Civilian AI Is Already at the Front. Europe's Rules Can't See It.

Project Maven made the problem visible. The deeper break came later, when war and procurement turned commercial digital infrastructure from an experiment into a dependency.

Europe controls dangerous exports, but the technology shaping surveillance, reconnaissance and targeting increasingly does not arrive as a recognisable military object. It arrives as a model, cloud service, sensor feed or software update that can be adapted after purchase. The problem is therefore not simply that Brussels forgot to put "AI" on a list. It is that military capability is increasingly assembled from relationships among models, data, infrastructure, vendors and users, while much of Europe's control architecture still begins by classifying the item before use.

The model that sorts parcels can also support reconnaissance

A vision system trained to count boxes can, with retraining and different data, classify people or vehicles in aerial imagery. The same problem spans commercial drones, satellite imagery, cloud machine learning and general-purpose models.

EU law is not blind to end use. Regulation (EU) 2021/821 controls listed dual-use items and includes catch-all and national mechanisms; Article 5 links certain unlisted cyber-surveillance exports to their intended end use and human rights risks. But an ordinary general-purpose model is not controlled merely because it could later be adapted for military reconnaissance. The AI Act sets another boundary: Article 2(3) excludes systems insofar as they are placed on the market, put into service or used exclusively for military, defence or national-security purposes. Mixed uses still matter. The claim is not that repurposed AI falls outside every European rule. It is narrower: foreseeable military repurposing of an otherwise ordinary model is not, by itself, a general Union-level export trigger (Van Daalen, Van Hoboken & Rucz, 2023; Parisini, 2025).

Maven was the warning. 2022-2024 was the structural break.

Project Maven remains the right place to start, but not to stop. In 2017-2018, the Pentagon's use of commercial machine learning for drone-footage analysis exposed the **military - Silicon Valley relationship**. Google employees protested; Google declined to renew the contract and adopted principles restricting weapons work. Maven made the convergence politically visible.

That is also why it was not yet the strongest point of lock-in: a major vendor could still walk away. The more consequential inflexion came in 2022-2024. Russia's full-scale invasion of Ukraine showed at operational scale that military effectiveness could depend on private satellite imagery from Elon Musk, commercial connectivity, cloud infrastructure, analytics, dual-use drones and software. Research on the platform-military nexus and "infrastructural entanglement" treats this as evidence that **private digital infrastructure had become part of wartime capacity itself** (Coveri, Cozza & Guarascio, 2025; Javadi, 2026).

Procurement institutionalised the shift. **The Pentagon's 2022 Joint Warfighting Cloud Capability award made this concrete: Amazon, Google, Microsoft and Oracle joined a $9 billion multi-vendor framework, embedding commercial cloud directly in defence infrastructure**. Multi-vendor military cloud programmes and the growth of defence-tech markets meant that refusal by

one firm no longer removed the capability from the market. The unit of military capability had moved from a controversial project to an ecosystem. Google's later relaxation of its earlier weapons language is therefore better read as confirmation than cause.

Why the shift locks in

Paul David's QWERTY analogy is useful if treated as a mechanism, not as a proof of inefficiency. Increasing returns and complementarities can make an adopted system harder to reverse (David, 1985; Arthur, 1989). Here the mechanisms are concrete: models depend on cloud, data pipelines and sensors; organisations redesign workflows around platforms; licences and security accreditation raise switching costs; and commercial vendors often update faster than bespoke defence programmes. Separate military systems are not always worse — security, resilience and sovereignty can favour them — but a wholly separate stack becomes harder to sustain once the commercial one is embedded.

That changes authority as well as technology. Vendors can shape access, features, update cycles and contractual limits. Smaller states gain capability while depending on infrastructure they do not control. Winner's argument that artefacts embody political arrangements, and Beniger's account of information infrastructure as organisational control, help explain why procurement choices can redistribute practical power (Winner, 1980; Beniger, 1986).

What Europe should change

First, put procurement first. Defence contracts for AI-enabled reconnaissance, decision support and targeting-adjacent functions should disclose material civilian dependencies: model providers, cloud infrastructure, external data, update rights and suspension conditions.

Second, extend end-use logic narrowly. "Reconnaissance-capable AI" is too broad. A better trigger would combine exporter knowledge or official notification with specified military or intelligence functions — such as ISR, target development, targeting support or autonomous weapon control — and defined end users or destinations.

Third, clarify how the AI Act applies when systems developed for civilian use are later adapted for defence, or when one model serves both markets. Governance should follow lifecycle and deployment context, not a one-time label.

Finally, publish aggregated evidence on Article 5 notifications, specifications, authorisations, denials and national controls. Without such data, it is difficult to tell whether the real problem is legal coverage, administrative capacity or enforcement.

The date that matters

The history is best told in three stages: earlier dual-use technologies established the pattern; Maven made the political problem visible; 2022-2024 normalised commercial infrastructure as military capability. That distinction changes the remedy: If Maven was the turning point, stronger corporate ethics looks sufficient. If 2022-2024 was the structural break, Europe must govern procurement, end-use knowledge and dependency across the supply chain. **Civilian AI is already at the front. The regulatory question is whether Europe can see the relationships that put it there**!

Selected sources

Arthur (1989), Economic Journal 99(394), 116-131.
Beniger (1986), The Control Revolution.
Coveri, Cozza & Guarascio (2025), Review of Political Economy.
David (1985), American Economic Review 75(2), 332-337.
Javadi (2026), Contemporary Security Policy.
Parisini (2025), Global Public Policy and Governance.
Taddeo et al. (2021), Philosophy & Technology.
Van Daalen, Van Hoboken & Rucz (2023), Computer Law & Security Review.
Winner (1980), Daedalus 109(1), 121-136.
Regulation (EU) 2021/821; Regulation (EU) 2024/1689.