Chapter 12: From Dependency to Deterrence – Strategic Autonomy in the AI Age

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

"Deterrence is credibility under pressure. And credibility comes from the ability to act without permission." — NATO Strategic Concept, 2022 (interpretive briefing)

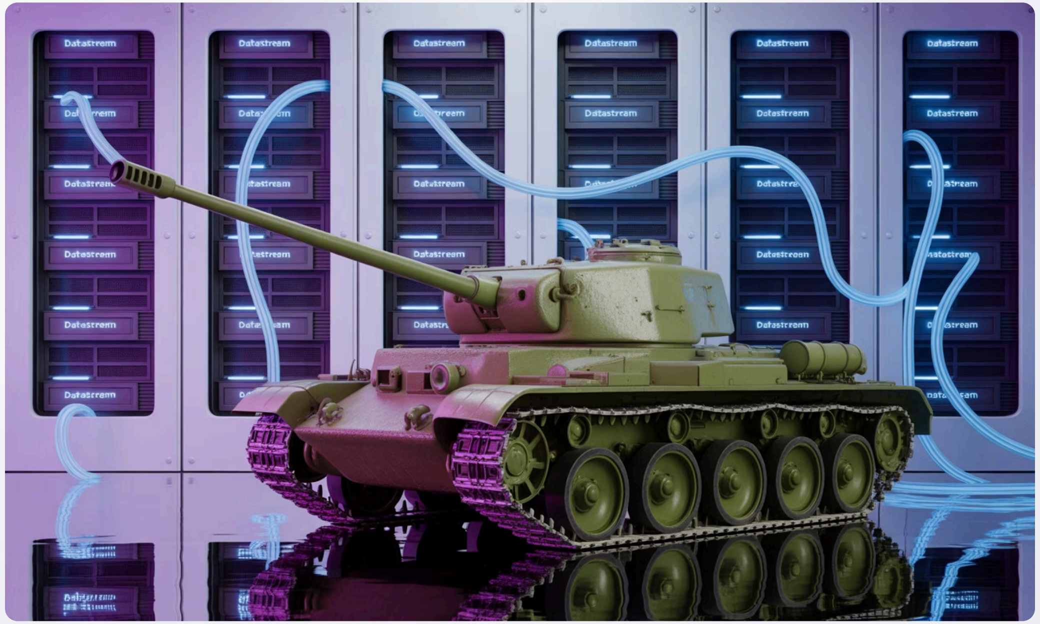
Published by Ambient Stratagem

June 2025

Redefining Deterrence in the 21st Century

In the 20th century, deterrence was defined by visible force—tanks, ships, aircraft, alliances. In the 21st, deterrence is increasingly defined by invisible infrastructure: who controls the data, the networks, the logic—and whether that control survives contact.

This chapter argues that AI is now a strategic asset—on par with energy, encryption, and aerospace capability. And as with all strategic assets, states must be able to operate it independently, transparently, and under national command. The shift to embedded logic at the edge is not just a technical evolution—it is a strategic transition from vulnerability to deterrence.



The Strategic Risk of Inaccessible AI

Foreign infrastructure

Defence systems reliant on overseas cloud computing resources may become inaccessible during conflicts

Foreign legal frameworks

AI systems subject to other nations' regulations can be restricted without warning

Commercial availability

Dependency on vendor-controlled AI creates vulnerability to policy changes or embargoes

Defence planners must now confront an uncomfortable reality: in a crisis, AI systems reliant on these factors may not be accessible when they are most needed. Whether due to geopolitical divergence, embargo, cyber attack, or political will, access to centralised AI may be delayed, degraded, or denied.

This fragility is invisible in peacetime, but becomes decisive under pressure.

Examples:

- 2024: A Northern European nation had to suspend a counter-UAV programme after model updates failed to deploy—due to a policy shift by the US-based provider.
- 2025: During Indo-Pacific war gaming, an allied reconnaissance platform lost AI functionality mid-scenario after cloud-access tokens expired during jamming.

Embedded Logic Enables Persistent Deterrence

Logic is present on the platform at all times

AI capabilities remain functional regardless of external connectivity

No remote permission is required

Mission-critical functions can execute without external authorization

Offline updates and adaptations

Systems can be reconfigured at the unit or national level

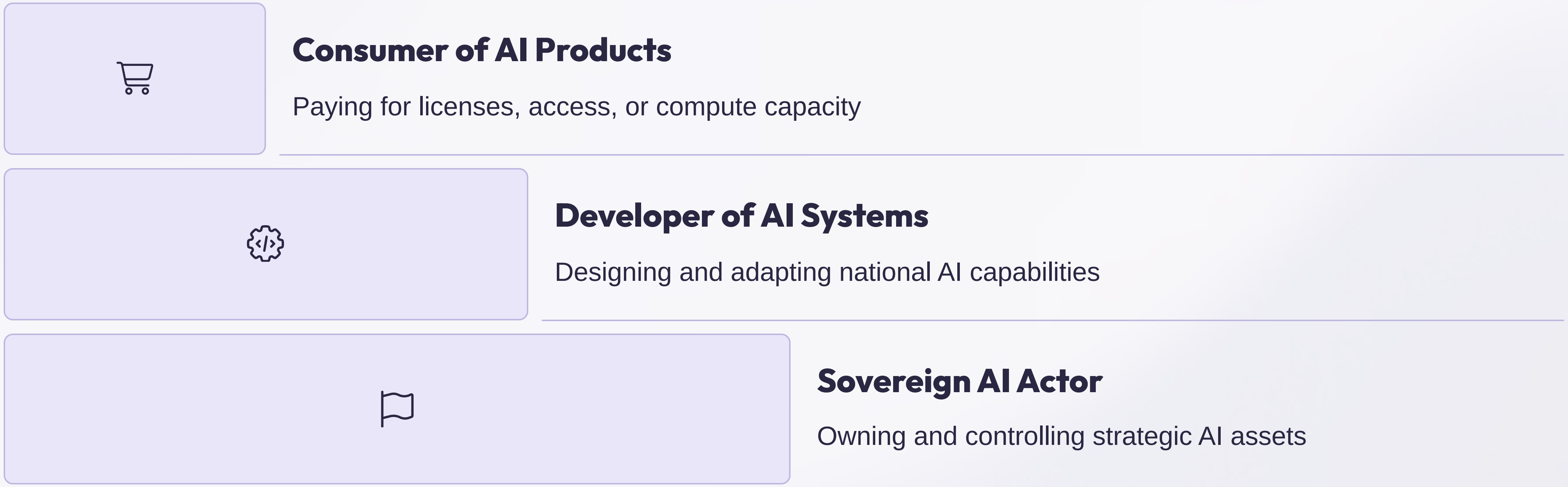
Embedded AI systems remove these vulnerabilities by ensuring these capabilities, allowing nations to:

