# Cross-Domain Adversarial Inference

by Nick Clark | Published April 25, 2026

## What Cross-Domain Inference Specifies

Civilian autonomous vehicles use Tier 2 (turn signals, brake lights) and Tier 3 (trajectory inference) to coordinate with non-cooperative human drivers, with hostility classification disabled by default. Commercial fleet operations use behavioral inference for safety analysis under actuarial-credentialed framework. Emergency response uses cross-tier intent fusion for dispatcher-coordinated multi-agency operation. Defense ISR uses tier-weighted intent with hostility classification enabled under credentialed mission ROE. Homeland security uses cross-tier inference for adversarial-detection applications.

Each domain configures the architecture differently. Civilian admits the operator-intent fusion at low adversarial sensitivity; defense admits it at high adversarial sensitivity with explicit hostility-classification enabled. The mechanism is invariant; the configuration changes.

## Why Cross-Domain Reuse Matters Architecturally

Per-domain engineering produces structural fragmentation. Civilian AV fleets build their own intent architecture; commercial fleet management builds its own;

emergency response builds its own; defense ISR builds its own. The cumulative effort across domains is substantial; cross-domain learning is limited.

Cross-domain architectural reuse changes the pattern. The same primitives operate across domains; investment in the architecture benefits all domains. Innovations from one domain (defense ISR's adversarial-detection improvements, civilian AV's mixed-fleet improvements) propagate structurally through configuration updates.

## How Configuration Differs Across Domains

Civilian-context configurations weight Tier 2 and Tier 3 contributions for non-cooperative-driver coordination, with hostility classification disabled. Defense-context configurations weight all three tiers for fully-cooperative-allied + non-cooperative-civilian + adversarial mixed scenarios, with hostility classification enabled under credentialed ROE.

The credentialing chains differ. Civilian configurations operate under state-DOT credentialed policy. Defense configurations operate under national command authority through theater command through mission ROE.

## What This Enables for Multi-Domain Industry

Defense contractors with civilian operations (Anduril's commercial counter-UAS, Shield AI's emerging civilian work) gain architectural reuse across their domain mix. Civilian fleet operators with regulated operations gain access to defense-grade hostility classification under appropriate credentialing.

The patent positions the primitive at the layer where the multi-domain industry has been operating with per-domain architecture investment.