



MINISTERO DELLA DIFESA



# IA E DIFESA

## Strategia della Difesa in materia di Intelligenza Artificiale

Edizione 2026



**PAGINA NON SCRITTA**





MINISTERO DELLA DIFESA



# IA E DIFESA

## Strategia della Difesa in materia di Intelligenza Artificiale

Edizione 2026





**PAGINA NON SCRITTA**





Ministro della Difesa  
**On. Guido Crosetto**

"Quando si parla di IA e Difesa, i giovani sono il volto più innovativo dell'Italia.

... Sostenere questi giovani, sostenere la ricerca, sostenere le università, significa investire nel futuro dell'Italia. È da qui che nasce la crescita: dal talento, dall'impegno e dalla capacità di innovare delle nuove generazioni...

... Nell'innovazione, l'Intelligenza Artificiale è la nuova frontiera della difesa e dello sviluppo."

23 ottobre 2025  
Inaugurazione dell'Anno Accademico e Scolastico  
degli Istituti di Formazione dell'Esercito  
alla Scuola di Applicazione dell'Esercito di Torino

**PAGINA NON SCRITTA**



# MINISTERO DELLA DIFESA



## ATTO DI APPROVAZIONE

Approvo la presente "IA E DIFESA - Strategia della Difesa in materia di Intelligenza Artificiale" – Edizione 2026.

Roma, lì 16 gennaio 2026

**IL MINISTRO DELLA DIFESA**

On. Guido Crosetto





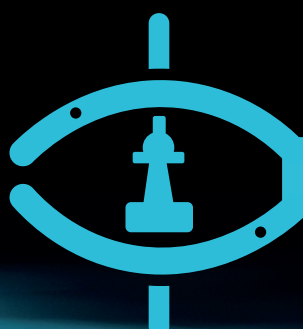
# INDICE

|                                                       |           |
|-------------------------------------------------------|-----------|
| <b>LA STRATEGIA IN SINTESI</b>                        | <b>4</b>  |
| <b>1 VISIONE E ASSET ABILITANTI</b>                   | <b>11</b> |
| 1.1 VISIONE                                           | 11        |
| 1.2 CONSIDERAZIONI STRATEGICHE                        | 12        |
| 1.2.1 AUTONOMIA STRATEGICA E CAPACITÀ INTERNE         | 12        |
| 1.2.2 SOVRANITÀ TECNOLOGICA                           | 13        |
| 1.2.3 RIDUZIONE DEL CARICO COGNITIVO PER L'OPERATORE  | 14        |
| 1.2.4 ETICA E LAWFARE                                 | 14        |
| 1.3 ASSET STRATEGICI ABILITANTI                       | 14        |
| 1.3.1 RISORSE UMANE                                   | 16        |
| 1.3.2 COMPONENTI TECNOLOGICHE FONDAMENTALI            | 16        |
| <b>2 IL CONTESTO NAZIONALE E INTERNAZIONALE</b>       | <b>21</b> |
| 2.1 INIZIATIVE ITALIANE SULL'IA                       | 21        |
| 2.2 LO SCENARIO INTERNAZIONALE                        | 22        |
| 2.2.1 NATO                                            | 22        |
| 2.2.2 UNIONE EUROPEA                                  | 23        |
| 2.2.3 ORGANIZZAZIONE DELLE NAZIONI UNITE (ONU)        | 23        |
| 2.3 INIZIATIVE NAZIONALI ESTERE                       | 25        |
| 2.3.1 STRATEGIE E GOVERNANCE                          | 25        |
| 2.3.2 SVILUPPO DI ALGORITMI E TECNOLOGIE PROPRIETARIE | 26        |
| 2.3.3 INFRASTRUTTURE E POTENZA DI CALCOLO             | 26        |
| 2.3.4 GESTIONE DEI TALENTI                            | 27        |
| 2.3.5 FOCUS SULLA FORMAZIONE E LA RICERCA             | 27        |
| 2.3.6 CENTRALIZZAZIONE DI COMPETENZE E RESPONSABILITÀ | 27        |
| 2.3.7 PARTNERSHIP CIVILE-MILITARE                     | 27        |
| 2.3.8 TEMI ETICI E USO RESPONSABILE DELL'IA           | 27        |
| 2.3.9 CONSIDERAZIONI FINALI                           | 28        |

|          |                                                                                                   |           |
|----------|---------------------------------------------------------------------------------------------------|-----------|
| <b>3</b> | <b>L'IA PER LA DIFESA: CONTESTI DI INTERESSI</b>                                                  | <b>31</b> |
| 3.1      | L'IA NEI CONTESTI OPERATIVI                                                                       | 32        |
| 3.1.1    | LE OPZIONI DI IMPIEGO DELL'IA NELLA PIANIFICAZIONE E NELLA VALUTAZIONE DEGLI EFFETTI NON CINETICI | 33        |
| 3.1.2    | LE PROSPETTIVE DI IMPIEGO FUTURO DELL'IA NELLA CONDOTTA DELLE OPERAZIONI                          | 34        |
| 3.2      | L'IA NEI CONTESTI ORGANIZZATIVI                                                                   | 37        |
| 3.2.1    | L'IA A SUPPORTO DELLA PRODUTTIVITÀ INDIVIDUALE                                                    | 37        |
| 3.2.2    | L'IA A SUPPORTO DELL'UTENZA                                                                       | 38        |
| 3.2.3    | L'IA A SUPPORTO DEI PROCESSI STRUTTURATI                                                          | 39        |
| 3.3      | IA, FORMAZIONE, ADDESTRAMENTO E RICERCA                                                           | 41        |
| 3.3.1    | FORMAZIONE ALL'IA                                                                                 | 42        |
| 3.3.2    | FORMAZIONE CON L'IA                                                                               | 42        |
| 3.3.3    | IA E ADDESTRAMENTO                                                                                | 43        |
| 3.3.4    | IA E RICERCA                                                                                      | 44        |
| 3.4      | IA E INDUSTRIA                                                                                    | 45        |
| 3.4.1    | LO SCOUTING TECNOLOGICO QUALE LEVA STRATEGICA                                                     | 46        |
| 3.4.2    | L'INNOVAZIONE QUALE LEVA STRATEGICA PER AMPLIARE LA BASE INDUSTRIALE DI RIFERIMENTO               | 47        |
| 3.4.3    | POTENZIAMENTO DEL RUOLO ATTIVO DELLA DIFESA NELLE RELAZIONI CON L'INDUSTRIA                       | 49        |
| <b>4</b> | <b>FABBISOGNI E DIRETTRICI DI INTERVENTO</b>                                                      | <b>53</b> |
| 4.1      | REVISIONE ORGANICA E FUNZIONALE                                                                   | 53        |
| 4.1.1    | LIVELLO POLITICO-STRATEGICO                                                                       | 54        |
| 4.1.2    | LIVELLO STRATEGICO-MILITARE                                                                       | 56        |
| 4.1.3    | LIVELLO OPERATIVO E TATTICO INTERFORZE                                                            | 56        |
| 4.1.4    | AREA GIURIDICA                                                                                    | 56        |
| 4.2      | RISORSE                                                                                           | 57        |
| 4.3      | DIRETTRICI STRATEGICHE DI INTERVENTO                                                              | 58        |
| <b>5</b> | <b>CONCLUSIONI</b>                                                                                | <b>61</b> |



# LA STRATEGIA IN SINTESI



CONTESTO E VISIONE STRATEGICA



PRINCIPI GUIDA E AUTONOMIA

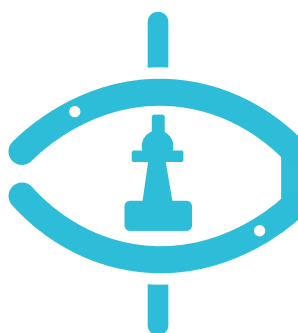


La presente Strategia si propone di **definire un quadro organico e coerente di interventi per l'adozione dell'IA in tutti gli ambiti della Difesa italiana**, valorizzando le potenzialità offerte da questa tecnologia con un approccio responsabile, etico e in linea con i principi del Diritto Internazionale Umanitario (DIU).

Sulla scorta delle lezioni apprese dalle recenti evoluzioni negli scenari geopolitici, questo documento si inserisce in un percorso già avviato a livello nazionale ed europeo, con l'**obiettivo di allineare le iniziative della Difesa con l'elevata accelerazione tecnologica e di impiego operativo della citata tecnologia**. Esso intende fornire indirizzi per promuovere lo sviluppo di capacità tecnologiche autonome, rafforzare il capitale umano, nonché innovare i processi organizzativi e le capacità operative.

La Strategia definisce, pertanto, un percorso articolato e modulare.





