Cross-Medium Composite Disruption Signatures

by Nick Clark | Published April 25, 2026

What Composite Signatures Specify

A composite signature is a credentialed observation describing the multi-medium pattern that characterizes a specific disruption cause. The signature includes: the cause it identifies (GPS spoofing, optical blinding, coordinated RF jamming, weather-related propagation anomaly, equipment-aging drift, etc.), the constituent observations across media that the signature requires (RF, optical, acoustic, etc., with declared modalities and uncertainty), the expected correlations (temporal alignment, magnitude relationships, spatial coherence), and the confidence thresholds for attribution.

The signature library is composed and maintained by credentialed authorities. Defense authorities sign signatures for adversarial causes. Spectrum authorities sign signatures for spectrum-related anomalies. Meteorological authorities sign signatures for natural disruption. The library is governance-extensible: new signatures register through credentialed governance updates.

Why Heuristic Detection Cannot Substitute for Credentialed Signatures

Heuristic disruption detection (rule-based detectors, ML classifiers trained on known patterns) produces useful signal but lacks the credentialing chain that operational response requires. When a heuristic flags 'possible jamming,' the operating system cannot tell who endorsed the detection criteria, what evidence supports the detection, or whether the criteria are current with adversary capabilities.

Credentialed signatures provide what heuristic detection cannot: a chain of custody from the credentialing authority to the detection event. The signature is signed by the relevant authority (FCC for jamming-detection criteria, defense authority for adversarial-attribution criteria); the detection event references the specific signature; the credentialing authority bears responsibility for signature accuracy. The architecture supports the operational and legal foundations that pure heuristic detection lacks.

How the Library Composes With Operating Systems

Operating systems subscribe to credentialed signature feeds from authorities they admit. New signatures propagate through the governed mesh. The system's admissibility evaluator consumes both the live cross-medium observations and the relevant signatures, evaluating whether observations match any admitted signature pattern.

When a match occurs, the architecture produces a credentialed attribution observation: the cause is identified, the supporting evidence is recorded, the matched signature is referenced, and the credentialing authority is identified. Downstream consumers admit the attribution through their own policy and respond accordingly. When observations don't match any admitted signature, the architecture produces a 'novel disruption' observation that propagates back to the credentialing authorities for review.

What This Enables for Cross-Authority Disruption Response

Defense operations gain shared adversarial-attribution criteria across allied forces. Each ally signs signatures within its credentialed scope; operating systems admit allies they trust; the resulting signature library provides cross-coalition disruption attribution that single-nation libraries cannot.

Civilian critical-infrastructure operators gain access to credentialed signatures from authorities (FCC, DHS, ISACs) that produce attribution they can act on legally. The patent positions the primitive at the layer that cross-authority disruption response requires for coalition military operations and critical-infrastructure protection alike.