



IA e Difesa: un bel Passo Avanti, adesso decisi verso il Futuro

Pubblicato il 28/02/2026

C'è un momento in cui una tecnologia smette di essere "promettente" e diventa inevitabile. Per la Difesa, quel momento è arrivato: l'Intelligenza Artificiale non è più una scelta opzionale o una sperimentazione di nicchia, ma una leva strategica che tocca operazioni, organizzazione, formazione e relazione con l'industria. È questo il messaggio centrale della **"IA e DIFESA - Strategia della Difesa in materia di Intelligenza Artificiale, Edizione 2026"**, che definisce un percorso concreto e ambizioso, impostato su tempi brevi e obiettivi misurabili a similitudine di quanto già fatto dalla Gran Bretagna nel 2022.



Una visione chiara: integrare rapidamente, ma con responsabilità

La strategia parte da una constatazione netta: la competizione contemporanea è accelerata, multi-dominio, iper-informata. In questo contesto l'IA diventa l'elemento che consente di **ridurre il divario tecnologico**, rafforzare la credibilità dell'Italia nelle alleanze (NATO e UE) e soprattutto aumentare l'efficacia operativa, senza perdere la bussola dei valori.

Il documento insiste su due "paletti" fondamentali:

- **approccio responsabile, etico e conforme al Diritto Internazionale Umanitario (DIU);**
- **controllo umano e responsabilità della linea di comando**, perché la tecnologia deve amplificare la decisione, non sostituirla.

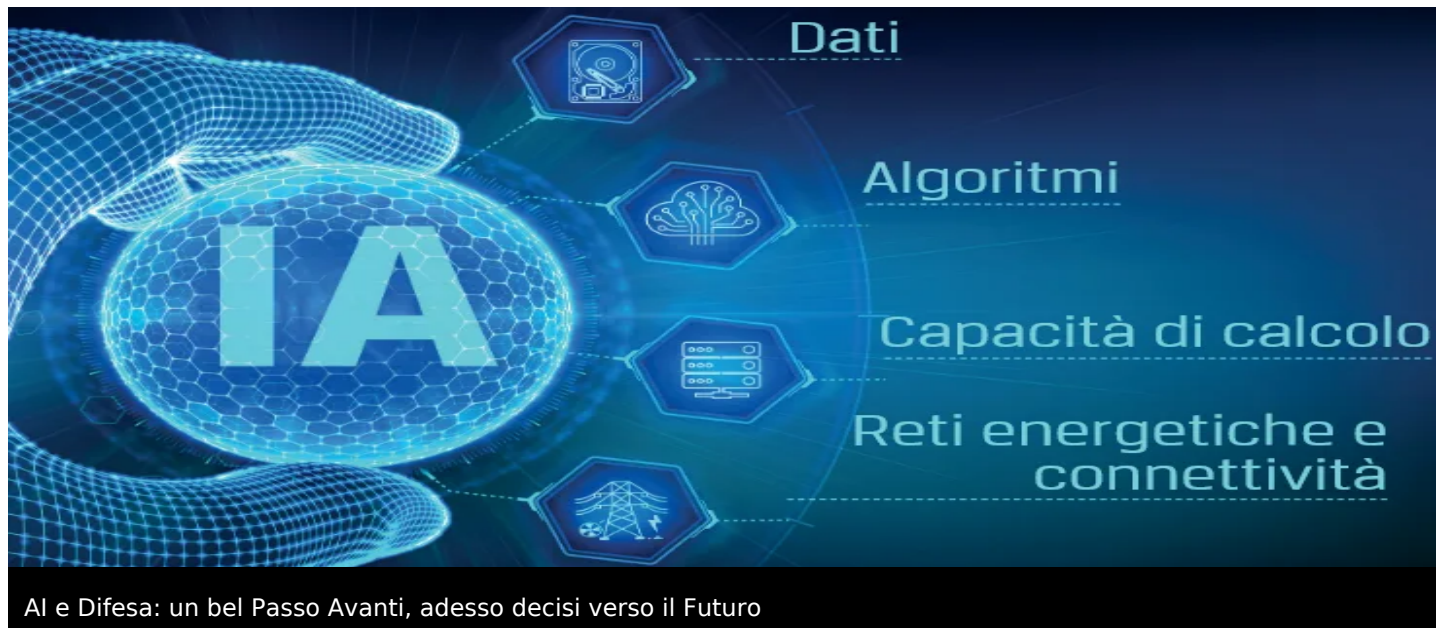
Questa cornice non è un dettaglio: è la condizione per far sì che l'innovazione sia sostenibile, interoperabile con i partner e difendibile anche sul piano politico e giuridico.

