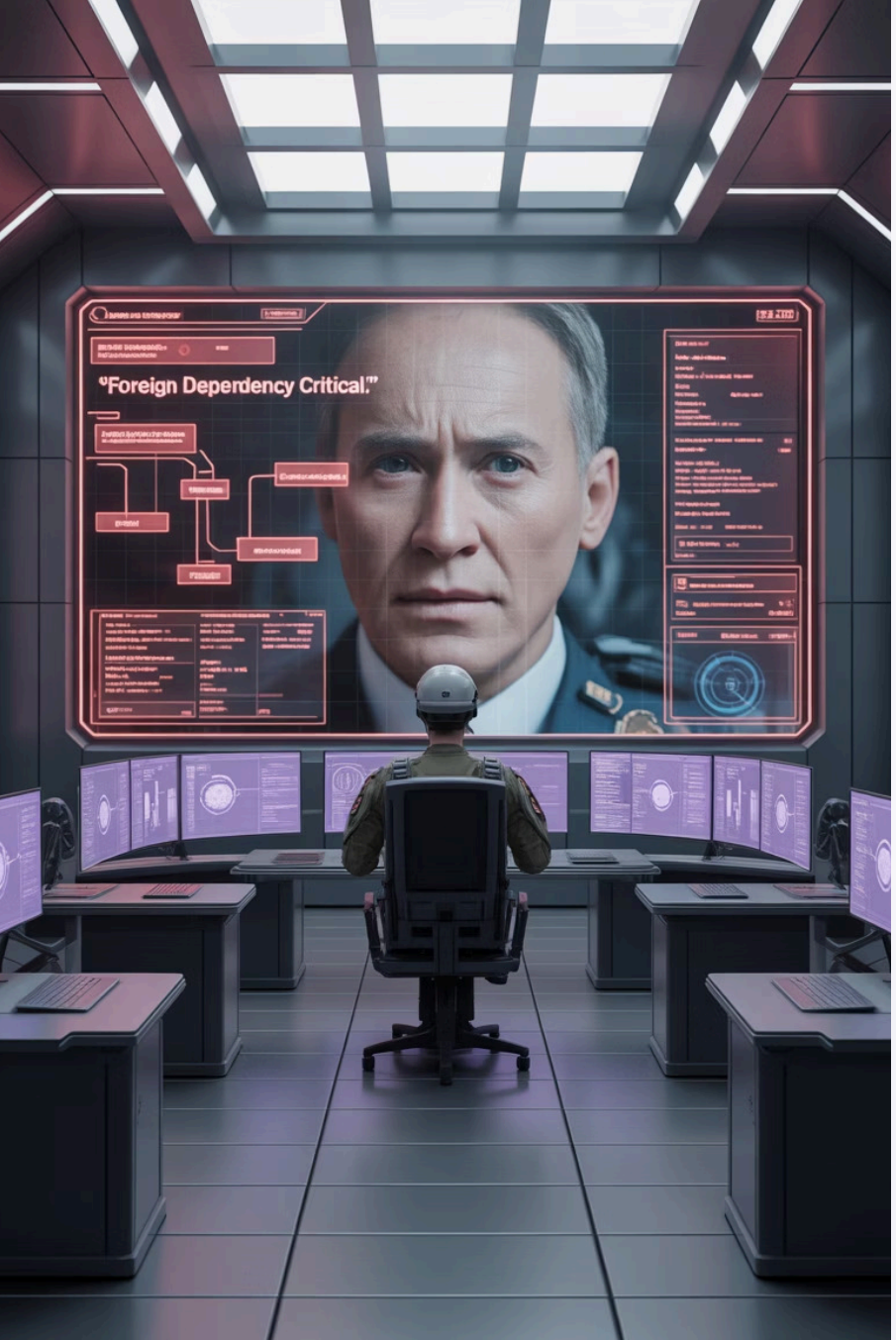


Chapter 9: Dependency by Design – How Centralised AI Undermines Sovereignty

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

Published by Ambient Stratagem

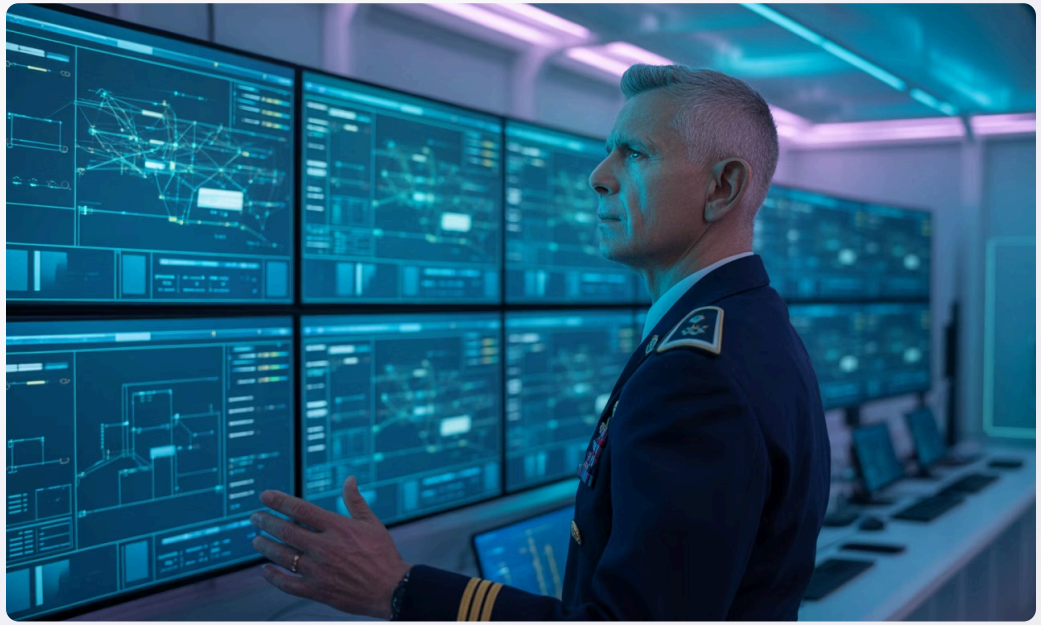
June 2025

"You cannot outsource the right to decide." — European Defence Agency Commissioner, 2024

The Strategic Paradox of AI Dependency

The ability to command, control, and adapt one's own technology is a foundational principle of national sovereignty. Yet in the race to modernise military capability with AI, many Western states have surrendered key elements of control—quietly, incrementally, and structurally. The result is a strategic paradox: systems designed to enhance national security are increasingly dependent on foreign-owned logic, platforms, and providers.

This chapter examines how centralised AI architectures—especially those hosted in foreign data centres or operated under external legal regimes—introduce systemic risk to sovereign defence and undermine strategic independence.



The Architecture of Vulnerability

Foreign Cloud Infrastructure

Are trained and hosted by US-based hyperscale cloud providers.

External Legal Frameworks

