the Russian airfields, if we limit ourselves to the drone operation, was both straightforward and not at the same time. It was simple because they utilised existing technology readily available on the market, which they could obtain quickly and affordably. It was also simple, as they would not have to train drone pilots to use unfamiliar software with unknown controls. It was, simultaneously, not simple because they had to gather over 100 pilots and ensure they could connect to their assigned drone, which was assembled in another location. While the pilots would know how to operate software and controls, they would have to adapt to controlling a drone with greater latency than usual, not forgetting the complexity in coordinating all drones and collecting all video feeds for exploitation. Ukraine kept it simple without advanced AI targeting or dedicated satellite communication, utilising the experience about drone operations already obtained during the war, which meant that they could focus on the logistical aspect of how to conduct a large-scale covert military operation on foreign soil.

Operational security (OPSEC) can also benefit from this type of simplicity when selecting equipment that can be purchased at a low cost from a hobby or electronics store, especially when purchasing various components in large quantities, such as motors and ArduPilot-compatible autopilots.[8] Gathering equipment for this type of operation would likely not stand out compared to procuring a unique, custom-built platform for this purpose.[9]

There is no end to the possibilities

In an era where many people discuss drone swarms and the potential for a single operator to control multiple drones, we must look to the past to see what has already been accomplished. In 2015, using the same type of software used in the Russian attack, an operator from the Advanced Robotic Systems Engineering Laboratory (ARSENL) at the Naval Postgraduate School, based in California, successfully flew 50 aircraft simultaneously for nine minutes and 45 seconds. Just launching all the drones took 27 minutes.[10] Imagine what we can achieve today, 10 years later, with smaller, more efficient, and sometimes less expensive components.

> *Every unit can now influence the equipment it receives based on its specific needs.*

Having access to the internet today also means having access to an infinite amount of knowledge. Encountering a problem is often no more than an inconvenience, since someone else has likely faced the same challenge, found a solution, and made a video on YouTube about it. The internet has brought the metaphor "standing on the shoulders of giants" to a new level. Nowadays, everyone can reach further, building on what others have learned and shared. This also means we have the conditions to learn quickly from ongoing conflicts worldwide today, not only in Ukraine and certainly not only about drones. For example, Marines from the United States Marine Corps have demonstrated that it is possible to build a spectrum analyser for use at the squad level for under $650, using parts purchased on Amazon.[11] The ability for units to buy parts and develop their own spectrum surveillance equipment represents a paradigm shift, not only for military procurement but also for how adaptable units can become in response to the ever-changing battlespace. Democratisation (or gamification) of war comes with decentralised warfare, where power is shifted from central command down to the lowest echelon. This means that every unit can now influence the equipment it receives based on its specific needs. Units can step outside the ordinary command and logistical hierarchy when necessary, as a means to enhance combat effectiveness and survivability.

Ukraine has not only been able to adapt open-source software and turn it into deadly weapons but also modify available software so that it fits into how Ukrainian units are fighting. One example is the adaptation of the ELRS firmware into MILELRS, which enables Ukrainian operators to better avoid Russian jamming by using multiple frequencies simultaneously (by connecting several transmitters and receivers in parallel), changing frequencies with the controller while flying, and protecting against cyberattacks.[12] It further proves that it is not the components that are critical for the survival of a system on the battlefield, but rather how adaptable the software is. The predicted demise of the drone, much like the "predicted" demise of the tank, has been disproven time and again thanks to the adaptability of open-source platforms; however, that ability to change hinges on the availability of programmers, or at least individuals that can write code with support from online knowledge sources.[13] People who know how to write code are in high demand, and as such, the armed forces may need to find ways to teach their personnel how to conduct basic programming even if it is not their primary speciality today. That ability may be the difference

in how adaptable and innovative the force can be tomorrow.

> *Ukraine continues to demonstrate that success can be achieved even with the most basic and widely available technology.*

Operation "Spider Web" did indeed mark a turning point, but not because of advanced technologies like AI but rather because of the lack thereof. In a global technology race where we often turn to large industrial complexes for war-winning solutions, Ukraine continues to demonstrate that success can be achieved even with the most basic and widely available technology, as long as it can be adapted to existing conditions and demands.

Being blinded by the halo of AI

When the news of the attack spread throughout social media and news outlets, the initial narrative was that the drones were guided by AI and had been trained using photographs from a museum. From the videos shown, there is very little, if any, evidence supporting that conclusion. The narrative spread seems to be an equal part of information warfare and wishful thinking. Ukraine has demonstrated exceptional talent in information warfare, ensuring that all technological breakthroughs, including AI, are effectively communicated to the world to influence Russian soldiers and countries' willingness to support the Ukrainian defence. With that in mind, we must note that SBU has not mentioned any use of AI or machine learning to target specific airframes. That statement was made by the Turkish social media account

The responsibility of our personnel is to continually try new ideas or reinvent old ones. Photo: Joel Thungren, Swedish armed forces.

"Clash Report" without giving a source.[14] Instead, SBU has mentioned that if the link between the operator and the drone were lost, the drone would automatically follow a predefined path, which is not the same as having AI.[15] ArduPilot and the mission planner enable the operator to plan a flight path and specify the drone's actions upon reaching a specific waypoint.[16] As such, it is possible that the drones had endpoints where previous gathered intelligence said a bomber would likely be parked. Thus, giving the drone the command to land on that coordinate and then self-destruct would be possible.

