

Photo: EDM4S drone jammer, Ukraine's 28th Mechanised Brigade · CC BY 4.0 · Wikimedia Commons

OSINT · THREAT ASSESSMENT

WHEN JAMMING STOPS WORKING

For most of the drone war, electronic warfare was the default defence: find the control frequency, flood it, and the drone falls or flies home. That assumption is breaking down, in Ukraine's trenches, over a Belgian air base and on a German airport apron. This report sets out the four ways drones now slip past jammers, and what that means for anyone who relied on them.

REPORT DETAILS

PUBLISHED	SUBJECT	SOURCE BASE
October 2026	How drones evade jamming, and what that means for counter-drone defence	Ukrainian frontline accounts, government statements, RSF safety guidance, U.S. federal guidance, incident records
METHOD	**VERDICT**	**CONFIDENCE**
Group evasion methods by the control link they remove or disguise	Detection that does not depend on the drone's radio link is now essential	Moderate
AUTHOR		
Ghulam Mujtaba, Ph.D.		

BOTTOM LINE

Jamming works by attacking a drone's radio link, and the drones that matter most are learning to do without one. In Ukraine, one electronic-warfare company's jammers went from one module to seven during 2024 as Russian drones spread across frequencies, and then fibre-optic drones arrived with nothing to jam. Over Belgium's Kleine-Brogel air base in 2025, a jamming gun fired at a drone failed to bring it down. At Leipzig/Halle airport in 2026, a drone controlled over the mobile network reportedly looked like an ordinary phone to the anti-drone system. Ukraine's Operation Spiderweb showed drones finishing their attacks with onboard target recognition when links dropped. Jamming still defeats many drones, but a defence built around it now has predictable holes, and closing them needs detection that does not depend on the radio link.

1 → 7

JAMMER MODULES ONE UKRAINIAN UNIT NEEDED DURING 2024

◆ AS DRONES SPREAD ACROSS FREQUENCIES

25–30 km

FIBRE-OPTIC SPOOLS IN UKRAINIAN PRODUCTION

◆ 50 KM EXPERIMENTAL

0

RADIO LINKS TO JAM ON A FIBRE-OPTIC DRONE

◆ DETECTABLE ONLY BY SIGHT OR SOUND

KEY QUESTIONS

Why doesn't jamming stop all drones?

A jammer works by drowning out a drone's radio control link. Drones steered through a fibre-optic cable have no radio link to jam, drones on mobile networks look like ordinary phones, and drones with onboard autonomy can finish an attack after the link is lost.

Can fibre-optic drones be jammed?

No. They are controlled through a physical cable, so there is no radio link to block. Reporters Without Borders' 2026 safety guide says electronic warfare is ineffective against them and that they can only be detected by sight or by sound.

THE RULER — THE WHOLE ARGUMENT

Four ways round the jammer

METHOD	WHAT IT DOES TO THE RADIO LINK	SEEN WHERE
FREQUENCY SPREAD MORE BANDS	Spreads control across many frequencies, so jammers must cover them all	Russian FPVs in Ukraine, 2024
FIBRE-OPTIC CONTROL NO RADIO NEW	Replaces the radio link with a cable	Both sides in Ukraine; Kramatorsk 2025
MOBILE-NETWORK CONTROL HIDDEN IN PLAIN SIGHT	Uses SIM cards, so the drone looks like a phone	Leipzig/Halle 2026; Poland 2025; reportedly Spiderweb 2025
ONBOARD AUTONOMY LINK OPTIONAL	Finishes the attack after the link is lost	Spiderweb 2025; machine-vision FPVs

METHOD	WHAT IT DOES TO THE RADIO LINK	SEEN WHERE
THE COUNTER DETECT THE DRONE ITSELF	Ignores the radio link and listens for the rotors every control method still needs	DroSonic's approach; field-tested at DIRT Days 26.04, 2026

