Resilience against Cyber and Electronic Warfare (EW) Threats - Conclusion & Call to Action

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

Resilience Is the New Superiority

> "In war, resilience is the difference between systems that are available—and systems that are relevant." — UK Defence Command Insight Report, 2025

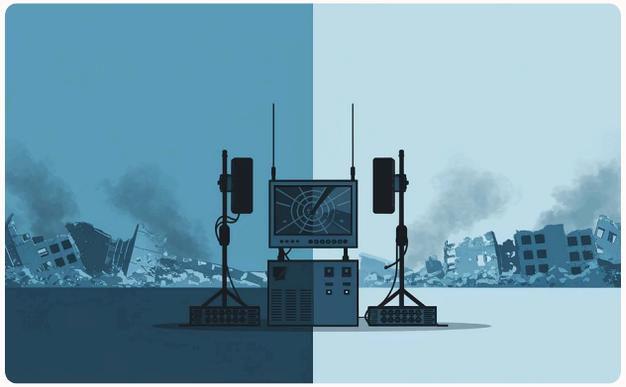
We are entering an era where war is won not by the most connected, but by the least dependent. Cyber and electromagnetic warfare have radically changed the calculus of survivability. Every drone, sensor, and system that depends on centralised compute or cloud inference is a potential liability—fragile in contested space, vulnerable to disruption, and disconnected from reality at the edge.

The Evidence Is Clear

This white paper has made a clear and evidence-based argument:

> Embedded logic at the edge is the only architecture capable of surviving, adapting, and delivering effect in a spectrum-contested battlespace.

From the jamming corridors of the Donbas, to the cyber-scrambled skies of the Red Sea, to the compromised cloud systems in Gaza, the message is consistent: Centralised AI fails under fire. Embedded logic does not.

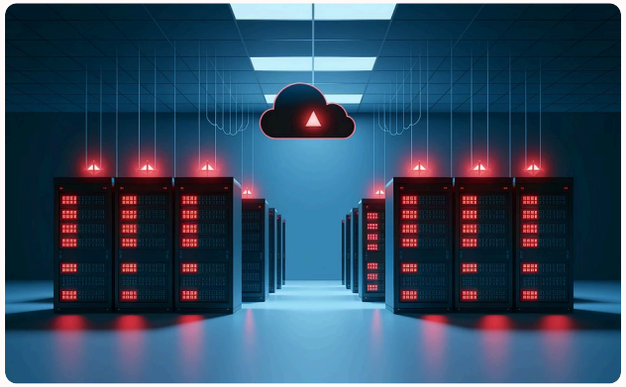


Donbas Jamming Corridors

Areas where centralized systems consistently fail under electronic warfare pressure

Red Sea Cyber-Scrambled Skies

Maritime environments where signal disruption creates critical vulnerabilities



Compromised Cloud Systems

Infrastructure vulnerabilities exploited in modern warfare

Strategic Imperatives Moving Forward

Design for denial

Assume jamming, spoofing, and cyber assault. Plan for disconnection.

Preserve sovereignty

Control the logic, own the outcome.

Embed mission logic

Push decision capability into the platform, not the datacentre.

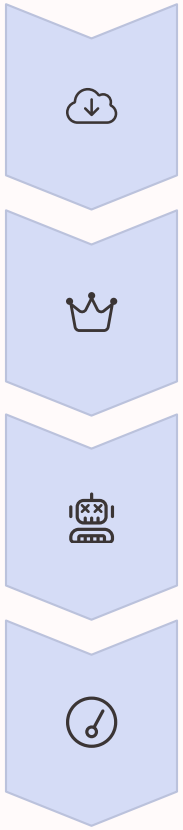
Close the loop

Shrink latency until the edge is the centre of action.

This is not just a technical shift—it is a doctrinal one. A nation's ability to fight in the grey zone, to persist in degraded environments, and to act without waiting for a signal is now a core pillar of deterrence.

Call to Action

For military planners, capability sponsors, and defence industry leaders across NATO and Europe, the course of action is clear:



Transition from cloud-first to edge-first AI design

Prioritize autonomous operation at the tactical edge

Fund sovereign logic development as a matter of national security

Invest in domestic AI capabilities that can operate without external dependencies

Mandate embedded autonomy in all next-generation tactical platforms

Ensure systems can function effectively when communications are compromised

Benchmark all AI-enabled systems against contested spectrum survivability

Test and validate performance under realistic electronic warfare conditions

The Future of Military AI

Survivability is the new credibility.

Systems that can withstand cyber and electronic attacks will define military capability in the coming decade.

Edge AI is no longer optional—it is operational.

The transition from theoretical advantage to battlefield necessity has already occurred.

> "Victory in future war will belong not to the best connected, but to the best prepared to disconnect."