HIBILTER · HUMAEL — WHITE PAPER

Vajra Sentinel

Defeating the swarm: agentic counter-UAS for contested airspace

Why drone swarms break legacy air defence, and how a sensor-fused, doctrine-grounded kill-chain with human-in-command defeat changes the maths.

Ankesh Tiwari · 26 Jun 2026 · 14 min read · hibilter.com

EXECUTIVE SUMMARY

Air defence was engineered for a small number of large, fast, expensive threats. The drone swarm inverts every assumption: many small, slow, cheap, autonomous objects, arriving together and saturating both sensors and shooters, with a cost-exchange that runs the wrong way. This paper sets out an agentic approach to counter-UAS: fuse radar, EO/IR, RF and acoustic sensing into one live air picture; classify intent from movement, not just signature; and run the full kill-chain — detect, track, classify, engage, neutralize — as a coordinated team of agents that escalate the decisions that matter to a human commander. We describe the sensor-fusion architecture, the doctrine-grounded reasoning that keeps engagement inside the rules, the layered, non-kinetic-first countermeasure model, and the metrics that decide whether airspace is actually held.

The threat changed faster than the defence

Air defence was built for a small number of large, fast, expensive threats — aircraft and missiles — detected at range and engaged by costly interceptors. The drone swarm inverts every one of those assumptions. The threat is now many objects that are small, slow, cheap and increasingly autonomous, arriving together to saturate the picture. A defence that spends a million-rupee interceptor on a fifty-thousand-rupee drone has already lost on cost, even when it hits.

The deeper failure is human. A single operator watching a radar cannot triage a hundred contacts in the seconds available, decide which are hobbyists and which are a coordinated ingress, and assign the right effector to each. The bottleneck in counter-swarm is no longer the sensor or the shooter — it is the speed and consistency of the decision.

One air picture from four kinds of sensing

No single sensor sees a small UAS reliably. Radar struggles with low-RCS slow movers; electro-optical and infrared need line of sight and good conditions; radio-frequency only sees emitters; acoustic is precise but short-range. Sentinel fuses all four into one continuous track per object, so a contact dropped by one modality is still held by another, and identity is built from agreement across sensors rather than the guess of any one.

- **Radar** — volume search and range, the backbone for early detection and track.
- **EO/IR** — visual and thermal confirmation, classification and effect assessment.
- **RF** — detection and geolocation of control and video links, and protocol fingerprinting.
- **Acoustic** — short-range confirmation that fills the gaps where radar and EO fail.

Movement-based attack-mode intelligence

Knowing a contact is a quadcopter is necessary and not sufficient. Intent lives in movement — loiter, reconnaissance, ingress, terminal run. Sentinel classifies attack mode from trajectory and behaviour, so a benign overflight and a coordinated strike are not handed to the operator as identical red dots. Behaviour, not just signature, drives the priority.

The agentic kill-chain

Sentinel runs the full kill-chain — detect, track, classify, engage, neutralize — as a coordinated team of agents, each accountable for its stage and evaluated against the standards of that stage. The chain runs at machine speed across the whole swarm at once, but it stops at the gates a commander sets, surfacing the engage decision rather than burying it in routine confirmations.

> *Against a swarm, the side that decides faster wins — but only if every decision stays inside the rules.*

Non-kinetic first, layered defeat

Effect should match threat. Sentinel recommends the lowest-collateral effector that will work, and reserves kinetic defeat for when softer means will not. Layered, non-kinetic-first defeat keeps cost and collateral down in exactly the cluttered, populated environments where counter-UAS usually has to operate.

- **Electronic warfare** — jam or spoof the control and navigation links to deny the mission.
- **Cyber / protocol takeover** — assume control of the airframe where the protocol allows.
- **Directed energy** — precise, low-cost-per-shot defeat with a deep magazine.
- **Kinetic** — last resort, when the threat and the rules of engagement demand it.

Doctrine-grounded, human-in-command

Sentinel reasons on a sovereign model grounded in rules of engagement and doctrine, so its recommendations are explainable in the language the commander already uses. Every defeat is human-in-the-loop and ROE-checked: the system presents the engage / no-engage decision with the evidence behind it, and a human owns the call. Every engagement is logged and reconstructable for after-action review — the property that makes autonomy acceptable where it matters most.

Sovereign and on-premise by default

Counter-UAS runs where the airspace is, often disconnected and always sensitive. Sentinel runs entirely within your perimeter, air-gapped, on a sovereign model, with no telemetry leaving the site. It is mission-grade software designed for the edge, not a cloud service pointed at a battlefield.

What 'holding the airspace' actually measures

Range & time

how early a swarm is detected, tracked and identified

Tracks held

simultaneous contacts maintained without dropping the swarm

Decision latency

detect-to-defeat time, the number that beats the swarm

Leakers

threats that reach the protected asset — the only score that counts

Where Sentinel is deployed

- **Air bases and forward operating bases** — protecting aircraft, fuel and crews from stand-off swarms.
- **Critical infrastructure** — refineries, power, ports, data centres and pipelines.
- **Border and infiltration** — detecting and defeating cross-border drone incursions and smuggling.
- **VIP movement and mass events** — stadiums, summits and processions where collateral risk is highest.
- **Maritime and offshore** — ships, rigs and harbours, where horizon and clutter defeat single sensors.
- **Convoy and mobile** — protection on the move, integrated with manoeuvre forces.

Conclusion

The swarm is a software problem as much as a hardware one. The defence that wins fuses everything it can sense, reasons about intent rather than signature, runs the kill-chain at machine speed, and keeps a human in command of the decision that matters. That is the difference between a radar full of red dots and airspace that is actually held.