Operate on infrastructure governed by foreign legal frameworks, including the US CLOUD Act.

Limited Transparency

Are not fully auditable, with opaque inference logic, proprietary datasets, and limited explainability.

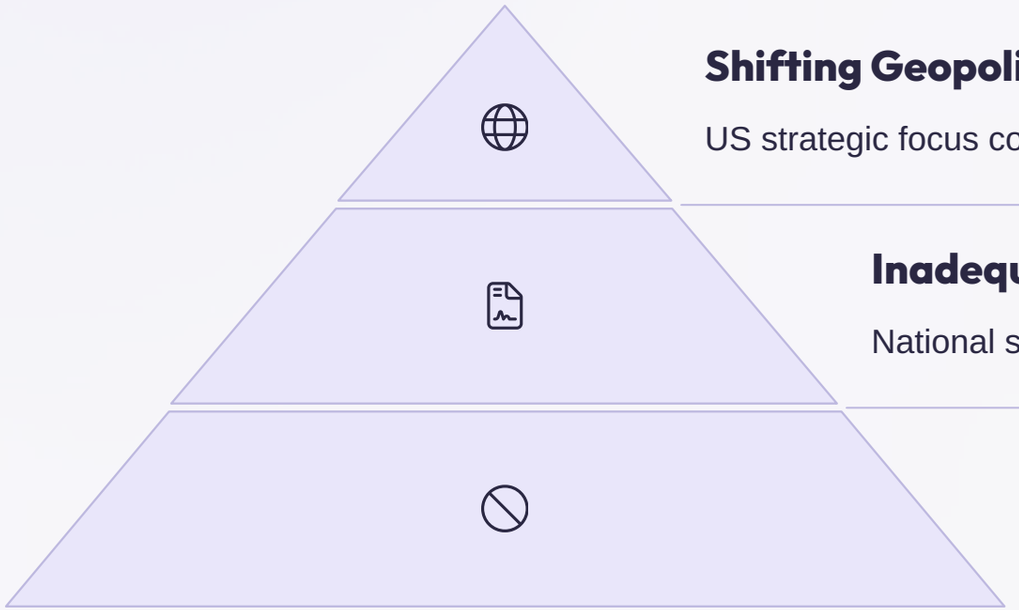
Constant Connectivity Required

Require constant connectivity to remote compute environments—typically outside national borders.

These dependencies mean that even when systems are physically operated by national forces, their ability to function—or be adapted, verified, or redeployed—is ultimately beholden to someone else's infrastructure, priorities, and permissions.

"The illusion of control is the most dangerous form of dependency." — French National AI Security Briefing, 2025

Political and Legal Constraints



Shifting Geopolitical Focus

US strategic focus continues to pivot to the Indo-Pacific

Inadequate Security Exemptions

National security exemptions in cloud contracts often fall short

Export Control Limitations

ITAR, EAR, dual-use restrictions can delay or prevent access

The geopolitical landscape is shifting fast:

US strategic focus continues to pivot to the Indo-Pacific, leaving European states uncertain of long-term tech access and alignment.