- Maintain credible autonomous capability, even in total isolation.
- Reconfigure AI systems in response to threat evolution, not commercial timelines.
- Project technological independence, reinforcing strategic posture.

> "Strategic autonomy doesn't mean going it alone. It means being able to stand alone—if we have to."

— EU Defence Cooperation Dialogue, 2025

From Consumer to Actor: AI as a Sovereign Instrument



Consumer of AI Products

Paying for licenses, access, or compute capacity

Developer of AI Systems

Designing and adapting national AI capabilities

Sovereign AI Actor

Owning and controlling strategic AI assets

Many nations have become consumers of AI products—paying for licenses, access, or compute capacity, without owning the underlying architecture.

Embedded AI allows a shift:

- From consumer to actor: states can design, own, deploy, and adapt their AI.
- From licence-based to capability-based AI: systems become national assets, not rented services.
- From external reliance to internal agility: forces can respond at machine speed without waiting for remote inference.

This transition mirrors the historical evolution of air power: at first a niche, then a dependency, and finally a core sovereign domain.

Strategic Stability Through Sovereign Capability

Immune to Third-Party Shutdown

Embedded logic systems cannot be remotely deactivated by external actors, ensuring operational continuity even during geopolitical tensions.

Free from Commercial Bottlenecks

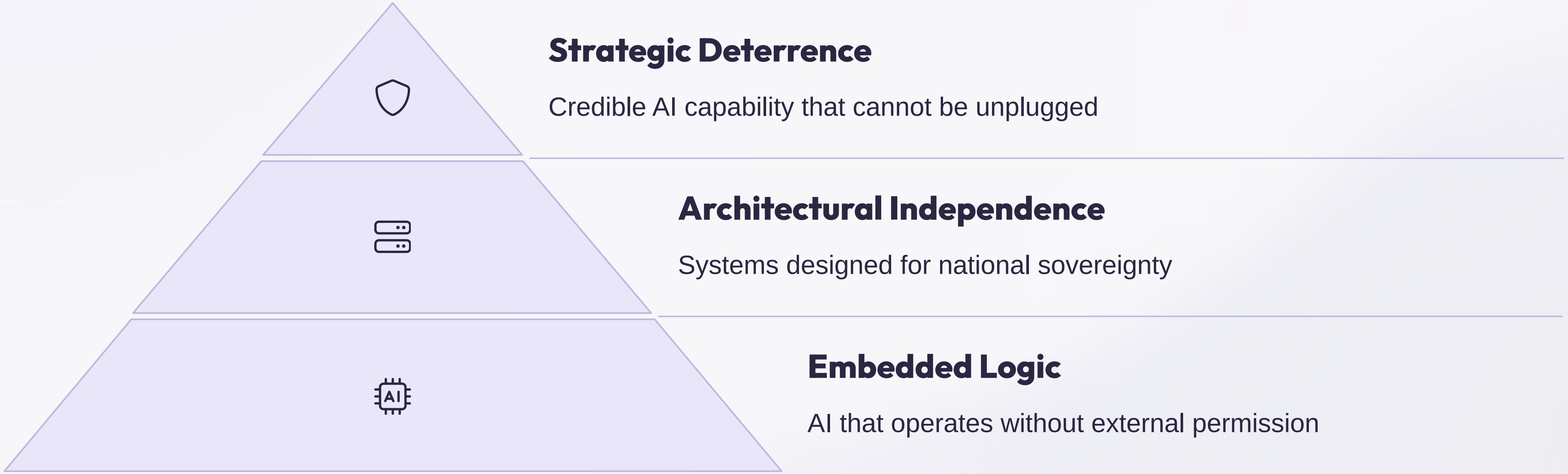
National defence capabilities remain unaffected by vendor priorities, supply chain issues, or commercial policy changes that might otherwise delay critical functions.

Protected from Dependency Risks

Strategic systems maintain integrity and reliability through national control, eliminating vulnerabilities from international divergence or conflicting interests.

In an age of great power competition, strategic stability rests not on promises, but on readiness. Embedded logic systems reinforce deterrence not by being louder—but by being credible, persistent, and always under national control.

Conclusion: AI as National Deterrence



Strategic Deterrence

Credible AI capability that cannot be unplugged

Architectural Independence

Systems designed for national sovereignty

Embedded Logic

AI that operates without external permission

AI is now part of national deterrence posture. It informs surveillance, command, fire control, and targeting.

To trust it, nations must own it. To own it, nations must embed it.

Strategic autonomy in the AI age begins with architectural independence—and ends with deterrence that cannot be unplugged.

NEXT - Strategic Sovereignty and Technological Independence - Conclusion & Call to Action