## CONTESTO E VISIONE STRATEGICA

L'IA emerge come un elemento strategico imprescindibile per il futuro della difesa nazionale, caratterizzato da una rapida evoluzione tecnologica e da crescenti sfide geopolitiche. **La Difesa italiana riconosce l'IA come una leva essenziale per il rafforzamento delle proprie capacità operative.**

L'obiettivo strategico primario è l'integrazione rapida, sistemica e sistematica dell'IA in tutti i principali ambiti: formativi, organizzativi e operativi. Questo permetterà di colmare i *gap* tecnologici accumulati e di posizionare l'Italia come *partner* credibile e proattivo all'interno delle alleanze multilaterali e delle organizzazioni internazionali, in particolare la NATO e l'Unione Europea.



## PRINCIPI GUIDA E AUTONOMIA

La Strategia si fonda su un approccio responsabile, etico e in linea con i principi del Diritto Internazionale Umanitario (DIU). **Un principio centrale è il mantenimento del controllo umano sulla tecnologia e la responsabilità della linea di comando.**

**Un elemento irrinunciabile della visione è il conseguimento dell'autonomia strategica e della sovranità tecnologica.** Questo richiede che la Difesa mantenga un *set* di capacità interne critiche, incluso il controllo profondo sui sistemi IA (addestrare i modelli, comprendere gli algoritmi e garantire la conformità al DIU).



La Strategia si inserisce in un percorso già avviato a livello nazionale ed europeo, fornendo indirizzi per promuovere lo sviluppo di capacità tecnologiche autonome, rafforzare il capitale umano e la valorizzazione dei dati, innovare i processi e, in particolare, fornire supporto ai decisori multilivello, coprendo **quattro principali aree di intervento**:

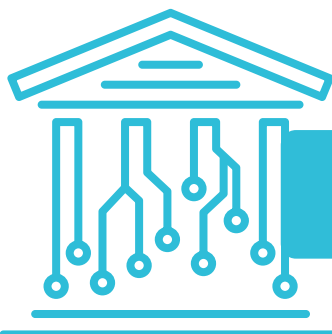
1. **OPERAZIONI**: sfruttare l'IA per il supporto alla pianificazione, la superiorità decisionale, la velocità di ingaggio e la protezione multi-dominio.
2. **CONTESTI ORGANIZZATIVI**: utilizzare l'IA a supporto dei processi decisionali, della produttività individuale, dell'utenza e dell'ottimizzazione dei processi strutturati.
3. **FORMAZIONE, ADDESTRAMENTO E RICERCA**: sviluppare una cultura dell'IA, formare il personale, e potenziare i sistemi addestrativi tramite simulazione e cooperazione uomo-macchina.
4. **INDUSTRIA**: valorizzare l'ecosistema industriale nazionale, inclusi start-up e PMI, promuovendo *partnership* sinergiche, *open innovation* e trasferimento tecnologico per garantire competitività e sovranità tecnologica.

Il percorso è articolato e modulare, con obiettivi definiti a breve, medio e lungo termine, allineati al rapido ritmo evolutivo della tecnologia:

- **Breve termine (entro 1 anno)**: consolidare le condizioni abilitanti fondamentali.
- **Medio termine (entro 2 anni)**: realizzare progetti operativi prioritari.
- **Lungo termine (entro 3 anni)**: integrare l'IA in modo diffuso, sicuro e sostenibile in tutti gli ambiti della Difesa.

**I termini temporali sopra esposti, diversi da una classica strategia, rappresentano un livello di ambizione che deve necessariamente allinearsi al ritmo evolutivo di questa tecnologia.**





## ASSET ABILITANTI E GOVERNANCE

Per implementare la strategia sono essenziali specifici **asset abilitanti**, tra cui:

- **risorse umane** qualificate (**talenti**);
- **dati**;
- **algoritmi**;
- **capacità di calcolo proprietaria** (*High Performance Computing – HPC e Quantum Computing*);
- **reti sicure**.

Sostenuta da questi pilastri, la visione strategica, invocando una revisione integrata della *governance* dell'IA, si dovrà realizzare prevedendo nuove articolazioni organizzative:



Un **Ufficio per l'IA (UIA)** preposto all'attuazione dell'indirizzo politico nonché alla supervisione e verifica di coerenza della sua implementazione. Tale Ufficio agirà in maniera sinergica con le analoghe strutture competenti per le tecnologie emergenti<sup>1</sup>.

<sup>1</sup> Innovazioni tecnologiche (tra cui l'IA) che portano a significativi cambiamenti in vari settori, trasformando prodotti, servizi e modelli di *business*.



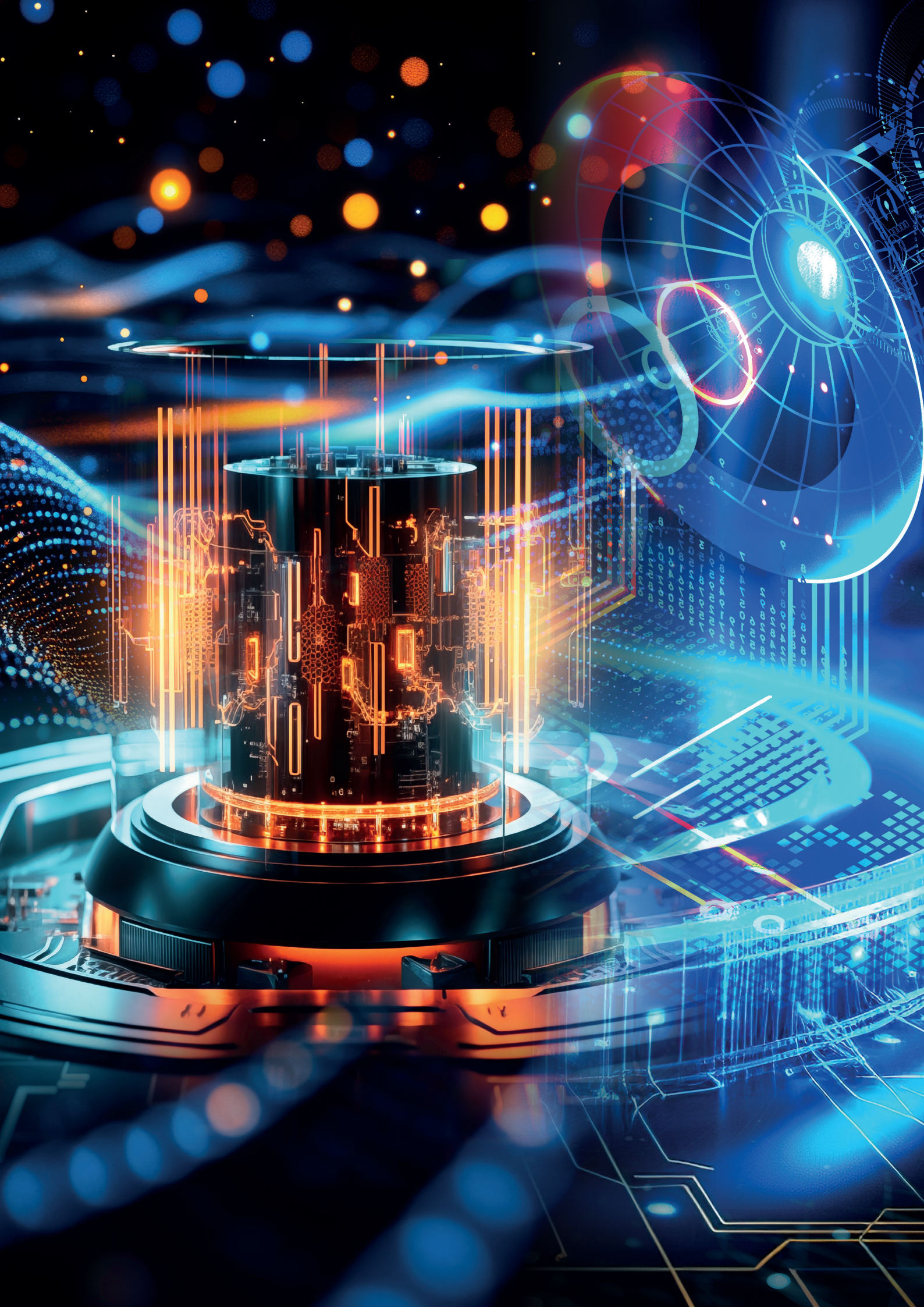
Il **Laboratorio di IA per la Difesa (LIAD)**, che fungerà da polo di eccellenza, aggregatore di idee e AI Delivery Center della Difesa, con il compito di sviluppare e sperimentare soluzioni in sinergia con gli utilizzatori finali.

