

The Strategic AI Sovereignty Challenge: How Military AI Dependencies on Foreign Ecosystems Shape Global Defense Postures

Your military AI procurement may look state-of-the-art—but is a hidden foreign dependency already threatening your national security? The real risk is less about algorithms, more about invisible control.

The Silent Chess Game: Military AI and the Race for Tech Sovereignty

Pull back the curtain on almost any major military AI system in 2024, and you'll discover uncomfortable truths: beneath the surface of sovereign procurement, most armed forces run on the invisible scaffolding of foreign technology. This is not just a back-office IT

issue—it's a strategic vulnerability reshaping alliances, deterrence, and even the future of warfare itself.

The Facade of Independence

Countries trumpet their independent AI-driven platforms, next-gen drones, or decision-support suites. But how much of that stack is truly "owned"? Dive deeper, and you'll find crucial layers—whether GPUs optimized for machine vision, pretrained language models, or cloud-based AI deployment platforms—sourced from, or outright controlled by, the US, China, or a handful of multinational tech giants.

> **The era of hardware sovereignty is over; in AI, the code—and the cloud—is king. Who controls the update pipeline, the model weights, or the API keys?**

Dependency as a Strategic Risk

Why does this matter? Because in a crisis, dependencies turn into levers. If your military's AI targeting suite is built on American AI cloud infrastructure, a snap policy change in Washington could shut systems down in an instant. If AI-powered cyber defense engines rely on Chinese neural architectures, vulnerabilities—or backdoors—could be exploited by a competitor, or simply rendered obsolete overnight by a denied update.

From Tech Stack to Policy Stack

Sovereignty in AI is not just technical—it's political, legal, and operational. The value of any given AI model is inseparable from the ecosystem supporting it: the chip foundries, the open source model standards, the regulatory guarantees underpinning data flows.

- **Hardware dependencies:** 90% of advanced AI chips today are produced outside the EU, with logistical chokepoints wholly outside their control.
- **Software dependencies:** Most "European" military AI engines rely on open source or closed libraries from American or Chinese origin, making audits and regulatory compliance an illusion.
- **Cloud dependencies:** True digital sovereignty is impossible if mission-critical AI is

run on third-party global hyperscalers.
- **Data dependencies:** AI's hunger for data often leads states to license datasets or labeling workflows from foreign suppliers, embedding risk deep within the model.

Case Studies: Dependency in Action

Ukrainian Battlefield AI—Powered by the West

The ongoing war in Ukraine is a real-world proving ground. Much of Ukraine's sophisticated AI-based targeting and reconnaissance solutions run atop US-supplied cloud AI infrastructure and models. This accelerates capability—but leaves Ukrainian planners constantly gaming if/when their access will be throttled for political reasons.

European AI Sovereignty: Ambition vs. Reality

The EU's stated ambition is "digital strategic autonomy" for defense applications. But decades of procurement focused on price/performance means supply chains for core AI tech—think chips from TSMC/Nvidia, cloud from AWS/Microsoft, NLP models from OpenAI—remain externalized. Recent efforts at indigenous chip fabbing and open source model hubs (EC Digital Decade) are still nascent and years away from parity.

The Real-World Impact: From Deterrence to Decisiveness

So what? Military postures are being fundamentally reshaped in at least three ways:

1. **Deterrence becomes porous:** If your adversary can switch off your AI by squeezing API or cloud access, your threats ring hollow.
2. **Procurement cycles slow down:** As states wake up to dependency risk, vetting and indigenization slow the fielding of urgently needed AI tools.
3. **Coalitions fracture:** Dependency creates a two-tier alliance system—those with homegrown AI platforms, and those at the mercy of foreign TechStack policy.

Technology Governance as the New Theatre

The traditional tools of international control—export bans, tech embargoes, supply chain

interventions—now play out not on hardware, but at the level of models, cloud, and update permissions. The state with the kill switch has tremendous influence far beyond traditional espionage or hacking.

Rethinking AI Sovereignty: Beyond the Buzzwords

Sovereignty is not about "autarky," but about knowing—and controlling—what can be switched off, sabotaged, or surveilled at a distance. It's about:

- Building deep local capacity in AI hardware and software—however costly or slower that makes initial deployments
- Designing redundant, fail-closed models: systems that degrade gracefully if external dependencies are cut
- Negotiating multi-polar "sovereignty pacts" with allies, where no single supplier holds all the keys

What Military Planners Can Do Now

1. Conduct full-stack dependency audits. Don't stop at the source code; go all the way down to firmware, data lineage, and supply contracts.
2. Invest in indigenous AI research—open source, open weights, local Clouds, and cross-border trusted data enclaves.
3. Develop diplomatic contingency protocols: what bilateral or multilateral levers exist if an AI vendor acts against your core interests?

Conclusion: The Coming AI Realignment

Over the next decade, the question won't just be "Who has the best AI?"—but "Who controls the critical points in the AI ecosystem?" The answers will redraw defense alliances, determine the winners of 21st-century deterrence, and set the protocols for war and peace in an era of automated, always-on conflict risk.

In military AI, sovereignty is not about who trains the algorithm, but who owns its dependencies—and that's the next true battlefield.



WRITTEN BY

Artur Markus

Software engineer in Basel building AI infrastructure and agentic systems, with a background in pharmaceutical automation, GxP compliance, and validation. I help teams turn AI from a chatbot into a reliable operational layer.

Book a meeting