Chapter 13: The New Tactical Battlespace – Disruption as a Default

Part of the series: The Argument for Embedded Logic at the Edge vs Centralised Large AI in Modern and Future Warfare

Published: Ambient Stratagem

July 2025

> "We have to stop designing for the assumption that the network will be there. In future fights, it won't be."
>
> — US Army Multi-Domain Task Force Briefing, 2025

The nature of tactical combat has changed. Where once militaries could expect to operate with assured connectivity, predictable logistics, and protected C2 networks, today's battlefield is contested, congested, and actively denied by capable adversaries. From electromagnetic jamming to GPS spoofing, from drone swarms to cyber-enabled deception, the modern tactical environment is defined less by certainty and more by volatility.

This chapter outlines how the character of tactical warfare has evolved, and why any AI capability that assumes persistent cloud access, centralised control, or unbroken connectivity is a liability, not an asset.

1. The Tactical Environment Has Been Rewritten

Contested environments are no longer hypothetical. They are the new operational standard. Tactical units must now contend with:

Signal Disruption

Persistent jamming of GNSS, tactical radios, and SATCOM terminals.

Deception Operations

Real-time spoofing and deception, including false sensor inputs and decoy signatures.

Network Attacks

Cyber interference against mesh networks and ISR platforms.

Communication Blackouts

Unpredictable latency or total signal loss, especially in urban, mountainous, or subterranean terrain.

These disruptions are not isolated. They are coordinated and layered, often beginning minutes or hours before physical contact. Their purpose is simple: to separate the operator from information, from logic, and from control.

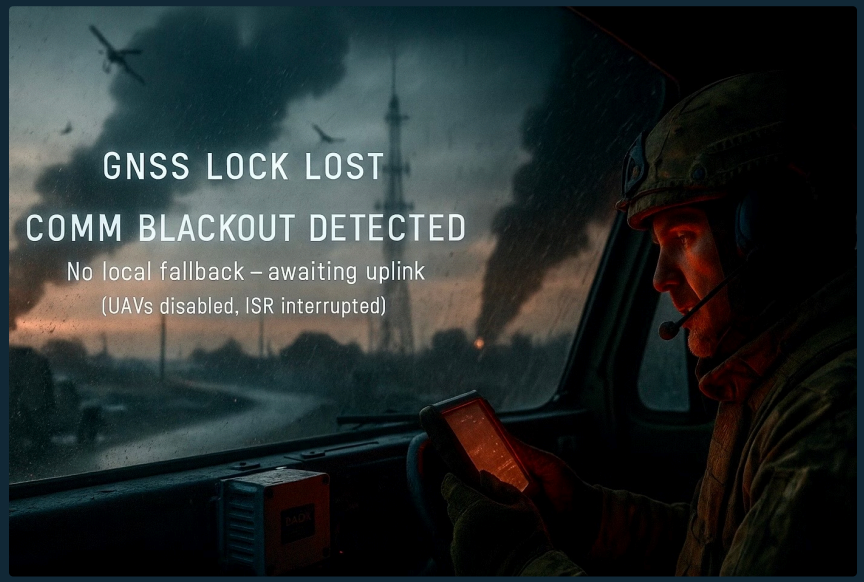
> "If your system needs a connection to think, it's already been defeated." — Polish Armed Forces Electronic Warfare Command, 2024

2. Case Study: Eastern Ukraine, Late 2024

Russian forces operating around Avdiivka launched a pre-assault EW barrage targeting Ukrainian UAV command links, GNSS signals, and troop communications.

- Commercial drones relying on cloud-based visual classification lost situational awareness mid-flight.
- AI-enhanced targeting apps, reliant on satellite connectivity, froze or misdirected fire support.
- Units equipped with locally embedded ISR classifiers continued to function, relay, adapt, even in blackout conditions.

The result: tactical advantage shifted not to the force with the best tech, but to the force with the most resilient tech—capable of functioning under attack.



3. The False Promise of Centralised Superiority

Much of the early investment in military AI focused on powerful, centralised systems:

General Knowledge Systems

Large language models trained on general knowledge.

Cloud Dependencies

Cloud-based fusion engines requiring constant data flows.

Integration Requirements

Predictive platforms that rely on real-time integration across multiple domains.

These systems perform well in peacetime trials or HQ-level wargaming. But in kinetic, degraded, or denied environments, they become:

Non-functional when disconnected

Opaque when delayed

Dangerous when misinformed

This isn't theoretical, it's operational. Tactical users in Ukraine, Gaza, and the Sahel have already experienced AI tools that simply vanish at the moment of need.

4. Embedded AI as the Tactical Standard

To fight and win in contested environments, AI must:

1 Local Processing

Run natively on the platform, with no reliance on cloud servers.

2 Edge Computing

Process data locally, enabling fast, reliable inference at the edge.

3 Graceful Degradation

Degrade intelligently, shifting into fallback modes rather than full failure.

4 Autonomous Adaptation

Respond dynamically, updating mission logic based on local input, not remote control.

This model of embedded AI logic ensures that:

- Drones keep flying.
- ISR nodes keep detecting.
- Operators keep deciding.

Even under denial. Even under fire.

Conclusion

The next generation of tactical systems will not succeed because they are the smartest in a lab. They will succeed because they are still thinking, still deciding, and still acting when every connection has been cut and every signal has gone dark.

> Tactical superiority now begins with resilience. And resilience begins with logic at the edge.

NEXT - Chapter 14: Local Logic, Instant Advantage – Outthinking the Threat at the Edge