AI and Defense: a Significant Step Forward, Now Decisively Towards the Future

Published on 28/02/2026

There comes a moment when a technology stops being "promising" and becomes inevitable. For Defense, that moment has arrived: Artificial Intelligence is no longer an optional choice or a niche experiment, but a strategic lever that impacts operations, organization, training, and industry relations. This is the central message of the **"AI and DEFENSE – Defense Strategy on Artificial Intelligence, 2026 Edition"**, which outlines a concrete and ambitious path, set on short timelines and measurable objectives similar to what the United Kingdom already did in 2022.

AI and Defense: a Significant Step Forward, Now Decisively Towards the Future

A Clear Vision: Integrate Quickly, but Responsibly

The strategy starts with a clear observation: contemporary competition is accelerated, multi-domain, hyper-informed. In this context, AI becomes the element that allows **reducing the technological gap**, strengthening Italy's credibility in alliances (NATO and EU), and above all, increasing operational effectiveness without losing sight of values.

The document emphasizes two fundamental “pillars”:

- **responsible, ethical approach in compliance with International Humanitarian Law (IHL)**;
- **human control and responsibility of the command line**, because technology should amplify decision-making, not replace it.

This framework is not a detail: it is the condition to ensure that innovation is sustainable, interoperable with partners, and defensible even on political and legal grounds.

Strategic Autonomy and Technological Sovereignty: The Direction is “In-House”

The core of the “step forward” lies in the declared objective of **strategic autonomy** and **technological sovereignty**. Translated: buying solutions is not enough. Defense must maintain critical internal capabilities to:

- train/update models even with recent data and in challenging contexts;
- understand algorithms, limits, biases, and risks;
- ensure compliance with IHL, doctrine, and values;
- maintain operational systems even without external support.

This is not an “ideological” stance, but a practical response to three real problems: supplier dependencies, vulnerabilities (even intentional), and the risk of losing freedom of action in geopolitical crises or in case of corporate failures.

AI and Defense: a Significant Step Forward, Now Decisively Towards the Future

Enabling Assets: Talents, Data, Algorithms, Computing, and Secure Networks

Every strategy is credible if it names the material conditions that make it possible. Here, Defense does so, clearly indicating the pillars:

- **qualified human resources**, with attention to “talents” and their attraction/retention;
- **data** (integrity, quality, absence of bias, overcoming “silos” and governance);
- **algorithms** (development, validation, maintenance, and certification);
- **proprietary computing capacity**, with high requirements (also in perspective of HPC and hybrid HPC–quantum);
- **secure networks and connectivity**, with resilience and continuity as non-negotiable criteria.

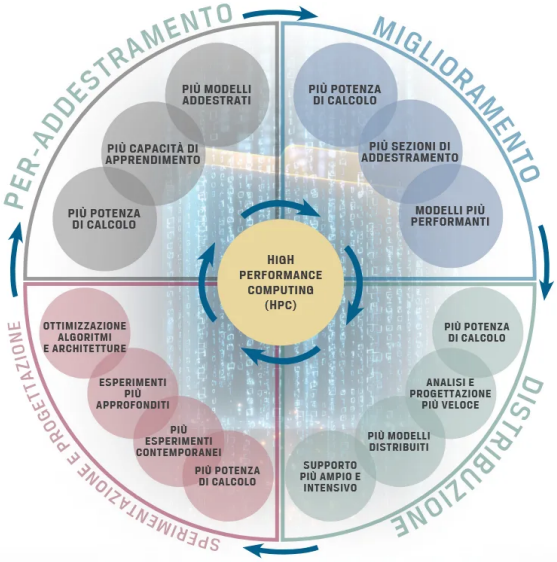
The very operational approach is striking: computing is not an “IT luxury,” but the factor that fuels a virtuous cycle (more computing → more experiments → better models → more capacity) that determines the pace of advantage.