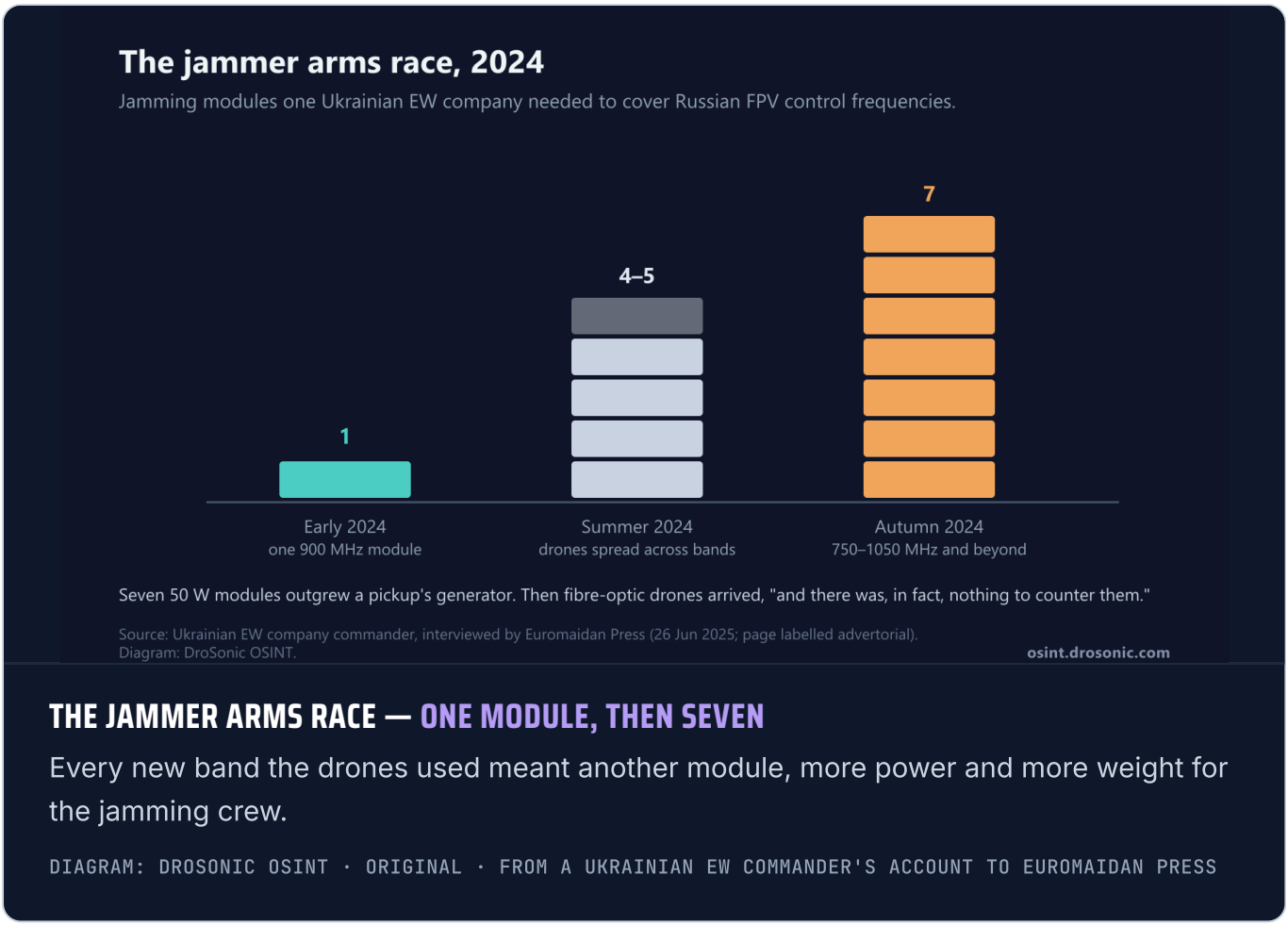
REMOVES THE RADIO LINK ENTIRELY · SOURCES BELOW

FIELD 01 — THE ARMS RACE

From one module to seven

A frontline account from Ukraine shows how fast the jamming contest moved. Senior Lieutenant Ihor Shutyi, who commands an electronic-warfare company, told Euromaidan Press that a single 900 MHz jamming module was enough until spring 2024. As Russian FPV drones spread across 750–1050 MHz and beyond, his unit needed four to five modules by summer and seven by autumn. Seven 50-watt modules outgrew a pickup truck's generator. Then came fibre-optic drones, against which "there was, in fact, nothing to counter them." EW, he said, is "gradually losing the battle against frontline quadcopters." Euromaidan Press↗ The article is labelled as advertorial; we use it for the commander's first-hand account.

A 2024 study of the war by the Center for Security Studies at ETH Zurich draws the general lesson. Jammers mounted on vehicles or carried in backpacks need enough power and cover only a narrow part of the spectrum, so an attacker can defeat them by putting each drone on a different frequency; and jamming can also disable friendly drones on the same bands. CSS, ETH Zurich↗



THE JAMMER ARMS RACE — ONE MODULE, THEN SEVEN

Every new band the drones used meant another module, more power and more weight for the jamming crew.

DIAGRAM: DROSONIC OSINT · ORIGINAL · FROM A UKRAINIAN EW COMMANDER'S ACCOUNT TO EUROMAIDAN PRESS

FIELD 02 — NO RADIO

The fibre-optic drone

A fibre-optic drone trails a hair-thin cable to its operator and sends nothing through the air. Ukrainian manufacturers have put 25–30 km spools into production, with 50 km still experimental. [Taifun↗] Reporters Without Borders' 2026 safety guide for frontline journalists puts the consequence plainly: electronic warfare is ineffective against these drones, and they can be detected only visually or by sound. [RSF guide↗] Russia has used them against cities well behind the front, including Kramatorsk in October 2025. [Euromaidan Press↗] Our report When the Detector Stays Silent looks at how they can still be heard.



