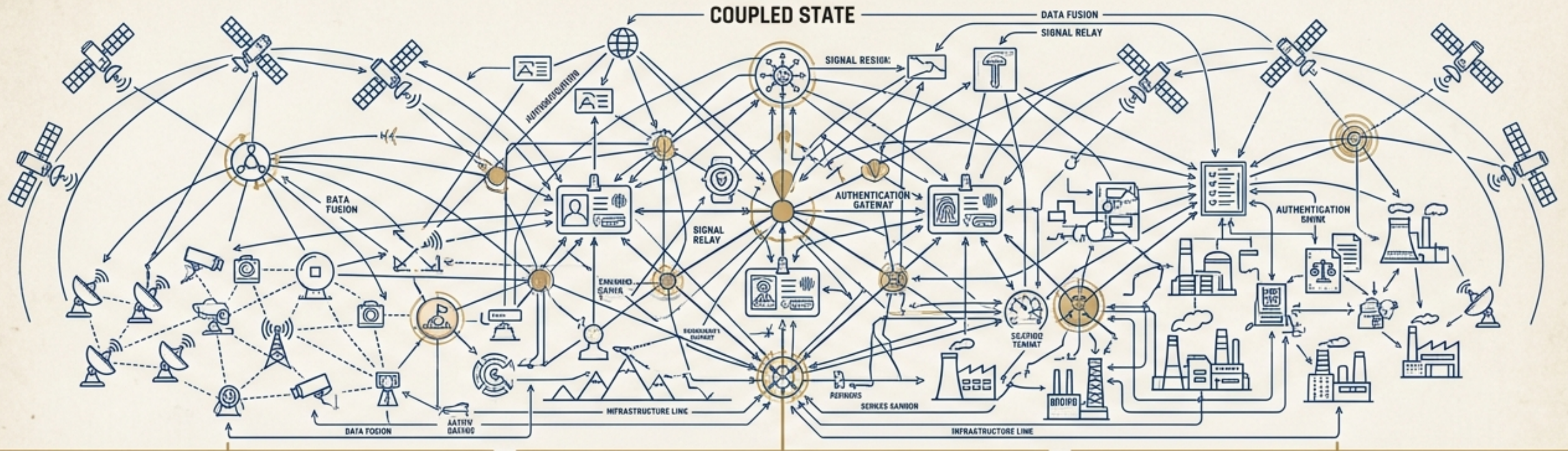


# Tensor-Geometric Mission Control

How PTCP + TNQG provide a predictive  
safety and intelligence substrate for CJADC2,  
Zero Trust, and Federal AI Governance.

# DEFENSE AND FEDERAL OPERATIONS ARE NOW HIGH-DIMENSIONAL CONTROL PROBLEMS.



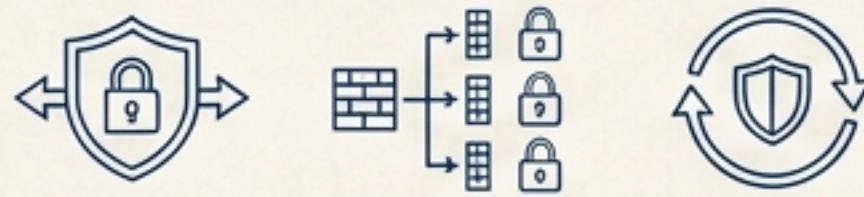
## CJADC2: Information & Decision Advantage

The mandate to iteratively connect sensors, shooters, and decision-makers across warfighting domains on 90-day cycles.



## Zero Trust: Continuous Evaluation

The DoD FY2027 and NIST 800-207 mandates requiring continuous identity, posture, and lateral movement control.

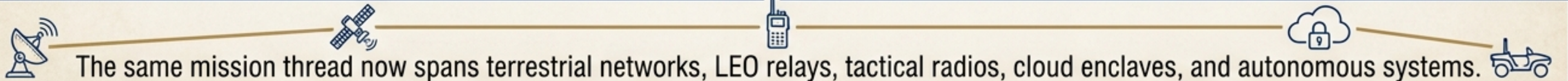


## AI Governance: Bounded Autonomy

OMB M-24-10 and CDAO rules requiring mechanisms to measure, audit, and roll back AI in safety-critical infrastructure.



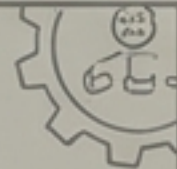
The same mission thread now spans terrestrial networks, LEO relays, tactical radios, cloud enclaves, and autonomous systems.