A procedure that looks like AI or machine learning to an observer. There may be a cultural difference in what constitutes AI and what does not between countries within NATO, on the one hand, and Ukraine and Russia, on the other. AI is a catch-all term that incorporates different levels of autonomy and algorithms.

> *The risk of being blinded by the "AI halo" is that we miss straightforward solutions available today for less sophisticated platforms.*

The risk of being blinded by the "AI halo" is that we miss solutions like the one described above—more straightforward solutions available today for less sophisticated platforms. It also means that we risk misjudging capabilities and thus what actions we need to take to protect ourselves. This might result from our subconscious desire for AI-empowered drones that can act autonomously and strike an enemy deep behind the front lines, as well as our wish for Ukraine to prevail. We cannot ignore that bias when preparing for the next war, since preparation is not about developing and buying military technology. It is also about preparing a mindset that seeks unconventional solutions and sometimes turns scrap into gold.

So what?

To conclude this article, the attack against Russian airfields in June was far less technologically sophisticated than some first thought. That is probably why it worked so well even without AI. Ukraine has demonstrated that almost all technology can be weaponised in war, and with an effective chain of command, technology can be refined and remain relevant for a long time. To achieve the same level of fast-paced development of disruptive technologies, we cannot only tell our personnel to be more innovative, but we also need to train them accordingly and provide them with the conditions to thrive in training, whether through exercises or resources. That responsibility lies with commanders and staff, while the responsibility of personnel is to continually try new ideas or reinvent old ones. Then we are more likely not only to do what Ukraine managed to do but also to protect ourselves against such an attack.

The author is a Master Sergeant in the Swedish Armed Forces.

Notes

1. Gozzi, Laura: "How Ukraine carried out daring 'Spider Web' attack on Russian bombers", *BBC*, 2025-06-02, *https://www.bbc.com/news/articles/cq69qnvj6nlo*, (2025-06-28).
2. Betaflight is a configuration software for a wide range of flying platforms used by RC-hobbyists. ExpressLRS is an open-source firmware that is used to communicate with the drone over radio. Both can be modified by a user with knowledge in programming.
3. Jajcay, Jakub: "I Fought in Ukraine and Here's Why FPV Drones Kind of Suck", *War on The Rocks*, 2025-06-26, *warontherocks.com/2025/06/i-fought-in-ukraine-and-heres-why-fpv-drones-kind-of-suck/*, (2022-06-28).
4. "СБУ буде бити ворога там, де він вважає себе недосяжним, – Голова СБУ Василь Малюк про спецоперацію «Павутина» (відео)", *ssu.gov.ua*, 2025-06-11, *https://ssu.gov.ua/novyny/sbu-bude-byty-voroha-tam-de-vin-vvazhaie-sebe-nedosiazhnym-holova-sbu-vasyl-maliuk-prospetsoperatsiiu-pavutyna-video*, (2025-06-28).
5. Raspberry PI builds low-cost micro computers which can be modified and built into a wide spectrum of technological solutions. From "do it yourself" SIGINT applications to AI targeting in drones.
6. BOMBs&UAV: "More details on 'Operation Spider Web' Each UAV was equipped with two 'cutting charges', using shaped charges initiated by two parallel-wired detonators. The comm setup relied on LTE utilizing the Russian cellular network, with a Teltonika RUT956 module", *X*, 2025-06-25, *https://x.com/eran_salmon/status/1936962058093809698*, (2025-06-28).
7. von Clausewitz, Carl: *On war*.
8. A common ArduPilot-compatible autopilot found in Ukrainian "Baba Yagas" is the Cube Orange+.
9. It should be noted that available imagery indicates that the drone used for the attack was Osa, commercially built by the Ukrainian company First Contact. However, it is unclear if the company built the modified drones used during the operation or if SBU bought and modified the drones themselves.
10. Clement, Mike: "From Zero to Fifty Planes in Twenty-Seven Minutes", *DIY Drones*, 2015-09-03, *https://diydrones.com/profiles/blogs/from-zero-to-fifty-planes-in-twenty-seven-minutes*, (2025-06-27).
11. Sher, Lucas: "Spectrum Danger Zones: How To Build and Employ a Grunt Friendly Analyzer", *The Connecting File*, 2024-09-24, *https://thecxfile.substack.com/p/spectrum-danger-zones-how-to-build*, (2025-06-27).
12. Removing the binding phrase function. A binding phrase works like a password that can be used to create a connection between a controller and a FPV drone.
13. Mitchell, Brandon: "FPV Drones BUILT in DONBAS: Realtime WarFare Collaboration. Production to Front!", *Youtube*, 2025-03-30, *https://www.youtube.com/watch?v=TYEwD4oFyIs*, (2025-06-28).
14. Clash Report: "EXCLUSIVE: Ukraine trained AI targeting algorithms using Soviet aircraft displayed in military museums. Poltava Museum of Long-Range and Strategic Aviation has both Tu-95MS and Tu-22M3", *X*, 2025-06-01, *https://x.com/clashreport/status/1929179925329641862*, (2025-06-20).
15. Служба безпеки України, Telegram, 2025-06-04, *https://t.me/SBUkr/14965*, (2025-06-28).
16. "Camera Control in Auto Missions", *ardupilot.org*, *https://ardupilot.org/copter/docs/common-camera-control-and-auto-missions-in-mission-planner.html*, (2025-06-28).