

Chinese Military Experts on the Spiderweb Assault: How Ukrainian Drones Evaded Russia's Air Defenses

OPINION

Insiders from Ukraine's Security Service say the "Spiderweb" operation destroyed 41 Russian strategic bombers. Chinese military experts agree that once-overlooked drones now play a key role on modern battlefields. The rising threat from many low-end drones to high-value targets contrasts with the limited defenses available. Why is defending against these small drones so difficult?

June 4, 2025

The Challenge of Early Detection

After careful planning, Ukraine's Security Service launched a drone strike on several Russian strategic bomber bases on June 1. According to Ukrainian sources, up to 117 drones were launched directly from truck compartments parked near the bases, targeting unsuspecting bomber fleets. Chinese experts interviewed by the Global Times noted that this indicates a key challenge in drone defense: early detection is becoming "increasingly difficult."



Fiber-Optic Guided Drones

Multirotor drones are considered classic examples of "low, slow, and small" targets. They fly at low altitudes, often below the coverage of traditional air surveillance radar; they travel slowly and unpredictably, making them easy to overlook by radar systems designed to detect large aerial threats; and due to their small radar cross-section and the clutter generated by ground interference, spotting them from long distances is inherently difficult.

To counter this kind of threat, many countries have developed low-altitude surveillance radars specifically aimed at detecting small drones. These systems typically operate on higher-sensitivity radio frequencies and use optimized algorithms to differentiate micro and mini drones from other echo signals and ground clutter; thus enhancing detection capabilities. Counter-drone radars must also be mobile to allow for rapid deployment. At the "Army 2024" International Military-Technical Forum, Russia showcased several models of such systems.

However, interviews with Global Times reporters revealed that anti-drone radars face additional challenges in real-world conditions. Terrain, forests, or buildings can obstruct detection, and radar effectiveness varies with different types of aerial targets. Detecting "low, slow, and small" objects generally requires higher radar sensitivity, which in turn increases the rate of false alarms. Today's more effective drone detection typically combines multiple technologies—deploying radars across different frequency bands, supported by optical, infrared, and acoustic sensors. These inputs are then integrated and filtered through advanced algorithms to isolate suspicious targets.

Such comprehensive systems are better suited to defending fixed, high-value installations. In field environments, however, their complexity and the quantity of equipment required make deployment more difficult. Moreover, temporary setups in rugged terrain can lead to detection blind spots. The effective range of these systems is also limited, often only 5 to 10 kilometers or less, allowing hostile drones to bypass them with relative ease.

Experts also noted another critical advantage of multirotor drones demonstrated in the Ukrainian attack: their ease of concealment and transport. The Security Service of Ukraine reportedly pre-positioned large numbers of FPV (First Person View) drones inside wooden compartments within truck cargo holds on Russian territory. These trucks were then parked near the Russian military bases, effectively enabling the drones to approach undetected and take off "right under the Russians' noses"—something no radar system alone could have prevented. Experts emphasized that early and accurate detection is essential to drone defense, but in this operation, Ukraine's use of camouflage and concealment severely compressed Russia's detection and interception window.

It is worth noting that the U.S. military faces similar challenges. On June 2, The War Zone section of The Drive reported that in recent years, Langley Air Force Base in the U.S. and numerous overseas installations have experienced multiple "unidentified drone intrusion" incidents. Pentagon investigations suggest that these drones may have taken off from nearby buildings or vessels, but due to "a tangled web of legal oversight and other constraints," the U.S. military has been unable to prevent such incursions.

Autonomous Navigation Undermines Soft-Kill Measures

According to information obtained by the Global Times, when an unidentified drone is detected approaching, the defending side typically chooses different countermeasures depending on the nature of the target. Traditional responses have largely focused on soft-kill techniques, such as radio frequency jamming and signal spoofing. For example, most multirotor drones rely on specific communication frequencies to maintain contact with their human operators. Counter-drone systems can detect and disrupt these frequencies, breaking the link between the drone and its controller, or transmitting false commands to cause the drone to malfunction. Some drones, however, are pre-programmed to follow fixed flight paths without real-time communication; for these, defenders may attempt to deceive them by transmitting fake satellite navigation signals, leading them off course. In an interview with Business Insider, a Ukrainian frontline drone operator admitted that Russian forces have deployed a large number of high-power radio jamming devices, which significantly affect the performance of Ukrainian drones.



Ukrainian soldiers operating drones

Since last year, however, the Russia-Ukraine conflict has seen the growing use of fiber-optic-guided drones. These drones represent a major shift by eliminating the need for radio communication. Instead, they carry a spool of fiber-optic cable onboard, which unreels during flight to maintain a physical connection with the operator. Because all command signals are transmitted internally through the fiber rather than via external radio emissions, these drones are extremely resistant to jamming and difficult to detect. According to Ukrainian sources, fiber-optic-guided drones have rendered traditional soft-kill methods largely ineffective; they can even pass directly over electronic warfare vehicles to pursue and destroy tank targets. Additionally, because fiber-optic data transmission offers much higher bandwidth than radio frequencies, these drones can deliver stable real-time video feeds, allowing for precise strikes on designated targets. Both Russian and Ukrainian forces are increasingly deploying this type of system.