A FIBRE-OPTIC FPV — THE CABLE IS THE LINK

The thin line trailing from the spool is the entire control link. There is nothing in the air for a jammer to hit.

PHOTO: ARMIYAINFORM · CC BY 4.0 · WIKIMEDIA COMMONS

FIELD 03 — HIDDEN IN PLAIN SIGHT

Drones on the phone network

The second route round the jammer is to use a link the defender cannot simply block: the mobile network. At **Leipzig/Halle Airport** in August 2026 (covered in Closed on a Sighting), the explosive-laden drone reportedly used a SIM card for remote control, which made it look like an ordinary mobile phone to the airport's anti-drone system. The system reportedly failed to detect it. Wikipedia↗ Some of the Russian decoys that crossed into **Poland** in September 2025 carried Polish SIM cards. Wikipedia↗ Jamming a mobile network near an airport or a town would cut off everyone else's phones too.

Even conventional radio drones can defeat a handheld jammer. Over **Kleine-Brogel** in November 2025 (one of the incidents in Watching the Bases), Belgian soldiers fired a jamming gun at a drone and failed to disable it; the defence minister suggested a frequency mismatch or range. Euromaidan Press↗

FIELD 04 — LINK OPTIONAL

When the drone finishes the job alone

The third route is to make the link unnecessary at the end. In **Operation Spiderweb** on 1 June 2025, Ukraine's security service launched quadcopters from trucks near Russian airbases thousands of kilometres from Ukraine. According to reporting compiled on the operation, the drones ran open-source ArduPilot software and used AI-based automatic target recognition to cope with communication delays and signal loss; an analyst suggested they also used SIM cards over mobile networks. Wikipedia↗ RSF's guide warns journalists about the same capability on the front line: drones with machine vision can lock on and complete the final phase of an attack even if the link is lost. RSF guide↗