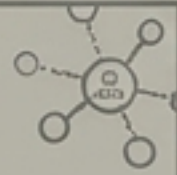
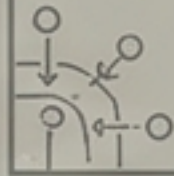
# THE CONTROL PARADIGM SHIFT

## CONVENTIONAL BASELINE

**State Representation**  
Isolated scalar metrics  
(bandwidth, CPU).



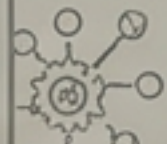
**Routing Metric**  
Expected cost / Shortest path.



**Security Detection**  
Isolated SIEM alerts and  
static trust rules.



**Autonomous Control**  
Unconstrained AI scripts or  
manual change boards.



## PTCP + TNQG PARADIGM

**State Representation**  
Multimodal tensor probability  
(joint pattern-of-life).



**Routing Metric**  
CVaR (Conditional Value-at-Risk)  
tail-risk geometry.



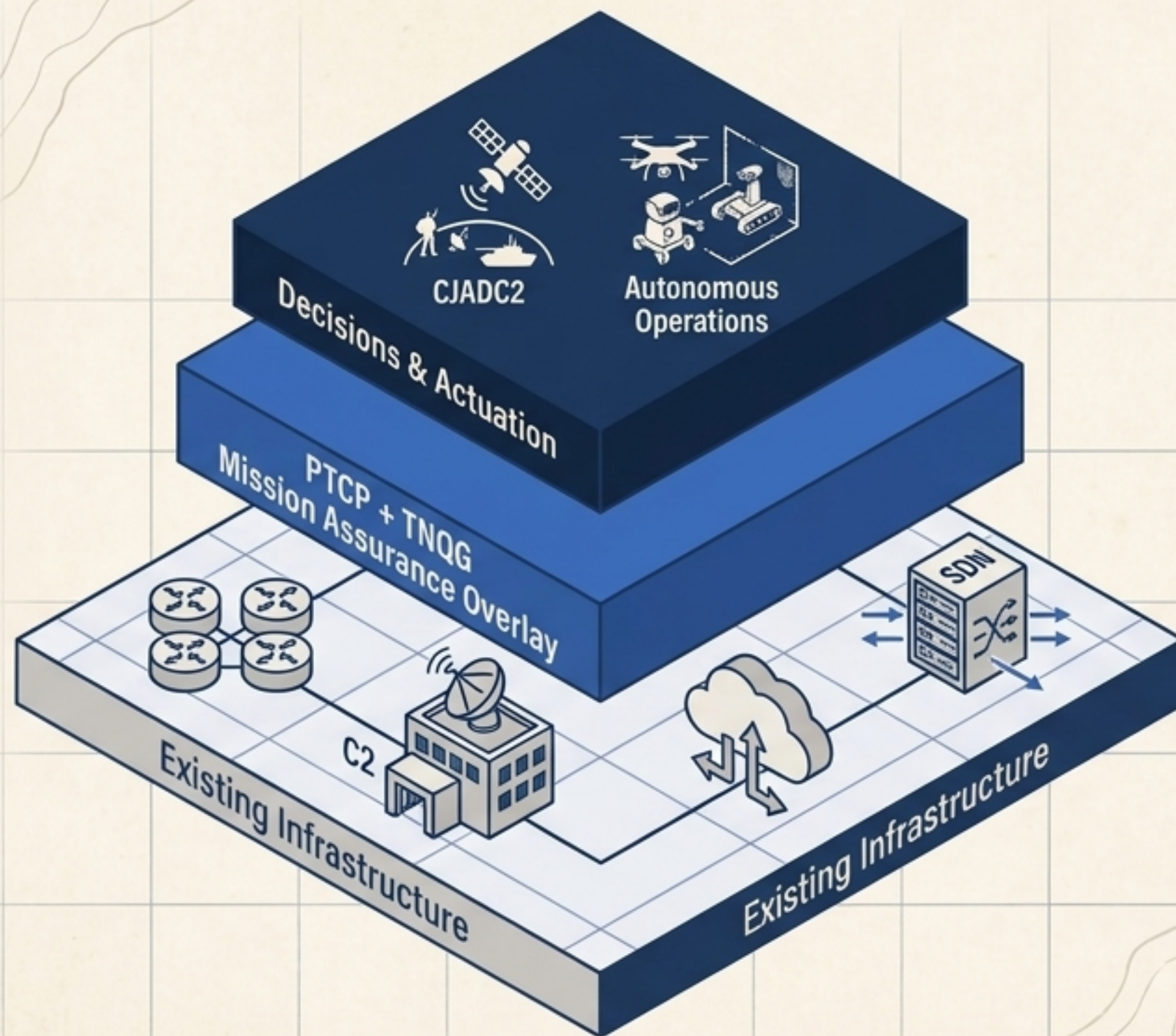
**Security Detection**  
Topology-native geometric defects  
(curvature, cut-entropy).

