Chapter 1: The Electromagnetic Battlefield – Lessons from Ukraine and Beyond

Part of the series: The Argument for Embedded Logic at the Edge vs Centralised Large AI in Modern and Future Warfare - April 2025

John Blamire

Founder - Ambient Stratagem

in: linkedin.com/in/john-blamire

The Contested Electromagnetic Spectrum

> "The electromagnetic spectrum is now as contested as the land, air, sea, and space."

— Admiral James G. Stavridis, former NATO Supreme Allied Commander

The war in Ukraine marked the beginning of a new epoch in military operations—one in which the electromagnetic spectrum itself is a target, terrain, and weapon. And it exposed a painful truth: digital systems built for peacetime will not survive wartime without redesign.

Russia's Doctrine of Digital Suppression

Russia entered Ukraine not only with tanks and missiles, but with a mature, well-integrated electronic warfare (EW) doctrine designed to suppress communications, disrupt satellite systems, and exploit unprotected data flows:

- GNSS jamming and spoofing rendered drones blind and disrupted navigation.
- SATCOM interference degraded strategic and tactical C2.
- Cellular and WiFi exploitation enabled real-time targeting and disinformation loops.

In the opening weeks of the war, commercial satellite communications used by Ukrainian forces were successfully hacked, leading to widespread disruption. This was not a theoretical failure—it had operational consequences: lost coordination, aborted missions, and avoidable casualties.

Centralised AI Under Fire: Structural Fragility Revealed

Cloud-based AI systems, designed for data-rich environments, quickly revealed their structural weaknesses when pushed into combat conditions:

Surveillance Failure

AI-enabled surveillance drones lost functionality when uplinks failed.

Processing Breakdown

Remote image classification pipelines timed out during active ISR operations.

Command Disruption

Centralised C2 platforms were disrupted by jamming and degraded networks.

These failures were not due to flawed AI models—they were due to architectural misalignment between system design and battlefield reality. Systems that required access to high-bandwidth cloud inference simply could not deliver value at the point of contact.

Ukraine's Tactical Pivot to Embedded Autonomy

By mid-2023, Ukrainian forces—supported by international partners—began transitioning to a tactical edge compute model:

On-Device Intelligence

AI-enabled drones began using on-device classification and pre-trained flight pattern logic.

Offline Operation

Counter-battery radar and targeting systems were upgraded with embedded decision loops, allowing operation in GPS- and comms-denied conditions.

Field Deployment

Units began deploying offline AI models, trained in-country and field-updated, running on ruggedised hardware platforms.

The result? A noticeable improvement in system survivability and operational consistency—even in areas saturated with Russian EW.

New Case Studies from 2024–2025

Recent operational incidents reinforce the urgency of shifting away from centralised AI architectures:

1

Red Sea, April 2025

A US MQ-9 Reaper lost target-tracking capability mid-mission due to Iranian-backed Houthi jamming. Its object classification module relied on a cloud link—rendering it ineffective.

2

Gaza, October 2024

Israel's cloud-based border AI suffered cascading failure after a targeted cyberattack overwhelmed the core inference systems. Legacy edge systems were reactivated to plug the gap.

3

NATO Black Sea Drill, March 2025

A live trial comparing cloud-based AI and embedded logic under simulated jamming showed the embedded system achieving mission objectives—while the cloud-reliant alternative failed to complete its ISR task.

Implications for NATO and European Forces

If Western forces are to maintain effectiveness against peer adversaries with advanced EW and cyber capabilities, they must accept a new reality:

Connectivity is not guaranteed.

Systems must be designed to operate effectively even when communications are degraded or completely lost.

Every signature is vulnerable.

Electronic emissions and digital footprints can be detected, tracked, and exploited by sophisticated adversaries.

Only logic that travels with the mission can be trusted.

Embedded AI and autonomous decision-making capabilities must be integrated at the tactical edge.

The future of warfare lies not in centralising intelligence, but in distributing it—surgically, securely, and resiliently—at the edge.

NEXT - Chapter 2: Latency Kills – The Fatal Cost of Cloud Dependence in Combat

Continue reading to understand how milliseconds of delay in cloud-based systems can mean the difference between mission success and catastrophic failure in modern combat scenarios.