A “Modular” and Fast Path: 1 Year, 2 Years, 3 Years

The strategy chooses an aggressive timeline, precisely because AI is advancing rapidly. The path is divided into three horizons:

- **short term (within 1 year)**: consolidate enabling conditions (governance, infrastructure, skills, processes, obstacle removal);
- **medium term (within 2 years)**: implement priority operational projects;
- **long term (within 3 years)**: widespread, secure, and sustainable integration in all areas of Defense.

This is a key point of the “decisively towards the future”: not a wish list, but a schedule that makes ambition controllable and verifiable.



AI and Defense: a Significant Step Forward, Now Decisively Towards the Future

Four Areas of Intervention: Where AI Truly Changes the Game

The strategy identifies four main areas covering the entire Defense machinery.

1) Operations: Decision Superiority, Engagement Speed, Multi-Domain Protection

In the modern battlespace, the mass of data and battlefield transparency make human analysis capacity alone insufficient. AI is described as a tool for **decision augmentation**, “adaptive” wargaming, predictive analysis, multi-source intelligence, and protection against cyber/electromagnetic threats and against drones/swarms.

The document also addresses the more sensitive implications (such as autonomous weapon systems) emphasizing the relevance of ethical profiles and governance.

2) Organizational Contexts: Productivity, Services, Processes

Here there is a concrete promise: to achieve rapid benefits. It explicitly mentions tools for individual productivity and a possible “Defense” Large Language Model trained on internal documentation, as a prerequisite for knowledge management, drafts, summaries, information extraction, and terminological consistency.

Alongside this: user assistance with natural language, integration with automations (RPA), and, in perspective, AI agents for unstructured problems — always with the rule: human judgment must not be eclipsed.

3) Training, Education, and Research: AI Culture and Digital Mindset

The idea is clear: without widespread training, adoption is fragile. It talks about structured **AI literacy** (cognitive, operational, critical, and ethical-normative dimensions) and reskilling/upskilling to bridge generational gaps and build a mixed human-machine workforce.

4) Industry: National Ecosystem, Open Innovation, More Agile Procurement

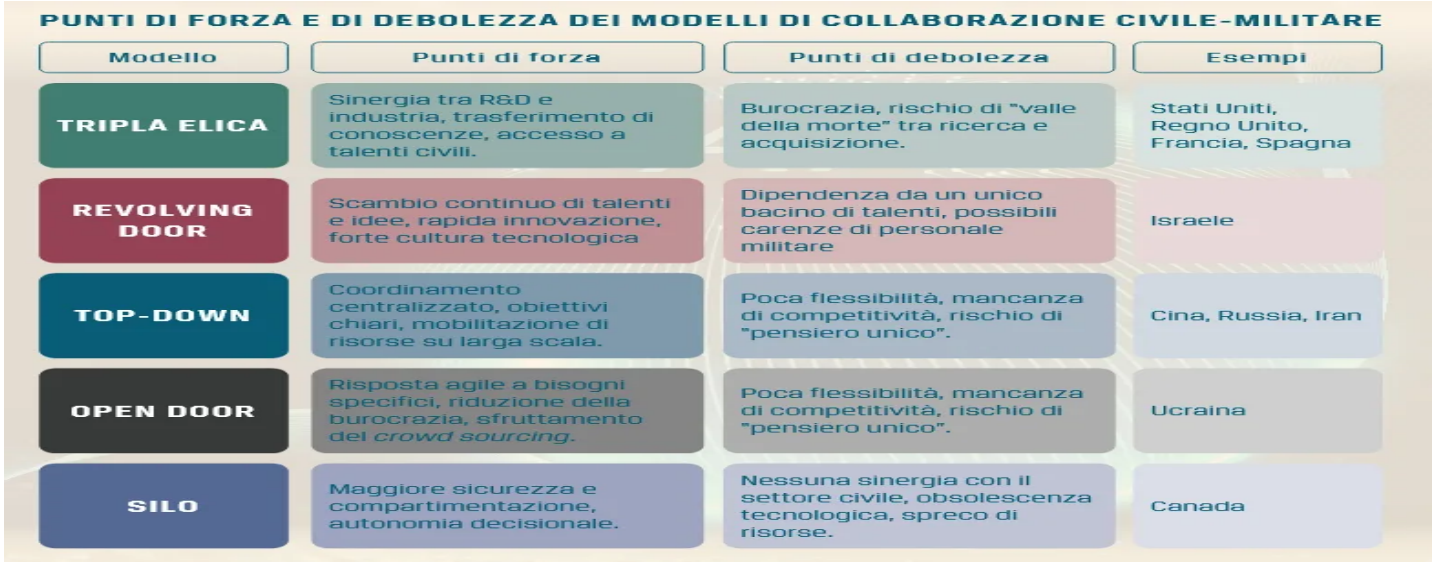
The document values the national industrial ecosystem (large players, but also startups and SMEs), with a shift towards partnerships, technological scouting, and more agile mechanisms for pilot projects. The goal is twofold: accelerate innovation and reduce dependencies, strengthening a competitive “Defense Tech” base.