L'intera strategia sarà guidata da **15 Diretrici Strategiche (DS)**, suddivise in sei gruppi (governance e risorse - fattori strategici abilitanti - l'IA nei contesti operativi - l'IA nei contesti organizzativi - IA, formazione, addestramento e ricerca - IA e industria), che ne definiscono l'attuazione.

**Entro 3 mesi dall'approvazione del documento, sarà diramato un Piano attuativo per definire le azioni chiave, le responsabilità e i Key Performance Indicator (KPI) per il monitoraggio.**

PAGINA NON SCRITTA







# 01

Una Difesa  
in possesso  
delle  
capacità  
critiche per  
garantire  
il controllo  
profondo  
dell'IA  
durante tutto  
il ciclo di vita

## VISIONE E ASSET ABILITANTI

### 1.1 VISIONE

La Difesa italiana riconosce l'IA come una **leva imprescindibile per il rafforzamento delle proprie capacità operative**, indispensabile per affrontare con efficacia le sfide complesse poste dall'attuale scenario geopolitico globale e per mantenere il proprio posizionamento di rilievo in ambito europeo e internazionale.

Essa si pone come obiettivo strategico primario **l'integrazione rapida e sistematica dell'IA** in tutti i principali ambiti formativi, organizzativi e operativi, in linea con le iniziative in essere dei principali Paesi di riferimento. Questo permetterà di colmare i *gap* tecnologici accumulati e qualificarsi come *partner* credibile, affidabile e proattivo all'interno delle alleanze multilaterali e delle organizzazioni internazionali a cui l'Italia aderisce, in particolare la NATO e l'Unione Europea.

La presente strategia, coerentemente con le migliori prassi internazionali, ha **un approccio sinergico con le altre iniziative** in corso di implementazione in ambito Nazionale e con gli altri documenti in fase di redazione, in particolare con la "Strategia per la Digitalizzazione" della Difesa e con il documento "Il contrasto alla guerra ibrida: una strategia attiva per la Difesa". Essa definisce un percorso articolato che copre l'intero arco temporale necessario alla maturazione e consolidamento di capacità IA robuste e sostenibili.

L'approccio adottato, focalizzato su **quattro principali aree di intervento** (operazioni, contesti organizzativi, formazione e industria), disegna, attraverso **15 Diretrici Strategiche (DS)**, un percorso di crescita progressiva e sostenibile che dal breve periodo, volto a consolidare le condizioni abilitanti fondamentali, intravede, nel medio e lungo periodo, una piena e totale integrazione dell'IA in ogni processo della Difesa. All'interno di questo percorso il **fattore umano, così come l'uso etico, trasparente, responsabile e conforme al DIU di questa tecnologia, resta centrale per il Dicastero**, al pari della piena autonomia gestionale dei modelli IA nel loro ciclo di vita e della responsabilità umana sulle tecnologie impiegate.



Un elemento distintivo della visione della Difesa italiana riguarda il **ruolo centrale assegnato all'ecosistema industriale nazionale**, patrimonio strategico da sostenere e valorizzare che vede al fianco delle grandi realtà di eccellenza un vivace e innovativo ecosistema di piccole e medie imprese (PMI), *startup* e *spin-off* altamente tecnologici. La strategia intende promuovere un cambio di passo nelle relazioni con questo ecosistema, favorendone l'espansione e incrementando collaborazioni sinergiche, programmi di *open innovation* e processi di trasferimento tecnologico, con l'obiettivo di intercettare soluzioni all'avanguardia e garantire competitività e sovranità tecnologica nel settore IA. La realizzazione della visione strategica presentata postula una revisione articolata e integrata della *governance* dell'IA nell'ambito della Difesa al fine di assicurare un'azione di indirizzo e monitoraggio centralizzata e garantire la coerenza delle iniziative e la tempestività nelle decisioni.

In tale ambito, è altresì prevista la costituzione:



dell'**Ufficio per l'IA (UIA)**, quale regista strategico in grado di dirigere e monitorare, sulla base dell'indirizzo politico, le attività inerenti a tale tecnologia, dando unicità di visione, creando sinergia, facendo economia di scala ed evitando ridondanza e sprechi;



del **Laboratorio di IA per la Difesa (LIAD)**, dotato di infrastrutture di eccellenza per creare un polo di attrazione ove creare collaborazioni, co-sviluppare soluzioni e coltivare talenti, fungendo da vero e proprio "**AI Delivery Center**" della Difesa.

A corollario, si prevede l'avvio di investimenti pluriennali mirati e orientati alla crescita coerente e sostenuta delle capacità IA nazionali, ad appannaggio dell'intero Sistema Paese.

La visione della Difesa per l'implementazione dell'IA è quindi quella di un percorso strategico, ambizioso e inclusivo, capace di modulare e adattare l'evoluzione tecnologica alle specificità e ai valori del nostro Paese, ponendo al centro l'equilibrio essenziale tra innovazione, responsabilità etica e sovranità tecnologica. **L'obiettivo finale è dotare le FF.AA. di sistemi basati su IA all'avanguardia, sicuri, resilienti e nativamente interoperabili, che mettano l'uomo al centro ed esaltino l'efficacia operativa.** Questo consoliderà la posizione del Dicastero quale *partner* affidabile e credibile, in grado di contribuire in modo determinante alla difesa e sicurezza militare nazionale, degli spazi atlantici ed euro-mediterranei e alla stabilità internazionale in un contesto caratterizzato da rapidi mutamenti e crescenti minacce.

## 1.2 CONSIDERAZIONI STRATEGICHE

L'implementazione dell'IA richiede un'attenta riflessione strategica, che esplori tutti gli aspetti che questa tecnologia trasversale e dirompente comporta. Di seguito sono riportati i principali temi di imperativo interesse.

### 1.2.1 AUTONOMIA STRATEGICA E CAPACITÀ INTERNE

L'adozione dell'IA, soprattutto in ambito operativo, comporta la chiara consapevolezza che non tutto può essere interamente demandato o condiviso con l'industria, finanche quella nazionale. Ciò deriva dalla non

**È IMPERATIVO CHE LA DIFESA MANTENGA UN SET DI CAPACITÀ INTERNE CHE GARANTISCANO L'AUTONOMIA STRATEGICA, PREVENGANO DIPENDENZE CRITICHE E PERMETTANO DI ESSERE RESILIENTI E ADERENTI ALLE SFIDE EMERGENTI**

condivisibilità di determinati dati, o dalla necessità di aderenza alle operazioni in contesti ad alto rischio – quali i più recenti scenari di crisi – in cui non è possibile prevedere l'intervento dell'industria. Per tale ragione, è imperativo che la Difesa mantenga un set di capacità interne che garantiscano l'autonomia strategica, prevenendo dipendenze critiche e permettano di essere resilienti e aderenti alle sfide emergenti.

Al riguardo, è necessario disporre di una adeguata infrastruttura di calcolo e dei dati necessari, così come possedere il controllo profondo dei sistemi IA. Con ciò si intendono le capacità critiche di:

- addestrare<sup>2</sup> i modelli di IA con i dati più recenti, anche sul campo di battaglia;
- comprendere il funzionamento degli algoritmi, di valutarne limiti, *bias* e rischi, e di intervenire per modificarli o migliorarli;
- garantire che i sistemi IA operino sempre in conformità con il DIU, la dottrina e i valori nazionali;
- poter mantenere operativi i propri sistemi di IA, anche in assenza di supporto esterno in contesti ad alto rischio, per manutenzione, risoluzione di problemi e questioni di sicurezza.

### 1.2.2 SOVRANITÀ TECNOLOGICA

La sovranità tecnologica nell'ambito dell'IA per la Difesa è la capacità del Paese (o dell'Europa) di poter progettare, sviluppare, produrre, controllare e proteggere le proprie infrastrutture digitali e i sistemi di IA critici, riducendo la dipendenza da fornitori esterni. Si tratta, in definitiva, di avere un controllo sufficiente sulle tecnologie abilitanti per:

- garantire autonomia strategica, sicurezza e resilienza;
- abbattere rischi quali vulnerabilità intenzionali (*backdoor*) o non intenzionali;
- evitare dipendenza tecnologica e limitazione della libertà d'azione<sup>3</sup>, ridotto controllo sui dati ovvero inclusione di *bias* e, in ultimo, impoverimento dell'**ecosistema nazionale "Defense Tech"** per numeri e capacità.

Al riguardo, **è necessario garantire il pieno controllo sul ciclo di vita dei sistemi IA, dalla progettazione all'implementazione e mantenimento, assicurando la protezione dei dati sensibili e l'allineamento delle soluzioni agli interessi di sicurezza, affidabilità e conformità etica nazionali e dell'Alleanza.**

**UNA DIFESA CHE PERSEGUE LA SOVRANITÀ TECNOLOGICA NELL'IA PER PREVENIRE DIPENDENZE E GARANTIRE SICUREZZA, AFFIDABILITÀ E RISPETTO DEI VALORI NAZIONALI**

<sup>2</sup> In particolare provvedendo al *fine tuning* e il *re-training* dei modelli.