**Autonomous Control**  
Safe actuation projected inside  
bounded reachability limits.



# NOT A REPLACEMENT. AN UPSTREAM INTELLIGENCE & SAFETY LAYER.

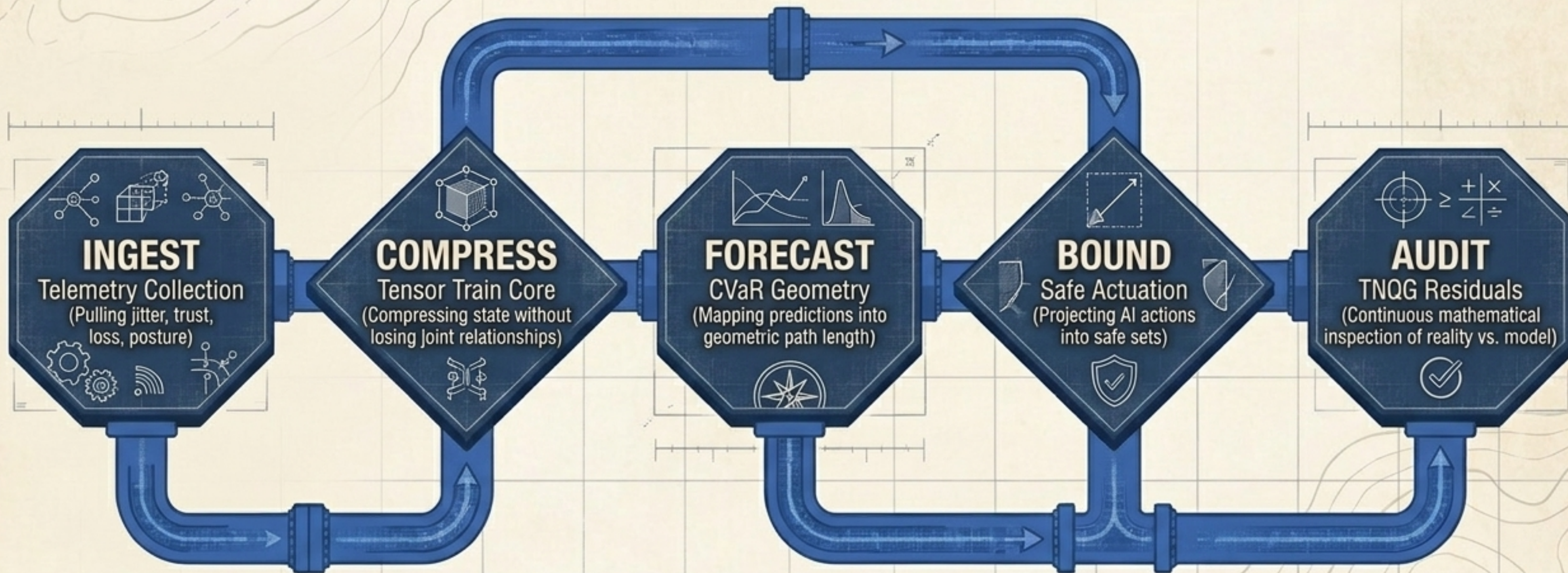
- Ingests telemetry from existing SIEM, SDN, identity, and routing tools.
- When uncertainty is low, reduces to baseline static/reactive control.
- Under attack pressure, jamming, or congestion, activates predictive, risk-aware, topology-preserving behavior.



**The Goal:**  
Safer decision  
Faster decisions  
whose infrastructure  
effects are bounded,  
explainable, and  
reversible.