Autonomia strategica e sovranità tecnologica: la direzione è "in casa"

Il cuore del "passo avanti" sta nell'obiettivo dichiarato di **autonomia strategica** e **sovranità tecnologica**. Tradotto: non basta comprare soluzioni. La Difesa deve mantenere capacità interne critiche per:

- addestrare/aggiornare modelli anche con dati recenti e in contesti difficili;
- capire algoritmi, limiti, bias e rischi;
- garantire conformità a DIU, dottrina e valori;
- mantenere sistemi operativi anche senza supporto esterno.

Non è una presa di posizione “ideologica”, ma una risposta pratica a tre problemi reali: dipendenze da fornitori, vulnerabilità (anche intenzionali), e rischio di perdere libertà d’azione in crisi geopolitiche o in caso di fallimenti aziendali.



Gli asset abilitanti: talenti, dati, algoritmi, calcolo e reti sicure

Ogni strategia è credibile se nomina le condizioni materiali che la rendono possibile. Qui la Difesa lo fa, indicando chiaramente i pilastri:

- **risorse umane qualificate**, con attenzione ai “talenti” e alla loro attrazione/trattenimento;
- **dati** (integrità, qualità, assenza di bias, superamento dei “silos” e governance);
- **algoritmi** (sviluppo, validazione, manutenzione e certificazione);
- **capacità di calcolo proprietaria**, con requisiti elevati (anche in prospettiva HPC e ibrido HPC-quantum);
- **reti e connettività sicure**, con resilienza e continuità come criteri non negoziabili.

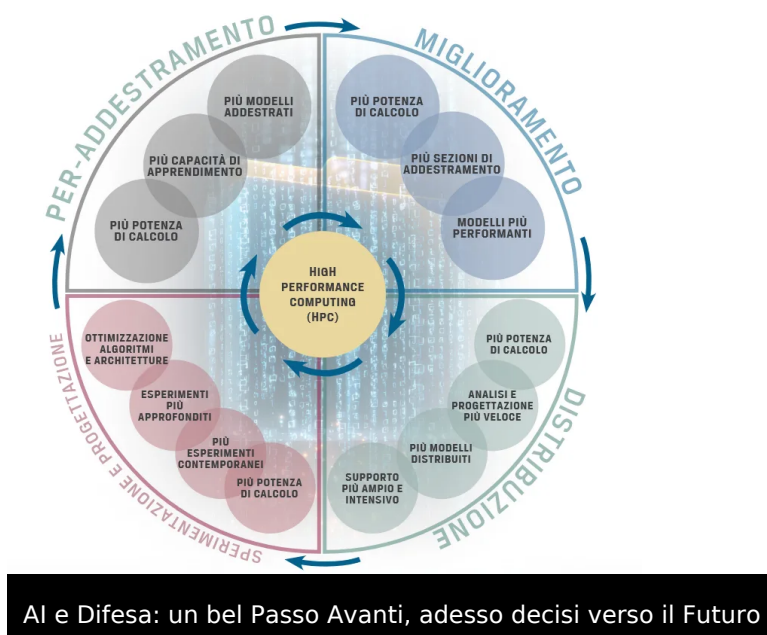
Colpisce il taglio molto operativo: il calcolo non è un “lusso IT”, ma il fattore che alimenta un ciclo virtuoso (più calcolo → più esperimenti → modelli migliori → più capacità) che determina il ritmo del vantaggio.

Un percorso “modulare” e veloce: 1 anno, 2 anni, 3 anni

La strategia sceglie una timeline aggressiva, proprio perché l’IA corre. Il percorso è diviso in tre orizzonti:

- **breve termine (entro 1 anno):** consolidare condizioni abilitanti (governance, infrastrutture, competenze, processi, rimozione ostacoli);
- **medio termine (entro 2 anni):** realizzare progetti operativi prioritari;
- **lungo termine (entro 3 anni):** integrazione diffusa, sicura e sostenibile in tutti gli ambiti della Difesa.