Nevertheless, fiber-optic drones have limitations. Their effective range is typically constrained to 10-20 kilometers, depending on the length of the cable carried. The fiber itself is vulnerable to being severed by obstacles, requiring skilled operation and making such drones unsuitable for dense environments like forests or shrublands.

Notably, reports indicate that some of the Ukrainian drones used in the June 1 operation were equipped with the open-source autopilot software ArduPilot, allowing them to autonomously identify and engage Russian bombers. The "War Zone" section of The Drive reports that with the advancement of artificial intelligence and machine learning, drone threats are escalating rapidly. AI-enabled drones exhibit self-navigation and targeting capabilities that can evolve through fast iterations—operating without any human input. These drones do not require real-time communication with human operators, are immune to external jamming, and emit no detectable radio signals that would reveal their presence. Furthermore, they are not constrained by the limits of radio control or fiber length, and can dynamically engage moving targets without relying on satellite navigation, thereby increasing the complexity of drone threats and making them significantly harder to counter.

The report cites Major General Paul Spedero, Vice Director for Operations on the U.S. Joint Staff, who recently warned during a congressional hearing on drone threats, unmanned aerial systems have evolved from being remotely operated via radio to becoming autonomous platforms that may no longer even rely on GPS. This will make interception significantly more challenging.

The Shortcomings of Hard-kill Measures

Videos circulating on social media show that during Ukraine's drone strike on the Russian military base in Sredny, Irkutsk Oblast, several local men climbed onto the roof of a truck, attempting to throw stones to shoot down or stop drones from taking off. Some witnesses reported that Russian personnel tried to shoot down the drones using small arms. On June 2, Irkutsk Governor Kobzev stated that these men would receive rewards.

Experts noted that these actions by Russian civilians can generally be categorized as hard-kill counter-drone methods. Currently, there is a wide range of hard-kill options available against drones—from traditional firearms and anti-aircraft autocannons to surface-to-air missiles and precision-guided rockets, as well as directed energy weapons like lasers and high-power microwaves. Most of these have already been deployed in combat or are undergoing testing. However, firearms and autocannons are limited in range and accuracy, making them largely ineffective at neutralizing drones. While surface-to-air missiles have high success rates, they are prohibitively expensive, often costing tens or even hundreds of thousands of dollars per missile—far exceeding the price of a multirotor drone. Countries such as Russia, the United States, and Israel are now developing and fielding new generations of precision-guided rockets in hopes of using these more cost-effective weapons to intercept drones flying on fixed routes.

Directed energy weapons like lasers and high-power microwaves are particularly attractive because they rely only on electricity and have extremely low operational costs. However, these technologies are still not fully mature. For instance, current laser weapons often lack the power to instantly disable a drone and must maintain a focused beam on the target for several seconds to achieve a kill, making them ineffective against swarms or rapid attacks. In this recent strike by Ukrainian drones on Russian strategic bomber forces, the damage was significant. Although Russia and Ukraine have offered differing accounts of the extent of the losses, available footage confirms that strategic bombers parked in the open are highly vulnerable to multirotor drones carrying explosives. Several U.S. media outlets noted that American B-52 and B-1B strategic bombers are also parked outdoors, meaning they could face similar vulnerabilities if subjected to such drone attacks.

Beyond the battlefield, both the United States and Russia are also facing increasing challenges in countering drones in urban environments. According to The War Zone section of The Drive, the Pentagon stated during its "Falcon Talon 2025" military counter-drone trials held in October 2024 that "current technologies like lasers, microwaves, surface-to-air missiles, and firearms are not viable options for eliminating drones within U.S. territory." Major Russian cities, including Moscow, have also experienced multiple drone attacks in the past. Experts point out that counter-drone operations in cities face numerous constraints. In addition to the monitoring challenges posed by complex urban terrain, the high density of people and infrastructure makes it difficult to implement countermeasures. For example, soft-kill methods such as GPS spoofing and electronic jamming involve the emission of high-power electromagnetic signals, which may interfere with nearby civilian electronic systems. Meanwhile, hard-kill options like firearms or missiles pose risks of collateral damage; falling drone debris could also harm people or facilities on the ground.

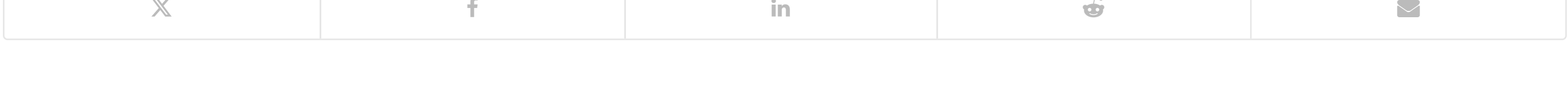
Additionally, Business Insider reported that the development of swarm-intelligent drones may pose an even greater threat in the future. These systems can autonomously assign tasks and react with extreme speed—faster than a human decision-making cycle. When combined with large numbers and flexible mission planning, they have the potential to quickly overwhelm any defense system.

Editor: LQQ

References

<https://mil.huanqiu.com/article/4Mwqey5inbt>

Share This Post



Comments

Latest Popular

You must be logged in to post a comment.

Raymond Li
Be wary of all newish tech being weaponized in these world order changing times ⚠️

0 Log in to reply