<sup>3</sup> Soprattutto in caso di tensioni geopolitiche, sanzioni o fallimenti aziendali.





### 1.2.3 RIDUZIONE DEL CARICO COGNITIVO PER L'OPERATORE

L'elevata densità di dati e informazioni può facilmente portare al sovraccarico cognitivo dell'operatore. Per tale ragione, l'IA deve essere concepita primariamente come uno strumento per la riduzione, e non per l'incremento, di tale complessità, divenendo abilitante strategico per renderla compatibile con le capacità umane e amplificarle, permettendo così al personale, sempre al centro, di concentrarsi sulla decisione e sull'azione strategica.

### 1.2.4 ETICA E LAWFARE

L'impiego dell'IA solleva complesse questioni etiche e legali, introducendo la delicata e complessa sfida del *lawfare*<sup>4</sup>. La potenziale eterogeneità degli approcci etici e legali all'IA tra le nazioni può comportare, infatti, un netto svantaggio operativo per chi aderisce a principi più restrittivi, avendo il potenziale di generare asimmetria operativa, esposizione a campagne di disinformazione e dilemmi etici.

Pur non ponendo vincoli allo sviluppo tecnologico<sup>5</sup>, risulta imprescindibile che l'utilizzo dell'IA sia sempre orientato alla tutela, difesa e sicurezza nazionale, nel pieno rispetto dei valori costituzionali, dei principi etici e delle norme internazionali relative a un uso responsabile delle tecnologie emergenti, assicurando la piena conformità ai seguenti criteri fondamentali:

- mantenimento del controllo umano sulla tecnologia;
- responsabilità permanente della linea di comando;
- rispetto del DIU, orientando ogni sforzo alla salvaguardia della vita umana e ai diritti essenziali dell'uomo;
- mantenimento di ragionevoli criteri di spiegabilità dei modelli.

## 1.3 ASSET STRATEGICI ABILITANTI

Il successo dell'integrazione dell'IA nel settore della Difesa dipende anche e soprattutto dall'efficacia dello sviluppo, armonizzazione e gestione dei suoi **asset abilitanti**. Questi ultimi, infatti, sono i pilastri su cui poggia l'intera strategia, garantendo che le capacità tecnologiche possano effettivamente tradursi in maggiore efficacia, efficienza e, in ultima analisi, in un reale vantaggio operativo.

Il presente paragrafo esaminerà in dettaglio i citati *asset*, focalizzando l'attenzione sulle componenti infrastrutturali fondamentali e sul capitale umano, al fine di tracciare una linea di sviluppo sinergico della cornice in cui le altre azioni strategiche potranno trovare compimento. Al riguardo, così come per tutte le Diretrici Strategiche descritte nel presente documento, sarà necessario implementare, attraverso uno specifico Piano Attuativo, una serie di azioni incisive per rinforzare e presidiare i fattori abilitanti di seguito esposti.

.....  
4 Questo termine si riferisce all'uso della legge come arma di guerra, sfruttando le differenze negli ordinamenti legislativi e nelle interpretazioni del DIU per ottenere un vantaggio strategico o per delegittimare le operazioni avversarie.

5 Che deve sempre permettere sufficiente flessibilità in base all'evoluzione del quadro di riferimento.

## UNA DIFESA CON PROFESSIONALITÀ DI ALTO PROFILO, PERCEPITA COME OPPORTUNITÀ DI CRESCITA UNICA NEL PANORAMA NAZIONALE

### 1.3.1 RISORSE UMANE

Come in ogni altro settore, lo sviluppo e l'integrazione delle soluzioni basate su IA nell'ambito della Difesa non può prescindere dalla disponibilità di professionalità in grado di guidare, supportare e gestire il processo in modo efficace. Tra queste<sup>6</sup>, si possono distinguere profili:

- **essenziali**: costantemente necessari poiché costituiscono il nucleo di competenze interne irrinunciabili per l' "autonomia strategica";
- **necessari a richiesta**: per periodi più o meno prolungati che, tuttavia, non giustificano un rapporto lavorativo permanente;
- **utili occasionalmente**: per progettualità specifiche, audit o consulenze, che richiedono un distinto approccio di accesso<sup>7</sup> da parte del comparto Difesa.

Si aggiungono, inoltre, i ricercatori, la cui missione è accrescere la conoscenza e perseguire la superiorità tecnologica, critica per la competitività del Paese.

Se per la maggioranza dei ruoli, soprattutto operativi e gestionali, un approccio pragmatico tendente al "*good enough*" risulta più efficace per garantire la costante disponibilità delle competenze, la vera differenza è determinata dai c.d. "**talenti**": profili con competenze di alto livello con disponibilità limitata e contesa sul mercato del lavoro che occorre attrarre, costruire e trattenere.

In tale ambito, la direttrice strategica è rivolta a incrementare l'**attrattività**:

- del **percorso formativo**, offrendo corsi specialistici di alto livello e prestigio prevedendo proporzionali estensioni del rapporto lavorativo con la Difesa;
- dell'**ambiente lavorativo**, favorendo modalità più agili<sup>8</sup> e consentendo l'accesso a Laboratori di IA pubblici o privati di eccellenza, dati pregiati ed esclusivi, e infrastrutture di calcolo all'avanguardia;
- della **carriera**, tracciando percorsi di sviluppo professionale che esaltino le competenze, consentano l'accesso a ruoli di leadership e responsabilità e prevedano misure e deroghe<sup>9</sup> atte a mitigare i vincoli percepiti penalizzanti;

6 Una tassonomia di riferimento sarà fornita all'interno del discendente Piano Attuativo della Strategia (rife. capitolo 4. paragrafo 3).

7 Approccio basato sul fattore "*build*", agendo sulla formazione, ovvero "*buy*", ricercandole all'esterno e stabilendo relazioni nell'ambito della c.d. Riserva Selezionata, contrattuali o di collaborazione strategica con industria, accademia e ricerca.

8 Il c.d. *smart working* è una modalità piuttosto nota e consolidata in ambito digitale, ma vi sono altre soluzioni esplorabili per garantire il risultato.

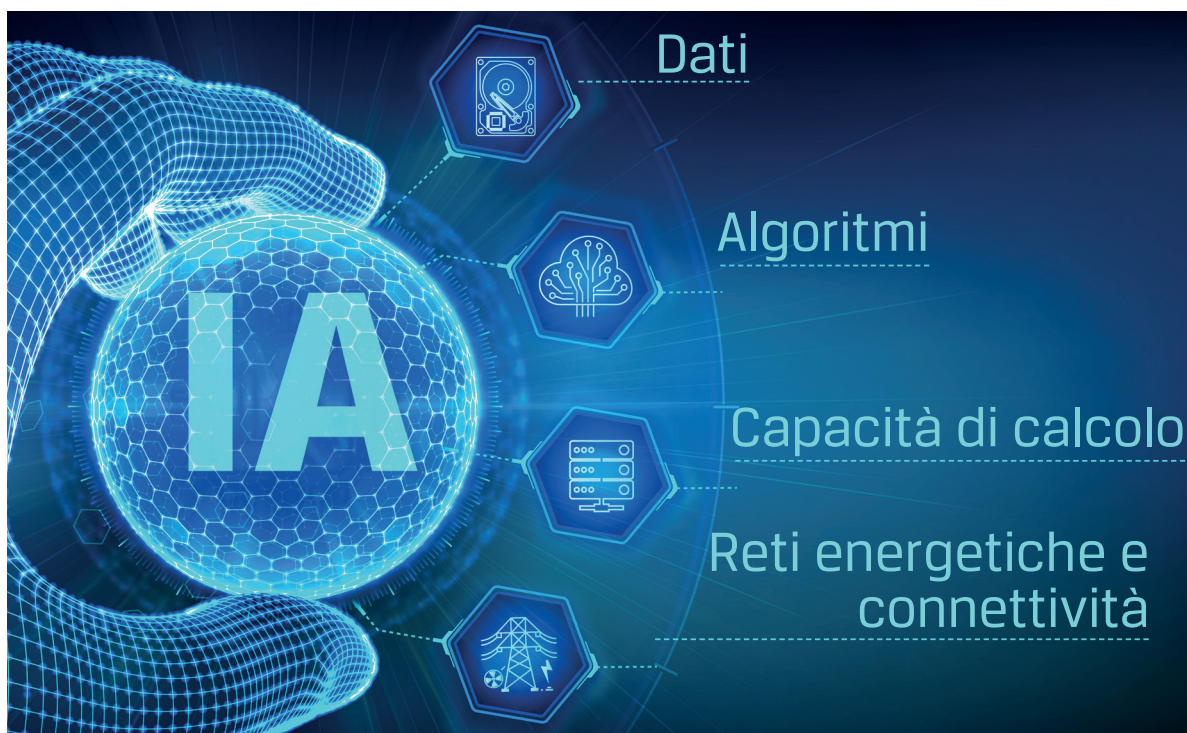
9 Un chiaro esempio, in tal senso, è la deroga all'art. 894 del Decreto Legislativo 15 marzo 2010, n. 66 (Codice dell'Ordinamento Militare), già prevista per il personale Medico Militare (ex art. 210 del COM), riferita all'attività libero professionale.