Governance and Implementation: UIA and LIAD as the Central Engine

To avoid fragmentation, the strategy provides for multi-level governance with two mainstays:

- **Office for AI (UIA)**: direction, supervision, strategic coherence, relations, and ethical-legal oversight;
- **AI Laboratory for Defense (LIAD)**: center of excellence and **AI Delivery Center**, aimed at prototyping, experimenting, and operationalizing solutions in synergy with end users.

Decisive element: within 3 months of approval, an **Implementation Plan** with actions, responsibilities, and **KPI** monitoring is expected. This is where the strategy stops being a “declaration” and becomes management.



PUNTI DI FORZA E DI DEBOLEZZA DEI MODELLI DI COLLABORAZIONE CIVILE-MILITARE

Modello	Punti di forza	Punti di debolezza	Esempi
TRIPLA ELICA	Sinergia tra R&D e industria, trasferimento di conoscenze, accesso a talenti civili.	Burocrazia, rischio di "valle della morte" tra ricerca e acquisizione.	Stati Uniti, Regno Unito, Francia, Spagna
REVOLVING DOOR	Scambio continuo di talenti e idee, rapida innovazione, forte cultura tecnologica	Dipendenza da un unico bacino di talenti, possibili carenze di personale militare	Israele
TOP-DOWN	Coordinamento centralizzato, obiettivi chiari, mobilitazione di risorse su larga scala.	Poca flessibilità, mancanza di competitività, rischio di "pensiero unico".	Cina, Russia, Iran
OPEN DOOR	Risposta agile a bisogni specifici, riduzione della burocrazia, sfruttamento del *crowd sourcing*.	Poca flessibilità, mancanza di competitività, rischio di "pensiero unico".	Ucraina
SILO	Maggiore sicurezza e compartimentazione, autonomia decisionale.	Nessuna sinergia con il settore civile, obsolescenza tecnologica, spreco di risorse.	Canada

AI and Defense: a Significant Step Forward, Now Decisively Towards the Future

Conclusion: A Step Forward That Demands Continuity

“AI and Defense” does not describe a distant future: it describes a present that demands choices. The significant step forward lies in the combination of **ambition and pragmatism**: close objectives, explicit enabling assets, clear governance, attention to ethics and IHL, and a strong push towards autonomy and technological sovereignty.

Now the decisive word is one: **continuity**. Because AI is not “introduced” once and for all: it is cultivated, governed, measured, and updated. If this path is followed with discipline, consistent investments, and the ability to attract talents, then yes: it will not just be a step forward. It will

be a trajectory, finally, decisively towards the future.

News link: https://www.difesa.it/assets/allegati/90197/ia_e_difesa_2026.pdf