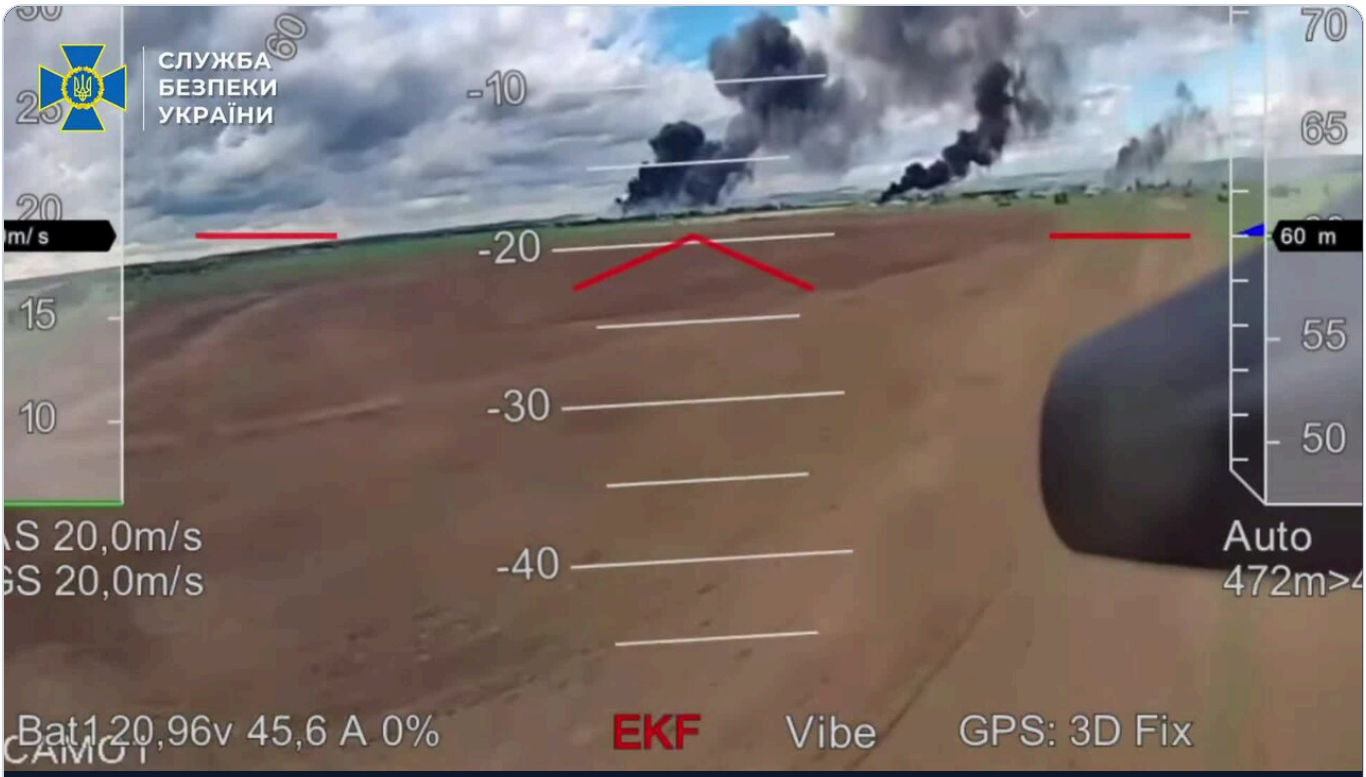
The trend predates Spiderweb. In September 2023 Ukraine's Defence Ministry approved the Saker Scout, a drone that recognises enemy equipment on its own, even under camouflage, and uses inertial guidance to resist electronic warfare. Euromaidan Press↗ The ETH Zurich study spells out what that means for defenders: as autonomous operation becomes the norm, "there will be no transmissions between the drone and its operator to jam or spoof." CSS, ETH Zurich↗



SPIDERWEB, 1 JUNE 2025 — "FAILSAFE" ON THE SCREEN

A frame released by Ukraine's security service from a drone striking a Tu-95 at Olenya. The on-screen display reads "FAILSAFE", the flight-controller mode for a lost or degraded link, as the drone reaches its target.