- dell'**ecosistema tecnologico**, incrementando le collaborazioni col mondo esterno per favorire una costante osmosi tra le diverse realtà in ottica di *open innovation*, soprattutto presso aree fertili ove sviluppare cooperazioni strategiche e attività e cercare di circoscrivere le eventuali fuoriuscite;
- delle **prospettive future**, evidenziando come un percorso di crescita nell'ambito della Difesa rappresenti un'opportunità unica per sviluppare competenze immediatamente spendibili all'esterno: un cambio di paradigma che possa anche valorizzare la "fuoriuscita" verso il settore privato come opportunità in più per attrarre e giovare dei talenti in una determinata fase della carriera per poi continuare a fruirne con altre tipologie di rapporto<sup>10</sup>.

### UNA DIFESA CHE DISPONE DI INFRASTRUTTURE E CAPACITÀ DI CALCOLO ALL'AVANGUARDIA, PER TRAINARE IL PROGRESSO TECNOLOGICO DEL SISTEMA-PAESE

#### 1.3.2 COMPONENTI TECNOLOGICHE FONDAMENTALI

Per operare efficacemente nell'ambito IA, oltre al capitale umano, è indiscutibilmente necessaria la disponibilità di un intero ecosistema tecnologico che, nel suo complesso, costituisca le fondamenta portanti e il presupposto fondamentale dell'efficacia della strategia.

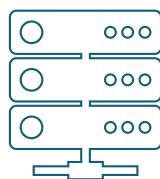
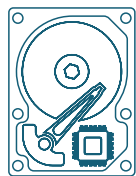


**Figura 1** – Quattro componenti tecnologiche fondamentali dell'IA

<sup>10</sup> Nell'ambito della c.d. Riserva Selezionata – eventualmente da prevedere quale vincolo a valle della cessazione del rapporto lavorativo con la Difesa – ovvero mediante contratti per specifiche progettualità.



Questo necessita di quattro componenti fondamentali (figura 1).



1. Il **dato**, asset strategico fondamentale che, oltre a essere disponibile, integro e sicuro, deve possedere intrinseche caratteristiche di pertinenza, accuratezza, consistenza e assenza di *bias*. Per tale ragione è necessario che la Difesa<sup>11</sup> rimuova gli ostacoli alla condivisione dei dati, superando, laddove ancora esista, la segmentazione "in silos"<sup>12</sup> e favorendo l'integrazione tra tutte le articolazioni a prescindere dalla *ownership*<sup>13</sup>. Ciò postula, altresì, un complessivo incremento della capacità di *storage*, un *repository* unico<sup>14</sup> e un approccio "cloud" nella duplice configurazione *class* e *unclass*<sup>15</sup>. È imperativo, infine, adottare una *policy* di *data management* e robusti processi di *data governance* per ottimizzare la gestione del patrimonio informativo con elevati standard nell'intero ciclo di vita del dato<sup>16</sup>.
2. L'**algoritmo**, in particolare lo sviluppo, la validazione e la manutenzione dei modelli. Con riferimento allo sviluppo, potrà avvenire "in house", ovvero intessendo relazioni con la base industriale di riferimento per realizzare soluzioni robuste, sicure e resilienti, in grado di operare con continuità, che garantiscano trasparenza e spiegabilità dei modelli, aggiornamento continuo, supervisione umana, interoperabilità e standardizzazione. La validazione e la certificazione, infine, sono fondamentali per fornire garanzie su efficacia, affidabilità, sicurezza e conformità del modello al DIU e ai valori etici. La disponibilità di nuovi algoritmi e modelli dovrà essere costantemente monitorata e andare ad appannaggio dell'intero Comparto Difesa.
3. La **capacità di calcolo**, quale requisito imprescindibile per l'autonomia strategica della Difesa. La disponibilità di capacità computazionale, infatti, è alla base dell'addestramento, del perfezionamento, dello sviluppo e della sperimentazione dei modelli di intelligenza artificiale; pertanto maggiore sarà tale capacità e maggiore sarà il progresso dell'intelligenza artificiale, innescando un ciclo che si autoalimenta (figura 2). Al riguardo, va evidenziato che tale capacità dovrà risiedere presso una infrastruttura di computazione proprietaria con i seguenti aspetti indispensabili:
  - ridondanza e resilienza;
  - modularità e isolamento degli ambienti di addestramento, test, rilascio e produzione;
  - flessibilità e scalabilità per far fronte alle evoluzioni del settore e alla possibilità di integrare gli HPC già disponibili, possibilmente anche in maniera federata;
  - rispetto dei più elevati requisiti di sicurezza, sia a livello fisico sia cibernetico<sup>17</sup>, tali da soddisfare anche esigenze *classificate*;
  - adeguate caratteristiche prestazionali, possibilmente dell'ordine dei *Petascale* o *Exascale*.

<sup>11</sup> Nell'ambito della redigenda Strategia per la digitalizzazione della Difesa.

<sup>12</sup> La mentalità "a silos" descrive una situazione in cui le attività all'interno di un'organizzazione vengono svolte ricorrendo ad una archiviazione e gestione separate di dati, rallentando i processi, aumentando i costi e ostacolando l'innovazione.

<sup>13</sup> Concetto non legato alla proprietà ma a quello di responsabilità di gestione del dato.

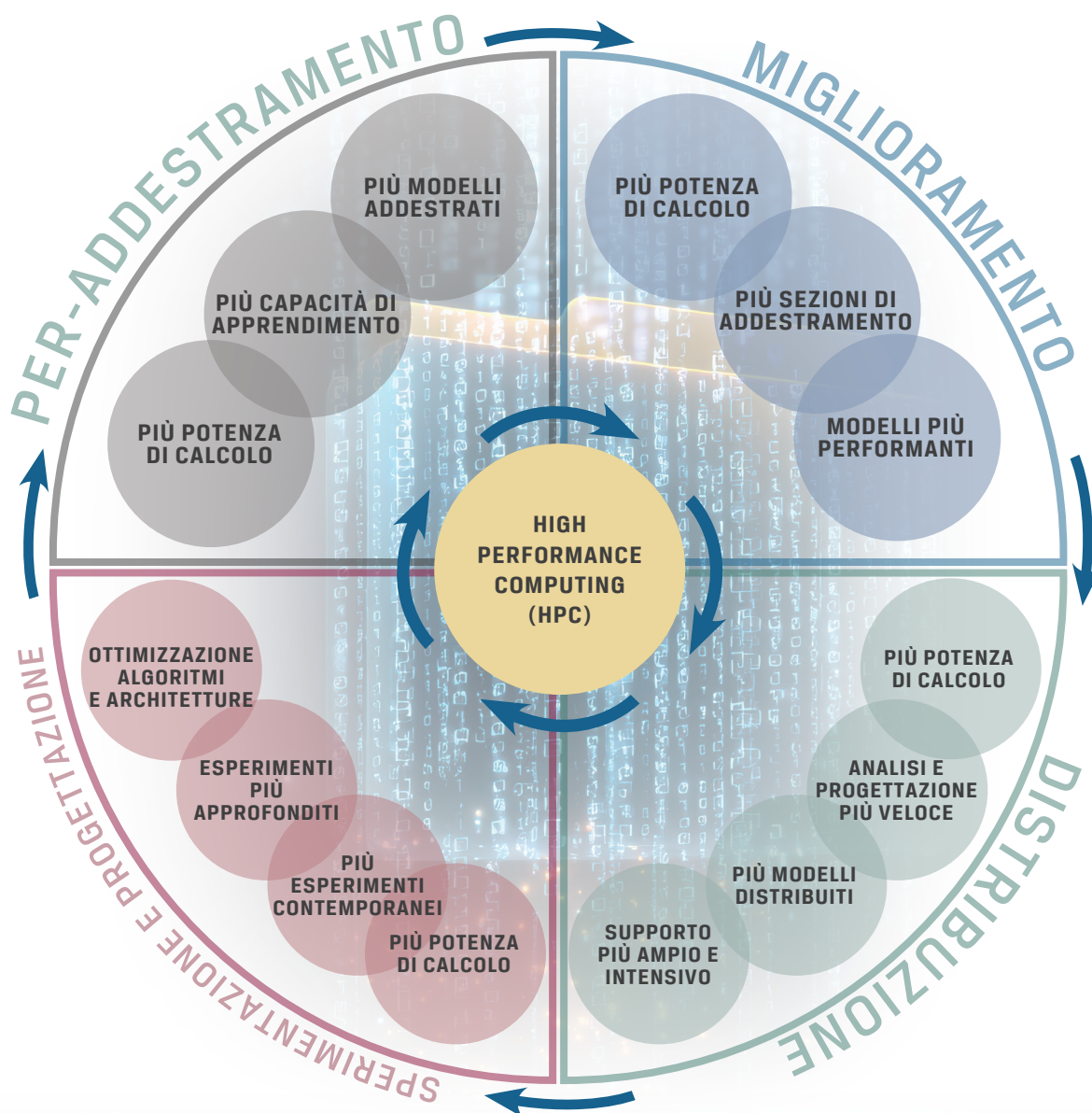
<sup>14</sup> Inteso come valenza logica. La stessa architettura *cloud* può prevedere la federazione di *cloud* distinti.