# THE TENSOR-GEOMETRIC OPERATIONAL PIPELINE



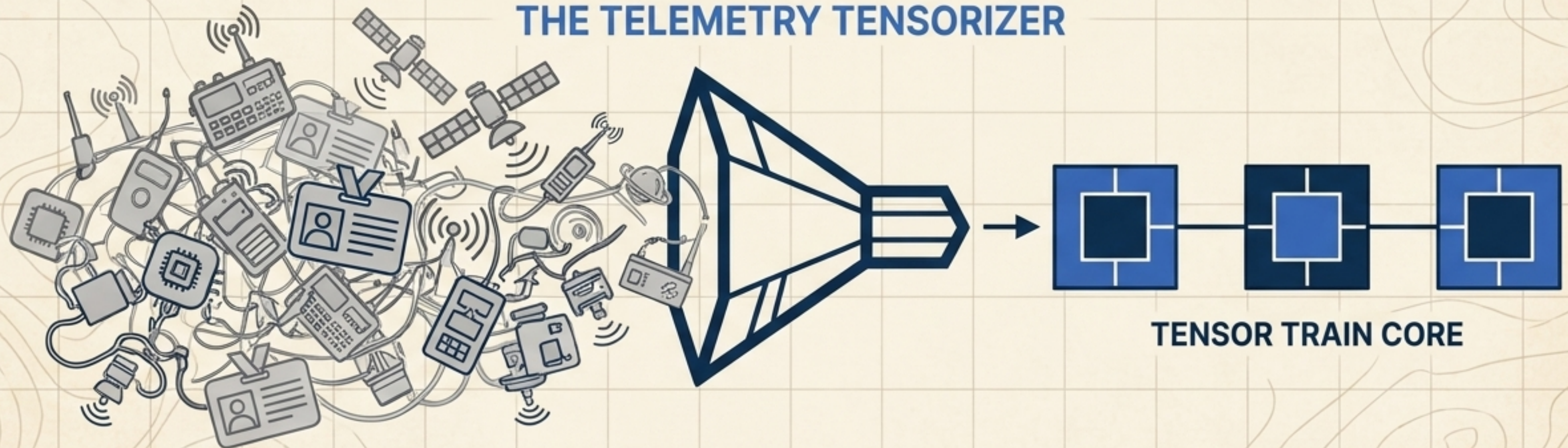
# MECHANISM 1: TELEMETRY TENSORIZATION

$O(n^d) \rightarrow O(dnr^2)$  COMPRESSION

Traditional logging stores high-dimensional state directly—an exponential explosion that crashes systems. PTCP approximates probability tensors using Tensor Train cores.

Takeaway: We create a highly compressed, joint pattern-of-life model for mission state that scales across domains, without forcing all complexity into a single scalar score.

## THE TELEMETRY TENSORIZER



# MECHANISM 2: PREDICTIVE GEOMETRY & CVaR ROUTING

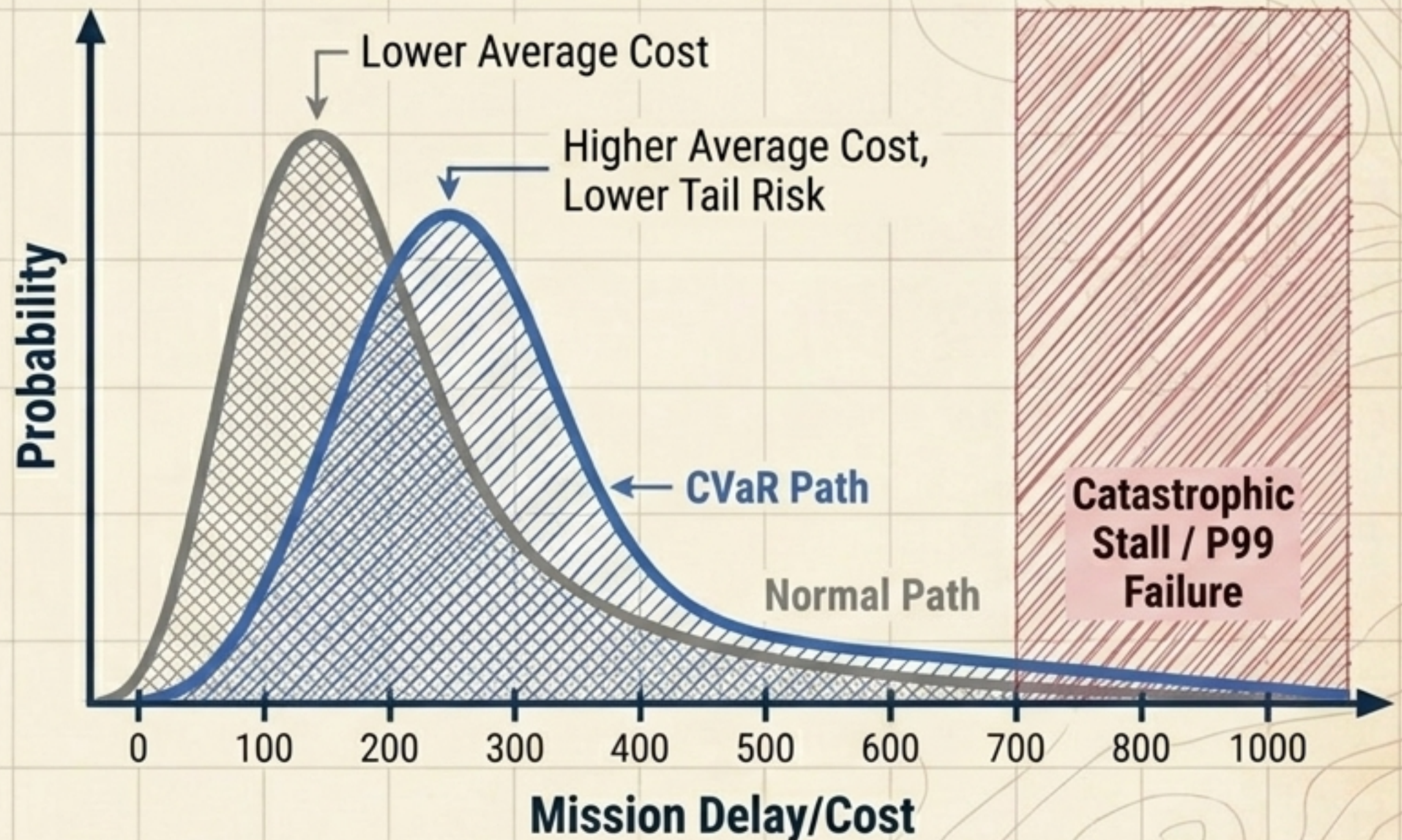
$$\min E[Z_{\pi}] + \rho * CVaR_{\alpha}(Z_{\pi})$$