IMAGE: SECURITY SERVICE OF UKRAINE · CC BY 4.0 · WIKIMEDIA COMMONS



VIDEO: PLAY IT IN THE ONLINE REPORT

SPIDERWEB — ONE DRONE, LAUNCH TO IMPACT

Footage released by Ukraine's security service following one FPV drone from its launch off the roof of a modular building to its strike on a Tu-22M3 bomber at Belaya airbase. The drone crosses open country and enters the airfield unopposed. About two minutes.

VIDEO: SECURITY SERVICE OF UKRAINE · CC BY 4.0 · WIKIMEDIA COMMONS

> **A jammer fights the link.** Fibre, phone networks and autonomy each take the link out of the fight.

FIELD 05 — THE LEGAL LIMIT

Who may jam at all

In the United States there is a further constraint: almost nobody may jam. The 2020 federal interagency advisory notes that jamming and spoofing should be evaluated against federal criminal laws, including aircraft sabotage provisions, and are "likely to implicate laws relating to the RF spectrum."[U.S. DOJ, FAA, DHS & FCC↗] Mitigation authority rests with certified government agencies; our report Allowed to Listen, Not to Shoot covers who they are. For airports, utilities and other private sites, jamming is not an option, and passive detection is the part of the chain they can control.

CONFIDENCE

How sure we are, and what would change it

High confidence that fibre-optic drones cannot be jammed and that mobile-network control defeats link-based detection; both follow from how the links work and are confirmed in multiple sources.

Moderate confidence in specific accounts: the Ukrainian EW commander's figures come from a single interview on a page labelled advertorial; Spiderweb's control methods are reported by analysts, not confirmed by Ukraine in full; Leipzig's detection failure is reported, not officially confirmed.

What would change it: affordable counters to fibre-optic drones that work through the cable, or published evidence that link-based detection catches mobile-network drones reliably.

DROSONIC — OUR APPROACH

Nothing to jam, something to hear

Every route round the jammer in this report removes or hides the radio link. None removes the propellers. DroSonic's sensors are passive microphones whose detection runs on low-cost edge hardware, so they need no clear spectrum and transmit nothing for an adversary to find or jam.[DroSonic↗] Its founder's September 2026 presentation at NDIA's Emerging Technologies for Defense conference was on passive acoustic detection and cueing of fibre-optic and radio-silent drones.[DroSonic↗]

Detection is only half the answer when jamming fails; the other half is handing the drone to something that can still stop it. DroSonic's U.S. provisional patent application, filed in September 2026, covers that step as tiered defeat cueing, alongside detection, classification and localisation.[DroSonic↗] The cue can go to a gun crew, an interceptor drone or a camera, whichever the defender has.

CLOSE — WHAT IT MEANS

Detect the drone, not its radio

Jamming is not obsolete. It still defeats large numbers of radio-controlled drones and will stay in every counter-drone kit. What has changed is that the most dangerous drones are designed to get around it, by flying on a cable, using the phone network or finishing the attack on their own. A defence that first has to find a drone's radio link will miss those drones.

The answer is detection that senses the drone itself. Radar and cameras do that within their limits; passive acoustic detection does it for the small, low drones that radar and RF find hardest, by hearing the propellers that no control method can silence. At DroSonic that is the gap we are closing. In September 2026 a DroSonic prototype was tested against live drones at DIRT Days 26.04, a field exercise supported by CMI2 with U.S. Central Command and U.S. Army DEVCOM and set up to resemble a contested electronic battlefield. DroSonic↗



DIRT DAYS 26.04 — LISTENING WHERE THE RADIO WAR IS LOUD

DroSonic's test position at a field exercise built to resemble a contested electronic battlefield. A microphone needs no clear spectrum to work.

