



What the Italian Defense Risks if AI Does Not Become the Center of the System

Published on 11/01/2026

When it is said that Artificial Intelligence “is not applied” in Defense, it often means something specific: not that there are no experiments, but that **AI is not yet integrated in a widespread, standardized, and scalable way** in key processes (intelligence, C2, logistics, maintenance, cyber, procurement, training), that is, *at the architectural level* and not in individual pilot projects.

In Europe, the push to digitize the armed forces and make Defense “data-centric” is now explicit: NATO and the EU have launched digital transformation programs and strategies, recognizing that **digitalization is the prerequisite** for the effective adoption of AI, cloud, data sharing, and “emerging and disruptive” technologies.

Yet, precisely because the prerequisite is difficult, many countries (including Italy) struggle to turn intention into operational capabilities.

Below, an “unsparing” reading of the main causes of the delay (with a particular Italian focus) and the probable consequences if there is no change of pace.

Digital backwardness: the bottleneck is not “the algorithm”, it is the infrastructure

AI in Defense really works only if there are:

- **accessible and governed data** (not “closed” in silos),
- **adequate networks and cloud** (even in classified environments),
- **end-to-end digital processes** (from data collection to decision-making),
- **standards and interoperability**.

Without this foundation, AI remains a gadget.

The general Italian framework indicates structural weaknesses: the [EU Commission](#) highlights that **only 5% of Italian companies use AI** (below the EU average) and that **only 45.8% of the population** has basic digital skills (also below the EU average).

It is a “civilian” indicator, but Defense draws from the same pool of skills, suppliers, organizational culture, and delivery capacity.

International analyses on the digitalization of European defense also indicate that the transformation is hindered by **procurement, budget alignment, data sovereignty/accessibility, digital underinvestment**, and long timelines (targets for 2030 and beyond).

Practical translation: if you don’t digitize *the machine* first, AI won’t make it run faster; it will only crash against existing limits.

What the Italian Defense risks if AI does not become the Center of the System

Classified data, silos, and “data sharing”: Defense has the data... but often cannot use it

In Defense, the problem is not the lack of data: it is that the data is:

- **classified** (legal and security constraints),

- **heterogeneous** (different formats, variable quality),
- **vertical silos** by armed force/program/supplier,
- often **not reusable** (missing “data products”, catalogs, metadata, governance).

The consequence is that AI cannot be trained and updated continuously, and above all, it cannot be brought “into production” reliably.

This is exactly the point that many Western strategies emphasize: [NATO links the adoption of AI](#) to principles and practices throughout the life cycle, including testing, interoperability, and information security.

Legal, ethical constraints, and responsibility: in Defense, it is not enough for it to “function”, it must be *attributable*

In the military field, the threshold of error acceptability is very different: the question is not only “how accurate is it?”, but:

- who is responsible if it makes a mistake?
- is it explainable and traceable?
- is it governable (can it be deactivated, limited, controlled)?
- how is *certification* done in changing scenarios?

Italian strategic reflection documents insist on the need for **significant human control** and the legal-organizational complexity of deploying AI, as well as the need for governance and implementation plans.

The EU framework is also particular: the AI Act **excludes exclusively military/defense/national security use**, but “dual-use” systems (which also touch on non-excluded purposes) can fall within the regulatory perimeter.

This creates a gray area: many technologies are “civilian+military” and thus impact compliance, supply chain, audit, and contracting.

What the Italian Defense risks if AI does not become the Center of the System
 What the Italian Defense risks if AI does not become the Center of the System

Slow procurement and “risk aversion”: timelines incompatible with the AI technological curve

AI (especially modern, and even more so generative) evolves in very rapid cycles. Defense procurement, however:

- thinks in terms of **years** (even decades),
- tends to crystallize requirements and solutions,
- rewards the reduction of contractual risk more than the speed of iteration.

Result: when a system enters service, it risks being **already outdated** or no longer upgradable.

An [analysis on procurement](#) and the need for “rationalizations/streamlining” highlights the necessity for clarifications and bureaucratic streamlining to make acquisition more effective. And a UK Parliament report (useful as a benchmark, not for “moral comparisons”) clearly states that to grow a defense AI sector, **digital infrastructure, skills, clearance**, and above all a [MOD more capable of working with rapid cycles](#) and non-traditional suppliers are needed.

Industrial structure and competition: few large players, dependent supply chains, “conservative” incentives

The point is well made: **if the market is not very contestable, disruptive innovation struggles to enter.**

In Italy, the defense “champions” are strong and often drive export and capability, but the ecosystem can result in:

- **imbalanced towards a few prime contractors**, with enormous influence on technological choices and supply chains;
- **dependent supply chains** on the ability (and convenience) of the large players to absorb innovation;
- **conservative incentives**: protection of established processes and platforms, supply lock-in, barriers to entry for new suppliers.

Complicating the picture is often the **public-private intermingling** typical of the sector (participations, institutional relations, dependence on public contracts). This can reduce real

contestability and shift attention from technological competition to protecting existing balances.