Defense systems cannot survive on average throughput.

A path that is usually fast but occasionally stalls during jamming or cyber attack causes mission failure.

**Takeaway:** PTCP minimizes Expected Cost plus a Conditional Value-at-Risk (CVaR) tail penalty. We actively route away from rare but catastrophic edge vulnerabilities.

## MISSION DELAY/COST DISTRIBUTION



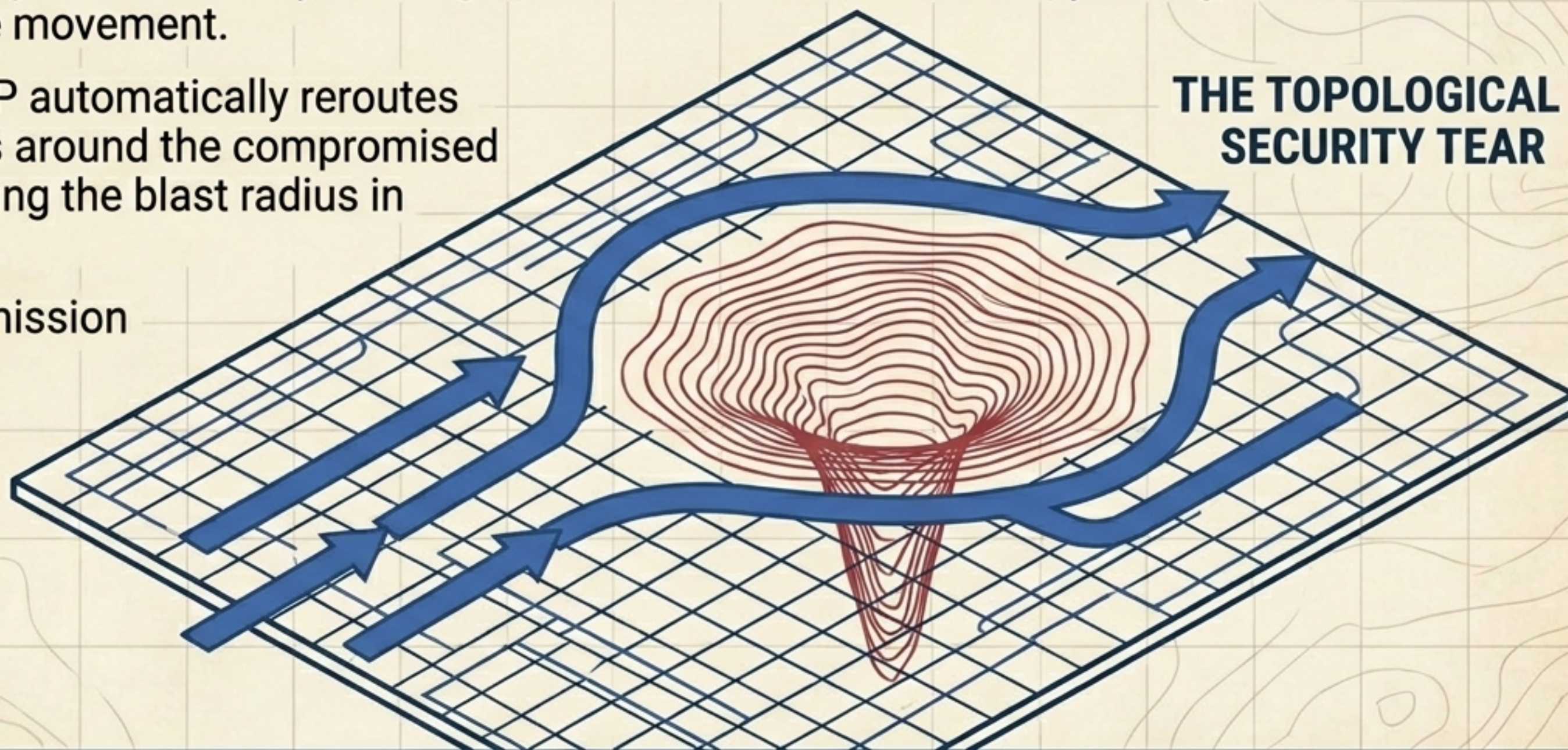
# MECHANISM 3: TOPOLOGY-NATIVE SECURITY

Security is no longer just a separate dashboard of text alerts. An attack, insider threat, or policy drift is mathematically modeled as a physical deformation in network geometry.

Diagnostics integrated: Anomaly score, graph-curvature shift, cut-entropy change, and trust-coordinate movement.