PHOTO: DROSONIC · FIELD-TEST WRITE-UP

ABOUT DROSONIC

DroSonic builds passive acoustic drone detection: networked sensors that listen for drones instead of their radio signals, using acoustic AI and edge computing. DroSonic OSINT is our open-source research into the threat that technology is built to meet.

THE RECORD SO FAR

OCT 2026	Joined the SOF RACER consortium, which connects USSOCOM with commercial technology companies
SEPT 2026	Prototype tested against live drones at DIRT Days 26.04, a field exercise supported by CMI2 with U.S. Central Command and U.S. Army DEVCOM
SEPT 2026	Technical presentation at NDIA's Emerging Technologies for Defense conference on detecting fibre-optic and radio-silent drones
SEPT 2026	Filed U.S. provisional patent 64/148,522 on passive acoustic detection, classification, localisation and defeat cueing
JUL 2026	Pitched to the U.S. Space Force at Space Systems Command's Reverse Industry Engagement Day, Colorado Springs

How DroSonic detection works → · Where it is used → · Talk to the team →

THIS REPORT ONLINE

https://osint.drosonic.com/assessments/drone-jamming-limits.html

Cite as: Mujtaba, G. (2026, October 20). *When Jamming Stops Working: Why Drone Jamming Fails*. DroSonic OSINT. https://osint.drosonic.com/assessments/drone-jamming-limits.html

Reusing this report. Text and original diagrams © DroSonic. You may quote this report and share its link with credit to DroSonic OSINT; to republish it in full, reuse our diagrams or use it commercially, contact us first. Photos and third-party figures keep the licences shown in their credits.

DroSonic OSINT: open-source assessments on drones and counter-UAS from DroSonic, passive acoustic drone detection. drosonic.com · sudo@drosonic.com



ABOUT THE AUTHOR

Ghulam Mujtaba, Ph.D.

FOUNDER AND CEO, DROSONIC

Ghulam Mujtaba, Ph.D., is the founder and CEO of DroSonic and leads its work on passive acoustic drone detection. A computer engineer with 13 years of experience building machine-learning systems for edge hardware, he holds a Ph.D. in computer engineering from Gachon University in South Korea, was an NSF postdoctoral fellow at West Virginia University in the United States, and is an Assistant Professor of AI and Data Science at Regis University in Denver, Colorado. An IEEE Senior Member, he has published more than 20 papers on deep learning, computer vision and multimedia for edge devices.

PROFILE ↗ LINKEDIN ↗ ORCID ↗

ALL SOURCES (15)

1. Euromaidan Press — EW company commander: 1 module → 4–5 → 7 in 2024; nothing to counter fibre-optic drones (page labelled advertorial)
2. CSS, ETH Zurich — Kunertova 2024, Learning from the Ukrainian Battlefield, Sec. 2.3: jammers need sufficient power and cover a narrow range of spectrum; a different frequency per drone defeats them; jamming impairs friendly drones
3. Taifun — 25–30 km spools in production; 50 km experimental
4. RSF guide — Fibre-optic drones: EW ineffective; detected only visually or by sound
5. Euromaidan Press — Fibre-optic drone strike on Kramatorsk
6. Wikipedia — SIM-card control; airport anti-drone system reportedly failed to detect
7. Wikipedia — Some decoys carried Polish SIM cards
8. Euromaidan Press — Jamming gun fired at drone over Kleine-Brogel failed to disable it
9. Wikipedia — ArduPilot; AI target recognition for signal loss; possibly SIM cards
10. Euromaidan Press — Saker Scout approved by Ukraine's MoD; independently recognises enemy equipment, even camouflaged; inertial guidance increases resistance to EW
11. U.S. DOJ, FAA, DHS & FCC — Jamming and spoofing: aircraft sabotage laws; RF spectrum laws
12. DroSonic — Passive acoustic detection: neural networks on low-cost edge hardware, no emissions
13. DroSonic — NDIA EmergingTechETI 2026 presentation
14. DroSonic — U.S. provisional patent application 64/148,522, September 2026

5. DroSonic — DIRT Days 26.04 field test