Nick Clark · Published June 2026 · PDF

When the Link Dies: What Ukraine's Drone War Proves About Trustworthy Autonomy

In Ukraine, electronic warfare takes the control link and GPS away first, and a drone that depends on either is dead weight. The counter that is winning is onboard autonomy, a drone that completes its mission with no signal from base. But a drone that acts with no link raises a harder problem than flight: how do you trust what it does when no one can see it or stop it? The answer holds across every autonomous domain. Authority, rules, identity, and the record of what was done have to travel inside the system, because there is no command post left to govern from.

A drone is only as good as the link that controls it, and in Ukraine that link is the first thing the enemy takes away.

Electronic warfare is now the dominant counter to the cheap first-person-view (FPV) drones and loitering munitions that define the war. Russian and Ukrainian forces both field jammers that sever the radio control link and deny GPS navigation. A drone that depends on either goes blind and unresponsive in the same instant. It drifts off course, loses its target, and falls. Along much of the front, drones are defeated not by being shot down but by being cut off.

Two engineering responses have emerged, and they divide on a single architectural question: where does the authority to act live?

The first response keeps the authority at the operator. Fiber-optic-tethered drones spool out a thin glass filament as they fly, an unjammable physical link back to the pilot. They work, and they pay for it with limited range, reduced speed, and a trailing wire that constrains maneuver. The design preserves the link at the cost of everything else, because the drone cannot act without it.

The second response moves the authority into the drone. Onboard machine vision locks onto a target and completes the engagement after the link is jammed. The operator designates an area or a target, and the drone finishes the run with no signal from base. From there the trajectory runs toward full mission autonomy and toward swarms that coordinate locally with no base at all. In a saturated electromagnetic environment, a drone that needs no signal is not an enhancement. It is the only design that keeps working.

This is a constraint of physics, not a doctrine preference. A guidance loop that must close in tens of milliseconds cannot wait on a round trip to a command post, and a jammer guarantees there may be no command post within reach. Autonomy is the property of acting without a round-trip to authority, and electronic warfare forces that property on any system that intends to function.

Controlling the drone is only half the problem. A drone that flies itself raises a harder question: how do you trust what it does when no one can see it or stop it? That question cannot be answered from a command post the jammer has already cut off. When the link dies, every form of external control dies with it, including the operator's abort, the rules of engagement enforced from the rear, and the live feed that would justify a strike after the fact. Authority cannot be exercised from a center that the system, by definition, is operating without.

The authority has to travel inside the drone. Three properties have to move from the base into the object:

- Rules of engagement, carried in the drone and checked before the strike. With no link, ROE cannot be enforced from outside. It has to be encoded in the drone and gate the terminal action, and aborting has to be an allowed outcome. A refusal to fire becomes the drone breaking off rather than striking a prohibited target on its own. This is the technical form of meaningful human control without a live link: human authority encoded as carried, checkable constraints instead of a real-time command channel the enemy can cut.
- Carried identity that resists spoofing and capture. Contested airspace produces impersonation, hijacking, and the recovery of downed units. Drones coordinating in a mesh with no base have to authenticate each other without a central authority, so each verifies a peer's credential before extending trust. A spoofed or captured unit cannot then join the swarm. Friend-or-foe becomes a property the drone carries, not a determination the base makes.
- An append-only record of what the drone did and why. With no link to observe the engagement, accountability has to be reconstructable from the drone itself. A tamper-evident log carried by surviving units, or recovered from a downed airframe, is the only after-action record that exists.

These three properties are what separate an autonomous weapon that is governed from one that is merely released.

Two limits are worth stating plainly. A drone captured fully intact, in adversary hands, marks the boundary of any software approach, because software alone cannot make a fully adversarial host report on itself honestly. That boundary belongs to hardware roots of trust and tamper resistance, which carried governance composes with rather than replaces. And lethal autonomy sits under serious legal and ethical constraint. Carried rules of engagement, fail-closed abort, and auditable lineage are a partial technical contribution to keeping humans meaningfully in control of systems that act alone. They do not resolve whether such systems should select and engage human targets, and the constraint against autonomous selection and engagement of human targets without meaningful human control is one to encode and enforce, not relax.

The logic holds across every autonomous domain, and Ukraine states it without ambiguity. Jamming makes external governance physically impossible. The battlefield makes non-autonomy a losing position. What remains is autonomy that carries its own authority, its own rules, its own identity, and its own record: governance that travels with the system, verifies itself, and fails closed when it cannot confirm that an action is permitted.

That is what trustworthy autonomy means when the link is dead and the stakes are real. The full argument, and why autonomy rather than decentralization is what forces authority into the data object across every domain, is in the white paper, Autonomy You Can Trust (/autonomy-you-can-trust).