**Takeaway:** PTCP automatically reroutes mission threads around the compromised topology, isolating the blast radius in

**real-time.** The Topographical mission anomaly well architectural flat-plane grid manifold.



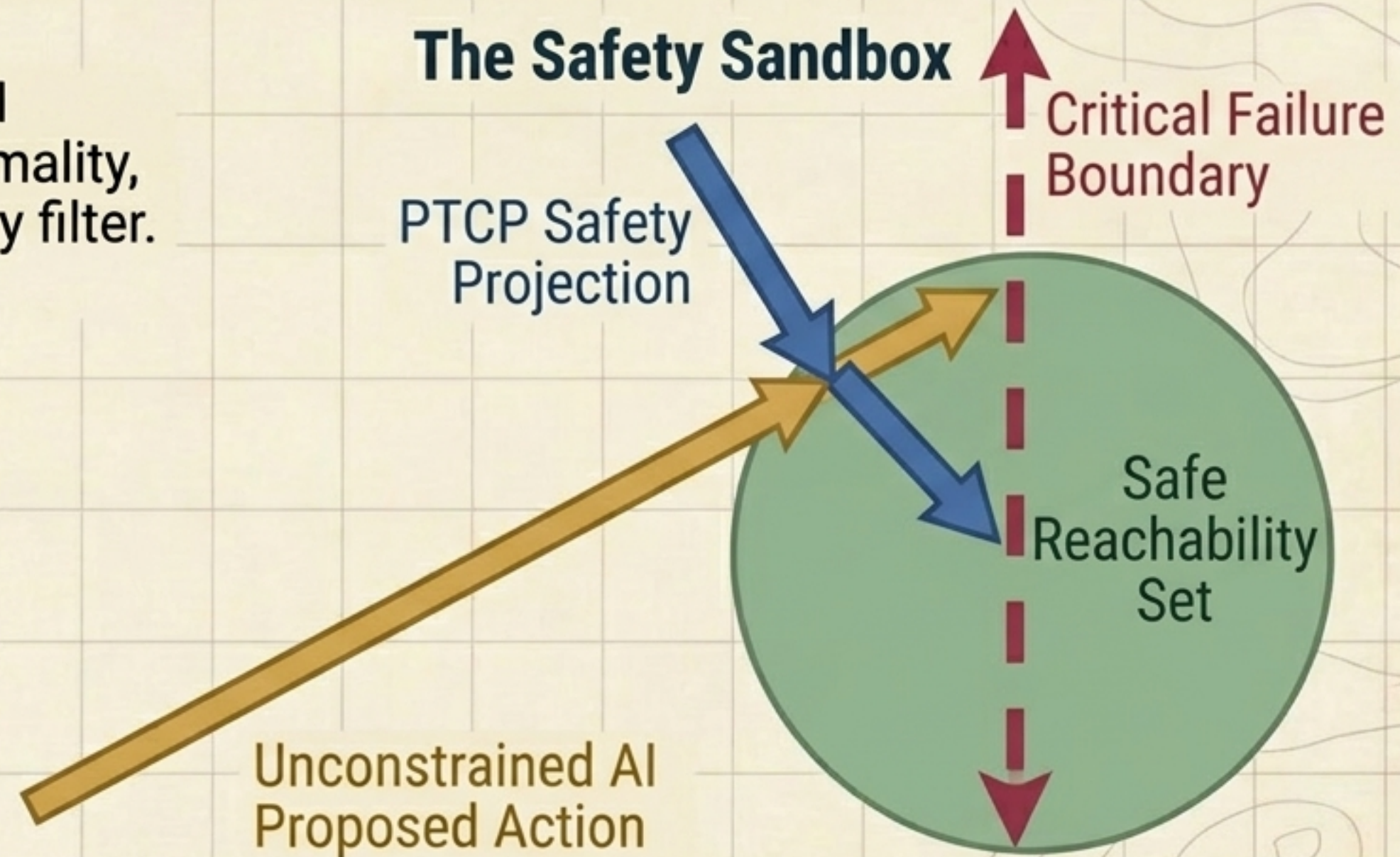
# MECHANISM 4: BOUNDED ACTUATION

AI cannot be granted unconstrained authority over socio-technical systems. PTCP explicitly separates optimization from authority.

Constraints Enforced: Reachability, Capacity Feasibility, Access Policy, and Rollback availability.

**Takeaway:** Prediction errors or AI hallucinations may degrade optimality, but they cannot bypass the safety filter. Zero critical policy violations.

**Takeaway:** Prediction errors or AI hallucinations may degrade optimality, but they cannot bypass the safety filter. Zero critical policy violations.



# THE SYNTHESIS: SEPARATION OF POWERS

## THE DRIVER



### PTCP Decides

Optimizes paths, forecasts risk, and drives autonomous action forward.

## THE INSPECTOR















### TNQG Audits

Acts as the mathematical physics inspector. Continuously runs residual tests (distance, capacity, curvature) to ensure the AI's internal map hasn't drifted from reality.

















