# Silence in the Skies: How Asymmetric Passive Air Defense Is Testing Western Airpower?

**By Syed Raza Abbas**

On March 19, 2026, an American F-35A took off on a combat mission over central Iran and was not able to return to base. It diverted mid-mission, landed under its own power at another U.S. base in the Middle East, and the pilot walked away in stable condition. What caused it is still contested Iran's Revolutionary Guard released footage it says shows the strike; Washington has not confirmed the cause; independent analysts remain divided. But if the Iranian account holds up, one of the most expensive aircraft ever built was hit by a truck-mounted missile system that costs a rounding error of its price tag, using a method that should not have worked against it.

That single incident, whatever eventually gets confirmed about it, points at something larger than one jet. For nearly half a century, Western air doctrine has rested on a simple sequence: find the enemy's radars, blind or destroy them, and then own the sky. Once Iran's long-range systems the Russian-supplied S-300, the indigenous Bavar-373 were degraded by early strikes, the assumption in Washington and Tel Aviv was that the rest would follow the sequence. No radar, no defense, open airspace.

It didn't play out that way. Iran didn't rebuild what it lost. It built something different.

**The Problem with Traditional Air Defenses**

Heavy, radar-based air defense has always carried a built-in vulnerability: to see, it has to announce itself. An early warning radar spinning up to track an incoming aircraft works like a flashlight in a dark room it lets the defender see, but it also tells every enemy sensor exactly where to look. Strike aircraft carrying anti-radiation missiles can home in on that signal and take the site out.

There's a cost problem here too, and it favors whoever is attacking. A single long-range interceptor can cost several million dollars, but it's often used against a cheap drone or a standoff munition worth a fraction of that so every intercept quietly loses money even when it succeeds. And because these systems are built around a handful of central radar hubs, taking out just those hubs does minimize the damage: it doesn't just remove a few sensors, it blinds and isolates every battery that depended on them, leaving the rest of the network easy to destroy piece by piece.

The pattern is visible in Iran's own experience over the past two years. In October 2024, Israeli strikes destroyed Iran's remaining long-range S-300 radars and detection systems in a single coordinated operation, and a senior White House Middle East advisor was reported at the time to have described Iran's air defenses as effectively stripped bare. It wasn't that Iran lost dozens of

individual weapons in that strike, it lost the radars that let the rest of the network see, which was enough to knock the whole layer out of the fight at once. By April 2026, Israel was still picking off individual S-300 batteries that had survived or been rebuilt, each strike costing Israel a single precision munition against a system that had taken Iran a billion-dollar deal with Russia to acquire in the first place. That asymmetry cheap to destroy, expensive to replace, catastrophic to lose the radar hub that ties it together is exactly the vulnerability the shift toward passive, decentralized sensing was designed to route around. The working assumption in Western planning was straightforward: kill the radar, and the ground defense underneath it stops mattering.

**What Iran Built Instead**

With its industrial base and radar networks under sustained attack, Iran reportedly leaned into a lower-tech, harder-to-kill alternative: passive sensing, spread wide instead of being concentrated. The idea borrows from what's been observed in Ukraine, where networks of ordinary microphones have been used to track drones by sound. Iranian planners are said to have pushed the same logic into cameras and thermal sensors.

The reported architecture rests on three pieces: commercial cameras and military-grade infrared sensors watching key approach corridors, acoustic posts listening for engine signatures at low altitude, and local processing hubs using machine learning to fuse it all into something resembling a live picture without a single radar pulse going out.

The appeal, on paper, is straightforward. A thermal camera emits nothing, so there's no signal for a jamming pod or an anti-radiation missile to lock onto. Software can now stitch together dozens of ordinary camera feeds into a coherent picture in a way that wasn't practical a decade ago. Destroying one $2,000 sensor barely dents a network built from hundreds of them a very different math than losing a single radar that anchored an entire sector.

**The Majid and the Stealth Question**

The system most associated with this shift is the **Majid (AD-08)** a short-range, truck-mounted platform that skips radar entirely, relying on thermal and electro-optical tracking paired with heat-seeking missiles. It's a modest piece of hardware: an eight-kilometer engagement range, a small fragmentation warhead, built for close-in ambush rather than area defense.

What makes it relevant to a conversation about F-35s is a simple physical fact: no airframe, however well shaped to scatter radar, can hide its heat. Air Friction and engine exhaust generate a thermal signature that stealth geometry does nothing to address. If Iranian forces were tracking aircraft through heat signature rather than through radar, a pilot's warning receiver built to detect radar illumination would have had nothing to alert on. That's the scenario Iran says played out on

March 19: no lock warning, no jamming, just a missile arriving from a system the aircraft was never designed to hear coming.

It's worth being honest about what's actually confirmed here and what isn't. The damage to the F-35 is confirmed. The pilot's safety is confirmed. The Majid system as the cause is Iran's claim, amplified by outlets sympathetic to that narrative, and not something U.S. officials have verified on the record. Readers should treat the attribution as plausible and consistent with the system's known capabilities not as settled fact.

**Why It Matters Even If the Details Are Still Fuzzy**

Even bracketing the attribution question, the broader pattern is real and worth taking seriously. For smaller and mid-sized states, the old choice was brutal: spend a fortune on top-tier radar-based air defense, or accept that a technologically superior air force could open your airspace within days. A passive, distributed, AI-assisted sensor network built substantially from commercial parts offers something in between: not air superiority, but the ability to make the other side pay for every sortie.

That changes the math for planners on both sides. Suppression of enemy air defenses has historically meant finding radar towers and jamming frequencies. You can't jam a camera, and you can't easily map a processing hub sitting in a basement, miles from the fight. None of this makes stealth aircraft obsolete, and none of it means Iran has found a way to contest the skies outright the F-35 in question flew again. But it suggests that the gap between what a billion-dollar air force can do and what a determined, resource-poor defender can survive may be narrower than the last thirty years of uncontested Western air campaigns led people to assume.

The people who have to plan the next air campaign, and the pilots who have to fly it, are the ones who'll find out how much narrower.