<sup>15</sup> In prospettiva, per massimizzare le potenzialità offerte dall'IA, occorrerà individuare soluzioni tecnologiche atte a interconnettere in maniera bidirezionale i due domini "classificato" e "non classificato" in modo sicuro.

<sup>16</sup> Dalla raccolta alla cancellazione sicura e negli stati, a "riposo", in transito, in uso. La *governance* dei dati garantisce qualità, sicurezza integrità, verifica della provenienza, tracciabilità e utilizzo responsabile dei dati.

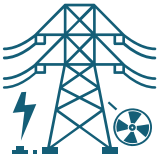
<sup>17</sup> Rispettando altresì anche i criteri "zero-trust architecture" e "quantum-safe".

Sarà inoltre fondamentale abilitare un ecosistema di computazione ibrida, in grado di adattarsi alle innovazioni del *quantum computing* e alle sfide del calcolo post-quantistico, per arrivare ad infrastrutture ibride HPC-*quantum* integrate e scalabili. Allo scopo, dovranno essere massimizzate le opportunità di finanziamento emergenti sia a livello nazionale sia europeo, centralizzando e armonizzando le iniziative per non disperdere risorse e capacità.



**Figura 2** – Ciclo di Progresso dell'IA sulla base delle capacità computazionali





4. Le **reti energetiche** in grado di alimentare l'infrastruttura e la **connettività** per supportare la trasmissione veloce di dati attraverso reti con garanzia di continuità, ridondanza e sicurezza. Tralasciando le valide soluzioni MANET<sup>18</sup>, emergono per importanza strategica la dorsale di connessione nazionale e le comunicazioni satellitari. Queste ultime, per superare i limiti attuali, richiedono soluzioni basate su orbita bassa. Per queste ultime è necessario perseguire l'acquisizione di ulteriori capacità rispetto quelle attuali<sup>19</sup>, espresse da sistemi caratterizzati da bassa latenza, elevata capacità di rete, copertura locale e flessibile, maggiore resilienza, scalabilità e ridondanza. In tal senso, tenendo conto delle tempistiche stimate per l'implementazione di costellazioni proprietarie *dual use* sia nazionali sia a livello UE<sup>20</sup> (non disponibili prima del prossimo decennio) si dovranno esplorare sia soluzioni per realizzare un eventuale sistema con un numero limitato di satelliti (tale da rispondere a specifiche e strategiche esigenze di scambio dati in scenari complessi), sia soluzioni *gap filler* di breve-medio periodo facendo ricorso ad operatori commerciali.



- 18 *Mobile Ad hoc NETWORK*, approccio – basato anche su soluzioni commerciali con cifratura "AES 256" – che si allontana dal concetto di architettura centralizzata e con un singolo punto di fallimento, per adottare reti formate da più sistemi di connettività/radio, permettendo a ogni nodo (soldato, piattaforma, sensore) di agire come un punto di trasmissione, reindirizzando automaticamente i dati in caso di guasti o interruzioni.
- 19 La Difesa può contare su piattaforme satellitari proprietarie geostazionarie, in particolare il SICRAL 1B e 2, (dal 2027 anche il 3) oltre all'italo-francese ATHENA FIDUS, che però garantiscono servizi sicuri con alta latenza.
- 20 Sistema *Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS<sup>2</sup>)* è un progetto dell'Unione Europea di una costellazione satellitare che, verosimilmente dal 2030, garantirà una connettività sovrana, sicura e resiliente, quale alternativa ad altre costellazioni satellitari, come le statunitensi *Starlink* e *Kuiper* (Amazon).







## 02

Una Difesa  
che punta  
ad avere una  
posizione di  
rilievo a livello  
nazionale e  
internazionale  
in materia di  
IA, in quanto  
settore  
critico per  
gli interessi  
nazionali

# IL CONTESTO NAZIONALE E INTERNAZIONALE

Al fine di contestualizzare in modo appropriato questa Strategia, è opportuno svolgere una ricognizione delle iniziative analoghe in campo nazionale, internazionale e multilaterale in materia di IA. Questo permetterà una valutazione del loro impatto, necessaria per ottimizzare l'efficacia delle iniziative della Difesa e la coerenza e sinergia delle stesse con la strategia nazionale, nonché con quelle delle organizzazioni multilaterali cui l'Italia partecipa.

## 2.1 VISIONE

Le prime indicazioni strategiche nazionali strutturate sul tema risalgono al "Programma Strategico Intelligenza Artificiale" del 2021, con la successiva redazione della "Strategia italiana per l'Intelligenza Artificiale 2024-2026"<sup>21</sup> del 2024. La suddetta strategia persegue obiettivi nei campi della **ricerca**<sup>22</sup>, della **pubblica amministrazione**<sup>23</sup>, delle **imprese**<sup>24</sup> e della **formazione**<sup>25</sup>.

<sup>21</sup> Al termine dell'orizzonte temporale per cui era stato previsto il "Programma Strategico Intelligenza Artificiale" (i.e. 2022-2024), il Governo ha emanato la "Strategia italiana per l'Intelligenza Artificiale 2024-2026" per contemplare le significative novità emerse dalla nascita dei sistemi generativi e inquadrare gli sforzi nazionali in un contesto europeo, promuovendo soluzioni antropocentriche, affidabili e sostenibili, senza che la Difesa sia stata chiamata a partecipare alla redazione del documento.

<sup>22</sup> Rafforzare gli investimenti sulla ricerca fondamentale e applicata nell'IA, promuovendo la creazione di competenze di ricerca e tecnologie specificamente calate nel contesto del nostro "Sistema Paese" e in linea con principi di affidabilità e responsabilità e antropocentrici, propri dei paradigmi Europei.

<sup>23</sup> Rendere più efficienti i propri processi amministrativi e migliorare la qualità dei servizi offerti ai cittadini attraverso l'impiego di tecnologie di IA.

<sup>24</sup> Agevolare lo sviluppo e l'adozione di soluzioni di IA nelle imprese, con l'ottica non solo di efficientare gli attuali processi ma anche di abilitarne di nuovi che sappiano aprire altrettante nuove possibilità di crescita.

<sup>25</sup> Promuovere una formazione di elevata qualità, allineata alle nuove competenze richieste per affrontare le sfide che l'IA ci porrà negli anni a venire.



La relativa attuazione (in merito alla quale sono stati individuati e valutati dei rischi<sup>26</sup>) prevede n. 24 azioni strategiche<sup>27</sup> e n. 3 abilitanti, tra cui due prevalentemente infrastrutturali ("patrimonio di conoscenza nazionale: *dataset* e modelli" e "infrastrutture di rete per l'IA") e la creazione di una "Fondazione per l'IA", incaricata dell'attuazione, coordinamento e monitoraggio. Il documento riconosce **l'IA quale "elemento determinante per garantire la sicurezza nazionale e la difesa del Paese" e la "difesa" quale settore "altamente critico" per gli interessi nazionali**<sup>28</sup>.

## 2.2 LO SCENARIO INTERNAZIONALE

### 2.2.1. NATO

La strategia della NATO del 2024 (che costituisce la revisione della prima edizione risalente al 2021) si inquadra nel più ampio campo delle iniziative dell'Alleanza finalizzate a promuovere l'adozione delle *Emerging and Disruptive Technologies* (EDTs).

Nella strategia alleata vengono delineati 4 scopi:

1. costituire fondamento per promuovere lo sviluppo e l'impiego responsabile dell'IA;
2. accelerare l'adozione della tecnologia nei processi di sviluppo capacitivo, incrementando l'interoperabilità;
3. proteggere e monitorare le soluzioni sviluppate in ambito alleato, garantendo il rispetto di principi di impiego responsabile;
4. identificare e prevenire le minacce derivanti dall'impiego malevole dell'IA.