**Achieves the modern DoD holy grail: Decision Advantage without Unconstrained Autonomous Risk.**



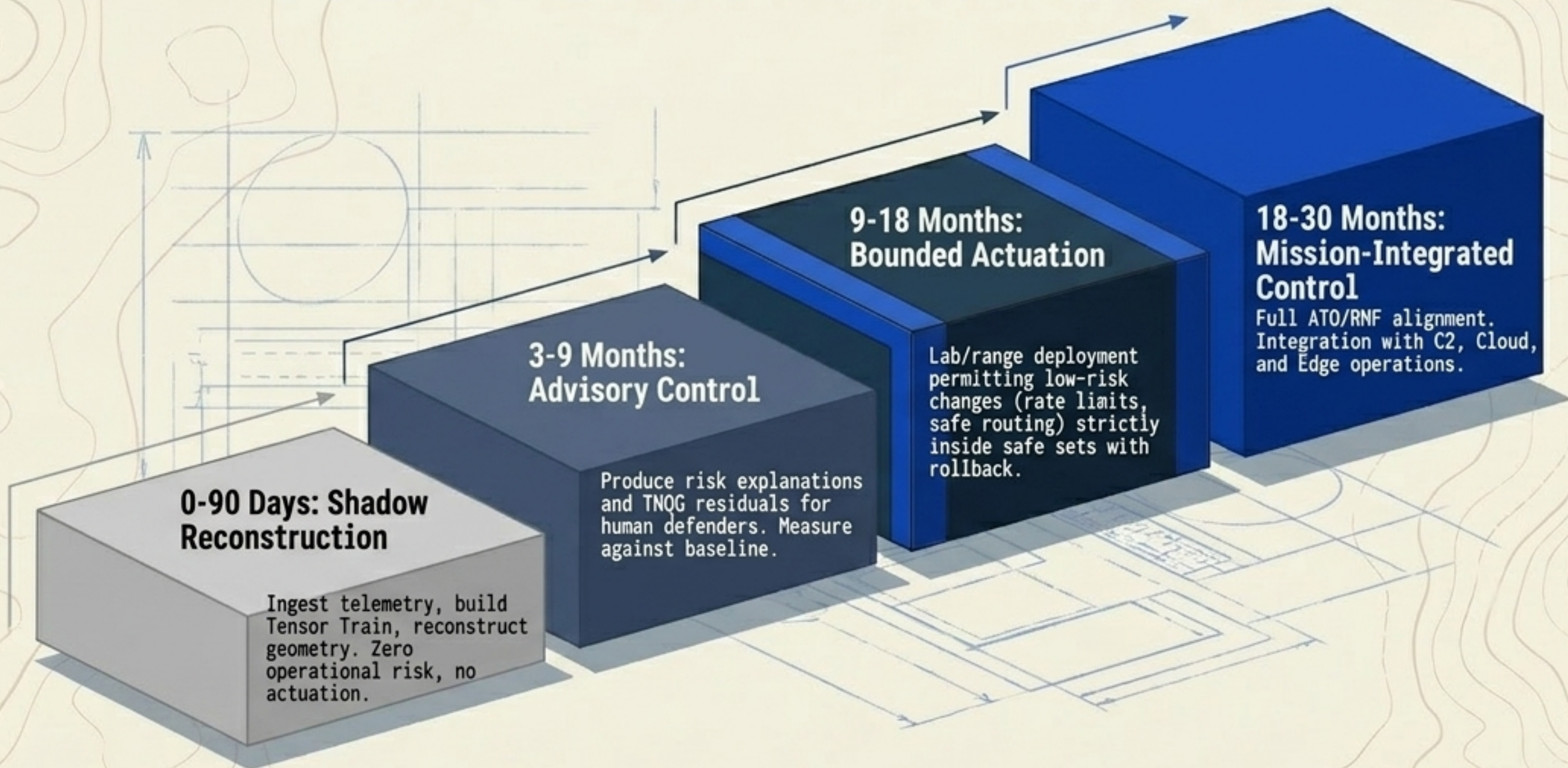
# THE DEFENSE MISSION MATRIX

Domain	Operational Challenge	PTCP Capability	TNQG Audit Function
Tactical Edge (Army / USMC) <small>categorical</small>	Contested kill webs, mobile units. 	Forecasting congestion before C2 loss. 	Auditing fragile tactical cuts. 
Proliferated Domains (SDA / Space Force) <small>categorical</small>	Dynamic graphs, moving satellites. 	Risk-aware space-ground routing. 	Identifying structurally brittle optical/RF links. 
Joint Operations (CJADC2 / COCOMs) <small>categorical</small>	Multi-domain data integration. 	Unified state tensor across theaters. 	Reconstructing latency hiding in coalition links. 
Maritime & Cyber (Navy / USCYBERCOM) <small>categorical</small>	Emissions control, defensive hunt. 	Topology-native partner risk mapping. 	Distinguishing transient noise from structural lateral corridors. 

# THE FEDERAL INFRASTRUCTURE MATRIX


Sector	Operational Challenge	PTCP Capability	TNQG Audit Function
Civilian Cybersecurity (CISA / DHS) 	Zero-trust implementation at scale. 	Microsegmentation analytics. 	Distinguishing real structural risk from noisy SIEM alerts. 
Energy & National Labs (DOE / NNSA) 	Safe AI on grid OT / HPC. 	Unifying IT/OT telemetry. 	Auditing mission-critical control loops for safety. 