Questo è un punto chiave del “decisi verso il futuro”: non un elenco di desideri, ma una scaletta che rende l’ambizione controllabile e verificabile.



Quattro aree di intervento: dove l’IA cambia davvero il gioco

La strategia identifica quattro aree principali che coprono l’intera macchina Difesa.

1) Operazioni: superiorità decisionale, velocità d'ingaggio, protezione multi-dominio

Nel battlespace moderno, la massa di dati e la trasparenza del campo di battaglia rendono insufficiente la sola capacità umana di analisi. L'IA viene descritta come strumento per **decision augmentation**, wargaming “adattivo”, analisi predittiva, intelligence multi-fonte e protezione contro minacce cyber/elettromagnetiche e contro droni/sciami.

Il documento affronta anche le implicazioni più sensibili (come i sistemi d'arma autonomi) sottolineando la rilevanza dei profili etici e della governance.

2) Contesti organizzativi: produttività, servizi, processi

Qui c'è una promessa concreta: ottenere benefici rapidi. Si parla esplicitamente di strumenti per la produttività individuale e di un possibile [Large Language Model](#) “**della Difesa**” addestrato su documentazione interna, come prerequisito per gestione della conoscenza, bozze, sintesi, estrazione informazioni e coerenza terminologica.

Accanto a questo: assistenza all'utenza con linguaggio naturale, integrazione con automazioni (RPA) e, in prospettiva, agenti IA per problemi non strutturati — sempre con la regola: il giudizio umano non deve essere eclissato.

3) Formazione, addestramento e ricerca: cultura IA e mindset digitale

L'idea è chiara: senza formazione diffusa, l'adozione è fragile. Si parla di **alfabetizzazione IA** strutturata (dimensione cognitiva, operativa, critica ed etico-normativa) e di reskilling/upskilling per colmare gap generazionali e costruire una forza lavoro mista uomo-macchina.

4) Industria: ecosistema nazionale, open innovation, procurement più agile

Il documento valorizza l'ecosistema industriale nazionale (grandi player, ma anche startup e PMI), con un cambio di passo verso partnership, scouting tecnologico e meccanismi più agili per progetti pilota. L'obiettivo è duplice: accelerare l'innovazione e ridurre dipendenze, rafforzando una base “Defense Tech” competitiva.

Governance e attuazione: UIA e LIAD come motore centrale

Per evitare frammentazione, la strategia prevede una governance multilivello con due perni:

- **Ufficio per l'IA (UIA)**: indirizzo, supervisione, coerenza strategica, relazioni e presidio etico-legale;
- **Laboratorio di IA per la Difesa (LIAD)**: polo di eccellenza e **AI Delivery Center**, orientato a prototipare, sperimentare e rendere operative soluzioni in sinergia con gli utilizzatori finali.

Elemento decisivo: entro 3 mesi dall'approvazione è previsto un **Piano attuativo** con azioni, responsabilità e **KPI** di monitoraggio. È qui che la strategia smette di essere "dichiarazione" e diventa gestione.

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 <i>crowd sourcing</i> .	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 e Difesa: un bel Passo Avanti, adesso decisi verso il Futuro

Conclusione: un passo avanti che chiede continuità

"AI e Difesa" non racconta un futuro lontano: descrive un presente che impone scelte. Il bel passo avanti sta nella combinazione di **ambizione e pragmatismo**: obiettivi ravvicinati, asset abilitanti espliciti, governance chiara, attenzione a etica e DIU, e una spinta netta verso autonomia e sovranità tecnologica.

Ora la parola decisiva è una sola: **continuità**. Perché l'IA non si "introduce" una volta per tutte: si coltiva, si governa, si misura e si aggiorna. Se questo percorso verrà seguito con disciplina,

investimenti coerenti e capacità di attrarre talenti, allora sì: non sarà soltanto un passo avanti. Sarà una traiettoria, finalmente, decisa verso il futuro.

Link notizia: https://www.difesa.it/assets/allegati/90197/ia_e_difesa_2026.pdf