Sono inoltre definiti 9 esiti desiderati, tra i quali si evidenziano i seguenti:

- sfruttare il programma DIANA (*Defence Innovation Accelerator for the North Atlantic*) per dare alla NATO e ai suoi alleati accesso a laboratori e infrastrutture per testare e validare le applicazioni di IA;
- definire passi misurabili per l'integrazione dell'IA tramite il NATO *Defence Planning Process* (NDPP); la correlazione con il NDPP costituisce elemento teso a concretizzare le azioni promosse dalla strategia e manifesta l'intento dell'Alleanza di "costringersi" a monitorare nel modo più efficace possibile lo sviluppo di capacità abilitate dall'IA nel proprio ambito, in tutti i domini operativi<sup>29</sup>;
- conseguire una forza lavoro, in ambito Alleanza, sempre più capace/competente in materia di IA, con il supporto di attività volte allo sviluppo di "talenti" (tramite iniziative quali borse di studio, identificazione di modalità per attrarre e introdurre nell'organizzazione profili professionali ad alta specializzazione, familiarizzazione delle risorse umane dell'Alleanza, militari e civili, con nuove competenze digitali).

Tra gli elementi che, secondo la strategia NATO, devono collaborare alla salvaguardia degli sforzi dell'Alleanza volti a favorire l'adozione dell'IA, vi devono essere la comprensione e il monitoraggio dello scenario interno ed esterno all'Alleanza, con un focus dedicato ai potenziali avversari, attesa la preoccupazione per le minacce poste dall'impiego malevolo della tecnologia, ad esempio, nel campo della *cognitive warfare*<sup>30</sup>.

26 Il rischio di non fare, il rischio dell'omogenizzazione, il rischio dell'iper regolazione nazionale, il rischio per il mondo del lavoro, il rischio del *digital divide* e il rischio dell'inefficacia (rife. "Strategia italiana per l'IA '24-'26", pag. 11-12).

27 6 per la ricerca, 6 per la pubblica amministrazione, 5 per le imprese e 7 per la formazione.

28 Rife. "Strategia italiana per l'Intelligenza Artificiale 2024-2026", pag. 23, Azione strategica PA.3 (Linee guida per la realizzazione di applicazioni di IA nella Pubblica Amministrazione).

29 *Land, Maritime, Air, Cyber and Space*.

30 La c.d. guerra cognitiva è una forma di lotta in cui il campo di battaglia diventa la mente umana, allo scopo di influenzare e manipolare il nostro comportamento.



Infine, si rileva che la strategia IA alleata tiene in debita considerazione il contributo delle attività di *Strategic Communication* (STRATCOM) all'efficacia degli sforzi posti in essere, con l'obiettivo di dimostrare che la NATO è "AI ready" a supporto della deterrenza e difesa.

### 2.2.2. UNIONE EUROPEA

A partire dal 2018, l'Unione Europea ha sviluppato un approccio progressivo e multilivello all'IA, combinando norme, orientamenti etici e politiche di investimento. Il percorso formale può essere ricondotto a due binari principali:

- la costruzione di un quadro normativo e di *governance* a tutela dei diritti fondamentali dei cittadini;
- iniziative politiche e di finanziamento volte a sostenere l'eccellenza tecnologica e l'adozione dell'IA nell'economia europea.

Questa strategia è stata esplicitata e raffinata tramite la pubblicazione di documenti strategici pubblicati dalla Commissione Europea, dal "*Coordinated Plan on Artificial Intelligence*" del 2018 fino all' "*AI continent Action Plan*" del 2025, e in strumenti legislativi condivisi con gli Stati membri, culminati con il Regolamento "AI Act", che è entrato in vigore il 1 agosto 2024 con varie scadenze di applicazione, differite per specifiche categorie di obblighi (es. alcune disposizioni e divieti sono già entrati in funzione in date diverse). L'AI Act ha fissato classificazioni di rischio, obblighi per operatori e fornitori e strumenti di *governance* per bilanciare innovazione e tutela dei cittadini. L'AI Continent Action Plan del 2025 è invece pensato per trasformare l'Europa in un "continente AI", cioè un ecosistema che non solo regoli l'IA ma la sviluppi e la diffonda su scala industriale e scientifica, con un insieme di azioni che spaziano dalla creazione di centri di calcolo distribuiti sul territorio europeo, la mobilitazione di investimenti per l'industria, la formazione e la valorizzazione dei talenti.

Riguardo all'utilizzo dell'IA in ambito Difesa, non esiste ancora un piano unitario e vincolante, ma una serie di iniziative, rapporti e orientamenti che ne delineano il ruolo emergente. Un punto di riferimento è il "*Strategic Compass for Security and Defence*" (2022), la *roadmap* politica che guida l'azione europea nel campo della difesa comune. Pur non dedicandosi esclusivamente all'IA, questo documento individua le tecnologie emergenti, inclusa l'intelligenza artificiale, come elementi chiave per la modernizzazione delle capacità militari, la resilienza e la sicurezza collettiva. Parallelamente, il Parlamento europeo ha elaborato analisi specifiche. Nel 2025, è stato pubblicato il briefing "*Defence and Artificial Intelligence*", che descrive come l'IA stia trasformando la guerra moderna, sottolineando sia le opportunità (sistemi di sorveglianza avanzata, supporto decisionale, difesa cibernetica) sia i rischi legati ad applicazioni letali autonome e al rispetto del diritto internazionale umanitario.

In tempi più recenti, l'UE ha lanciato iniziative come "*Readiness 2030*", che punta a rafforzare le capacità tecnologiche e produttive della difesa europea, includendo l'IA tra le aree da sviluppare, insieme a *cyber*, spazio e guerra elettronica. Inoltre, il Parlamento ha discusso risoluzioni su un Libro Bianco per la Difesa europea, dove si sollevano questioni legate al *dual-use* (tecnologie a uso sia civile sia militare) e all'impatto del nuovo AI Act, che ha escluso esplicitamente l'ambito militare dal suo campo di applicazione.

### 2.2.3. ORGANIZZAZIONE DELLE NAZIONI UNITE (ONU)

L'ONU ha intensificato il proprio impegno per una **governance globale dell'IA**, riconoscendo il potenziale trasformativo di tale tecnologia e i rischi associati alla sua diffusione incontrollata. Le iniziative mirano a promuovere un uso **etico, inclusivo e sostenibile** dell'IA, in linea con gli Obiettivi di Sviluppo Sostenibile (*Sustainable Development Goals - SDGs*).



Di seguito si riportano le principali iniziative:

- **Risoluzione "Seizing the opportunities of safe, secure and trustworthy Artificial Intelligence systems for sustainable development"** (marzo 2024): prima risoluzione in tale ambito che intende definire le capacità ed i limiti di utilizzo dell'IA, per l'avvio di una riflessione più strutturata nell'ambito dell'ONU. Nel merito, non esistendo ancora una disciplina univoca a livello internazionale che intervenga sulla materia, il testo proposto dagli USA, ancorché non vincolante, costituisce<sup>31</sup> un valido punto di partenza sull'impiego dell'IA al fine di garantire la centralità dell'uomo nel processo decisionale che impiega l'IA, massimizzare i risultati di utilizzo dell'IA e minimizzare le violazioni del DIU.
- **Global Digital Compact** (settembre 2024): primo accordo universale sulla *governance* digitale, incluso l'uso dell'IA, al fine di assicurare che la tecnologia serva l'umanità, promuovendo equità, trasparenza e sostenibilità.
- **International independent scientific Panel on AI**: iniziativa, con co-presidenza bilanciata tra Paesi sviluppati e in via di sviluppo, volta a fornire valutazioni scientifiche indipendenti sui rischi e benefici dell'IA attraverso la pubblicazione di report annuali redatti da un gruppo di 40 esperti globali.
- **Global Dialogue on AI governance** (settembre 2025): iniziativa per il dialogo tra Stati, settore privato, società civile e accademia su temi quali l'interoperabilità tra regimi di *governance*, l'innovazione aperta, la condivisione di buone pratiche e le implicazioni dell'IA in tutte le sue dimensioni<sup>32</sup>; integrerà gli sforzi esistenti in tutto il mondo, compresi quelli dell'OECD<sup>33</sup>, del G7 e delle organizzazioni regionali, e fornirà una piattaforma inclusiva e stabile per gli sforzi di coordinamento della *governance* dell'IA.
- **Coalizione per un'IA sostenibile dal punto di vista ambientale** (guidata da UNEP<sup>34</sup>, ITU<sup>35</sup> e Francia) con l'obiettivo di accelerare lo slancio globale per portare l'IA su un percorso più sostenibile dal punto di vista ambientale. Tale Coalizione riunisce le parti interessate<sup>36</sup> lungo tutta la catena del valore dell'IA per il dialogo e per ambiziose iniziative di collaborazione.
- **Digital@UNGA 2025** Iniziativa congiunta ITU-UNDP<sup>37</sup> per ridurre il *digital divide* attraverso l'implementazione di specifici progetti come i programmi "Elevate"<sup>38</sup> di Microsoft sulla formazione in competenze IA.