Intelligent Transport (DOT / FAA) 	Secure V2X and rail corridors. 	Forecasting congestion tail-risk. 	Reconstructing traffic-flow vs. information-flow residuals. 
Enterprise Services (HHS / VA / GSA) 	Aging tech and privacy. 	Resilient health data exchange. 	Cross-agency observability metrics. 

# THE DEPLOYMENT PATH: ABSOLUTE CONTROL OVER THE ADOPTION THROTTLE



# FALSIFIABLE VALIDATION BASELINES

CLAIM	REQUIRED VALIDATION METRIC	LEGACY BASELINE TO BEAT
Compression	TT Rank, reconstruction error, rare-event preservation.	Dense storage / PCA sketching.
Routing/Control	Mean latency, p95/p99 stall rate, recovery time.	OSPF/BGP, SDN TE, ECMP.
Risk Control	CVaR/tail-cost reduction under jamming/bursts.	Expected-cost routing.
Security	Detection delay, AUROC, blast-radius reduction.	SIEM anomaly-only detection.
Safety	Zero reachability violations, rollback success rate.	Unprojected AI scripts / manual boards.



**The value of PTCP + TNQG is not merely technical efficiency. It is the ability to operate AI-enabled government systems that are predictive without being reckless, adaptive without being unconstrained, and data-driven without losing auditability.**

- 1. Select one defense mission thread & one civilian critical infrastructure thread.**
- 2. Instrument telemetry and run PTCP in Shadow Mode.**
- 3. Evaluate falsifiable metrics against legacy baselines before authorizing control.**