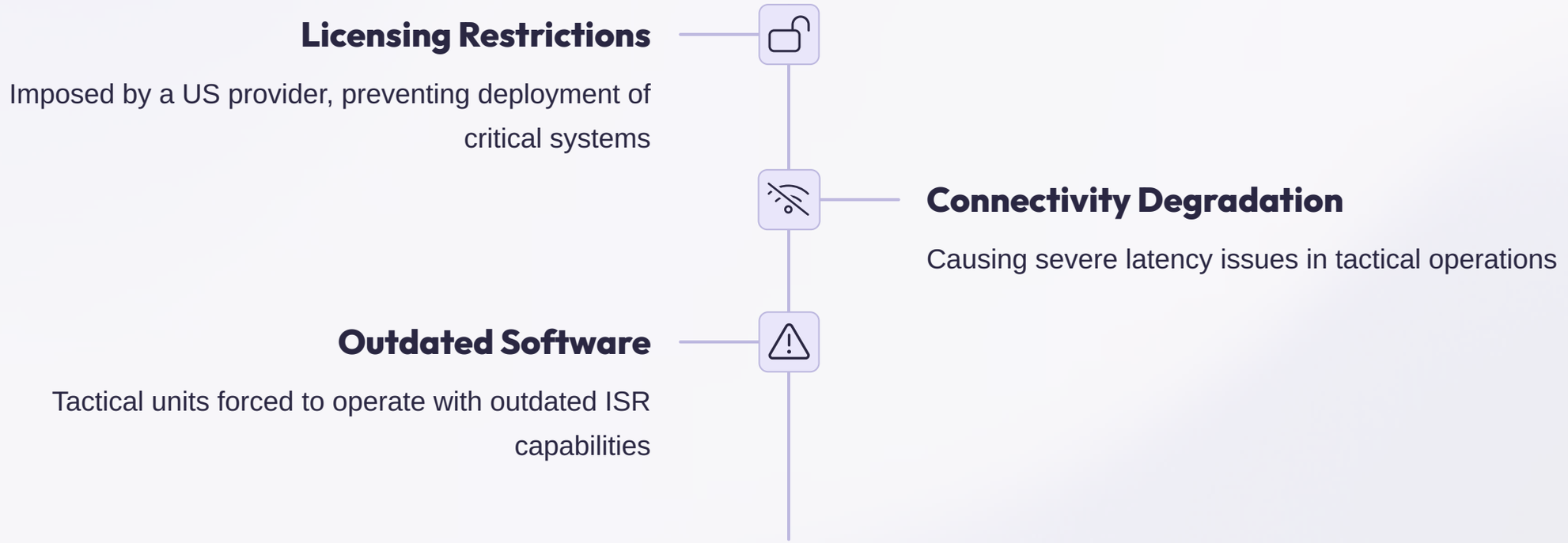
National security exemptions in cloud contracts often fall short of operational need, particularly in expeditionary or special operations.

Export control regimes (ITAR, EAR, dual-use restrictions) can delay or prevent access to key AI capabilities—even among allies.

If critical AI capabilities are tied to centralised models hosted outside sovereign control, nations may find themselves:

- Unable to deploy systems where needed.
- Unable to adapt logic to changing ethical, legal, or operational parameters.
- Exposed to legal challenges in coalition or humanitarian missions.

Case Study: The AI Cold Start in Gaza, 2024



During the October 2024 escalation in Gaza, Israeli forces were unable to rapidly deploy certain advanced pattern-recognition models due to:

- Licensing restrictions imposed by a US provider.
- Latency issues caused by connectivity degradation.
- Lack of local fallback models, meaning some tactical units operated with outdated software for critical ISR tasks.

The lesson was clear: cloud-based AI cannot be assumed to be available, adaptable, or deployable—especially in time-critical combat conditions.

A Fragility Hidden in Plain Sight

Model Layer

Proprietary LLMs, vision models, and classifiers are rarely available for sovereign modification

Infrastructure Layer

Compute and storage are often provisioned via transnational platforms

Governance Layer

Legal, ethical, and policy constraints are often driven by the host nation of the provider—not the user

The AI boom of the early 2020s has created an illusion of abundance. Models are everywhere. Tools are available. But underneath the apparent abundance lies a chronic shortage of sovereign control.

Strategic dependency now exists at multiple layers:

- Model layer: Proprietary LLMs, vision models, and classifiers are rarely available for sovereign modification.
- Infrastructure layer: Compute and storage are often provisioned via transnational platforms.
- Governance layer: Legal, ethical, and policy constraints are often driven by the host nation of the provider—not the user.

This fragility will be tested in future conflict—either by adversary disruption, legal divergence, or simple commercial unavailability in wartime.

Conclusion: The Architecture of Dependency

Command Authority

No military would outsource its command authority to a foreign general.

Logic and Control

Yet many are now embedding critical elements of logic, inference, and control in systems they do not own and cannot alter.

Architectural Dependency

Sovereignty is being lost not through espionage or betrayal, but through architecture—a dependency by design.

No military would outsource its command authority to a foreign general. Yet many are now embedding critical elements of logic, inference, and control in systems they do not own and cannot alter.

Sovereignty is being lost not through espionage or betrayal, but through architecture—a dependency by design.

NEXT - Chapter 10: Embedded Logic and the Architecture of Sovereignty