In the worst cases, “closed” dynamics (patronage, nepotism) and organizational rigidities more akin to administrative logics also emerge:

- slow processes and poor operational flexibility;
- constraints and protections that make it more difficult to quickly reorient people and investments;
- less drive for merit and experimentation.

The result is an ability to innovate and scale technologies like AI and data platforms **less rapidly** compared to more competitive ecosystems, like many realities in Northern Europe and the United States.

Artificial Intelligence at the Pentagon: Google for Office, Palantir for Operations.

An indicator (not exhaustive) of the concentration of large players: in the **SIPRI Top 100** rankings, Italy typically has few companies present; in the 2024 fact sheet, for example, the two Italian companies in the Top 100 total **\$16.8 billion** in arms revenues.

In parallel, the EU Commission highlights that the growth of innovative companies in Italy is hindered by a still weak ecosystem and relatively limited venture capital investments (few “unicorns”): if strong new entrants (startups/scaleups) are lacking, Defense tends to remain more dependent on traditional suppliers even in digital.

Lack of a national “AI leader” and poorly structured public demand: technology is bought, not capability

Here the distinction is crucial:

- **buying an AI product $\neq$ building an AI capability.**

A capability requires:

- data platforms,
- MLOps/ModelOps,
- continuous testing & evaluation,

- internal staff (product owner, data steward, AI safety, cyber),
- contracts that provide for updating, retraining, and performance measures over time.

Without “intelligent demand” (specifications, standards, governance), the risk is the purchase of “turnkey” solutions that **do not integrate**, do not update, or quickly become legacy.

In the Italian AI market, for example, the numbers are growing but with imbalances: in 2024 the market reached **€1.2 billion (+58%)**, driven mainly by experimentation and GenAI; however, the dynamic is often stronger in large companies and slower in smaller realities.

It is consistent with a scenario where the ability to “industrialize” AI is concentrated.

An Italian paradox: “awareness is there,” but systemic adoption is slower

From institutional sources, it emerges that the Italian Defense **declares** a path of digitalization and indicates AI among the central technologies, even with funds/actions linked to the digitalization of the Ministry.

Moreover, strategic analysis documents mention the development of an AI implementation strategy in the Defense sector (ed. 2023) and insist on governance and human control.

So the point is not “it is not talked about”: it is that between **strategy** and **implementation** there is a huge organizational, technical, and contractual leap.

The consequences of delay: what happens if AI remains “pilot” and does not become capability

Technological dependence and loss of operational sovereignty

If you do not develop (or at least control) the data-models-infrastructure chain, you end up depending on:

- foreign suppliers,
- proprietary stacks,
- ungovernable updates and roadmaps.

And while you delay, others accelerate: France, for example, has structured a “system” access to AI models/services through framework agreements and national infrastructure (Mistral AI case, cited by Reuters).

Operational gap: decision speed, C2, ISR, cyber

In modern scenarios (multi-domain, sensor saturation, drones, electronic warfare), the difference is made by:

- data fusion,
- automatic prioritization,
- decision support,
- “machine speed” cyber defense.

A delay here is not “inefficiency”: it is **vulnerability**.

Artificial Intelligence from Poland for German Satellites

Artificial Intelligence from Poland for German Satellites

Weaker national supply chain: less R&D, less “smart” export, fewer talents

If Defense does not create “enabling” demand (standards, testbeds, programs), the supply chain:

- invests less in defense-grade AI capability,
- loses talents to more dynamic markets,
- remains a traditional subcontractor.

The EU today explicitly funds areas like AI within industrial and defense R&D programs (e.g., EDF, projects on AI/quantum/drones). If you are not ready, you risk participating as a junior partner or not transforming funds into lasting industrial capacity.

Purchase of already outdated products: lock-in and waste of expenditure

This is the most concrete consequence of slow procurement:

- you buy when the technology is already outdated,
- without update clauses,
- with closed architectures,
- and you end up paying for endless integrations.

The risk is not only technical: it is **political-industrial**, because it creates a circuit where spending supports incumbents but does not generate technological leap (short-term gain vs long-term capability).

Reputational and strategic effect: you matter less in coalitions

In NATO/EU, the following are increasingly important:

- digital interoperability,
- data sharing,
- common standards,
- speed of innovation.

If you do not bring credible capabilities, you matter less in defining standards, joint programs, and European supply chains.

NATO and artificial intelligence: the JWC trains its teams on the Maven Smart System

NATO and artificial intelligence: the JWC trains its teams on the Maven Smart System

In summary: the causes are structural, not “lack of will”

The main blocks are not (only) technical. They are:

- **incomplete digital foundations** (data, cloud, processes),
- **procurement and risk posture** incompatible with rapid iteration,
- **legal/ethical constraints** requiring governance and certification,
- **industrial ecosystem and innovation** not sufficiently competitive,
- **public demand** that often buys “solutions” instead of “capabilities”.

The result, if not corrected, is a double damage: **military** (operational gap) and **industrial** (defense AI supply chain that does not mature and buys externally, or buys poorly).