La comunità internazionale ha avviato inoltre specifiche iniziative al fine di garantire che l'**IA in ambito militare** sia sviluppata e utilizzata in modo etico, trasparente e conforme al diritto internazionale. Nello specifico:

- **Risoluzione ONU "Artificial Intelligence in the military domain and its implications for international**

31 Tale risoluzione, insieme ai riferimenti normativi ivi contenuti ed agli obiettivi dell'Agenda 2030 dell'ONU, mira a fissare un quadro giuridico quanto più possibile condivisibile dagli Stati Membri dell'ONU, nel pieno rispetto della Carta delle Nazioni Unite e della Dichiarazione Universale dei Diritti Umani.

32 Sociale ed economica, etica e tecnica, culturale e linguistica.

33 *Organization for Economic Cooperation and Development*, di cui l'Italia è uno dei 20 Paesi fondatori.

34 *United Nation Environment Program*: agenzia dell'ONU che lavora contro i cambiamenti climatici a favore della tutela dell'ambiente e dell'uso sostenibile delle risorse naturali.

35 Unione Internazionale delle Telecomunicazioni.

36 Oltre 100 *partner*, tra cui 37 aziende tecnologiche, 11 Paesi e 5 organizzazioni internazionali.

37 *United Nation Development Program*: agenzia dell'ONU che lavora per sradicare la povertà, ridurre le disuguaglianze e promuovere lo sviluppo sostenibile, aiutando i Paesi a sviluppare capacità istituzionali, politiche di leadership e resilienza.

38 Elevate è un programma da 4 miliardi di dollari per formare 20 milioni di persone in competenze IA entro il 2027. Il progetto rientra nella piattaforma globale *Partner2Connect Digital Coalition* dell'ITU, che ha già mobilitato oltre 80 miliardi di dollari con l'obiettivo di raggiungere 100 miliardi entro il 2026.



**peace and security**" (dicembre 2024) avente l'obiettivo applicare il DIU a tutte le fasi del ciclo di vita dell'IA in ambito militare, promuovere trasparenza, responsabilità e cooperazione internazionale. Iniziativa discendente da tale risoluzione è il Workshop periodico *"Military AI, Peace & Security"* (MAPS), che mira ad approfondire le complesse opportunità e sfide poste dall'integrazione dell'IA nel dominio militare, esaminando il panorama normativo esistente e valutando revisioni delle proposte normative emergenti, identificando aree di potenziale convergenza tra le opinioni degli Stati membri, tra cui il rafforzamento delle conoscenze.

- **Political Declaration on responsible military use of Artificial Intelligence and Autonomy**, promossa dagli USA in sede ONU, che mira a costruire un consenso internazionale su comportamenti responsabili e a guidare lo sviluppo, l'implementazione e l'utilizzo dell'IA militare da parte degli Stati. La Dichiarazione fornisce una base per lo scambio di buone pratiche e il rafforzamento delle capacità degli Stati firmatari<sup>39</sup>, consentendo di condividere esperienze e idee.
- **Summit "Responsible AI in the Military Domain"** (REAIM): dialogo multilaterale tra Stati, industria, accademia e società civile avviato dal 2023 per promuovere un uso etico, trasparente e conforme al diritto internazionale dell'IA nel settore militare. Nel 2024 è stato firmato<sup>40</sup> un *"Blueprint for action"* che stabilisce linee guida (non vincolanti) per l'uso responsabile dell'IA nel contesto militare.

## 2.3 INIZIATIVE NAZIONALI ESTERE

### 2.3.1. STRATEGIE E GOVERNANCE

Dall'analisi delle iniziative strategiche in materia di IA intraprese dalle diverse nazioni in ambito globale, sono state individuate delle linee d'azione per le quali riportiamo sommariamente il livello di adozione.

Un'iniziativa cruciale per molti Paesi è la redazione di una strategia nazionale dedicata e l'istituzione di un **Ente di governance specifico per l'IA nella Difesa** (ove non già presente). Questo dimostra un impegno a livello governativo per coordinare lo sviluppo e l'implementazione della tecnologia.

Tuttavia, basandosi sulle ricerche effettuate<sup>41</sup> e sui rapporti ufficiali della Commissione Europea, attraverso l'**AI Watch Index**<sup>42</sup>, e di organismi internazionali, come l'**OECD** e la **Stanford University** (con il suo *AI Index Report*), si possono indicare alcune tendenze e Paesi di rilievo.

Quasi tutti i Paesi più industrializzati, o che mirano a esserlo, hanno lanciato una strategia per l'IA. Tra i più noti e citati nei rapporti internazionali ci sono:

39 Oltre 60 Paesi, tra cui Italia, USA, U.K., Corea del Sud.

40 Tra i 61 Paesi firmatari figurano: Italia, Francia, Germania, U.K., Spagna, Svezia, Svizzera, Giappone, Corea del Sud, Australia, Nuova Zelanda, Stati Uniti, Canada, Brasile, Sudafrica, Ucraina, Pakistan, Singapore. Tuttavia, circa 30 nazioni, tra cui la Cina, Russia, Israele Cina, non hanno sostenuto il documento, evidenziando ancora grandi divisioni globali su questo tema.

41 Borchert, H., Schütz, T., & Verbovsky, J. (2024). *The very long game: 25 case studies on the global state of defense AI* (pag. 603). *Springer nature*. Dalla presente pubblicazione sono stati tratti anche i dati utilizzati per l'elaborazione delle infografiche.

42 L'indice *AI Watch* fornisce un insieme strutturato di indicatori quantitativi sulle prestazioni e il posizionamento dell'UE in diverse dimensioni dell'IA rilevanti per l'elaborazione delle politiche. L'indice è organizzato attorno a cinque dimensioni: G: Visione globale del panorama dell'IA, I: Industria, R: Ricerca e sviluppo (R&S), T: Tecnologia, S: Aspetti sociali.



- **Paesi Europei (UE e non UE):** praticamente tutti gli stati membri dell'Unione Europea (come **Italia, Francia, Germania, Spagna**, ecc.) hanno strategie nazionali, in linea con il Piano coordinato sull'Intelligenza Artificiale dell'UE. Altri Paesi europei come il **Regno Unito**, la **Svizzera** e la **Norvegia** hanno strategie proprie.
- **Stati Uniti:** hanno adottato un approccio che combina strategie ed "**executive orders**" (ordini esecutivi) per indirizzare lo sviluppo e la regolamentazione dell'IA, con un forte impulso su ricerca e sicurezza.
- **Canada:** è stato uno dei primi a lanciare una strategia nazionale ("**Pan-Canadian Artificial Intelligence Strategy**").
- **Cina:** con la sua ambiziosa "**Next Generation Artificial Intelligence Development Plan**", è un attore globale di assoluto rilievo.
- **Singapore:** ha introdotto la "**National AI Strategy-2.0**".
- **Giappone, Corea del Sud, India:** hanno tutti adottato strategie nazionali, o sono in fase di redazione avanzata.

Anche Paesi come l'**Australia**, il **Brasile** e gli **Emirati Arabi Uniti** hanno sviluppato piani strategici.

Dal punto di vista della *governance* si possono individuare due modelli principali:

- **Ente dedicato alla sicurezza e all'etica** (Modello UK/USA): creazione di nuovi istituti specializzati per valutare e mitigare i rischi dei modelli di frontiera (c.d. *frontier AI*).
- **Autorità di vigilanza designate** (Modello UE/Italia): assegnazione del controllo e dell'applicazione delle norme (come l'*AI Act*) ad agenzie esistenti (e.g. Autorità di protezione dei dati) o la creazione di comitati interministeriali.

### 2.3.2. SVILUPPO DI ALGORITMI E TECNOLOGIE PROPRIETARIE

Le Nazioni stanno investendo in ricerca e sviluppo per creare algoritmi e tecnologie di IA proprietarie, al fine di garantire l'autonomia strategica e il vantaggio competitivo.

- **Nazioni con sviluppo proprietario:** Francia, Germania, Regno Unito, Stati Uniti, Finlandia, Norvegia, Estonia, Russia, Cina, India, Arabia Saudita.
- **Nazioni senza sviluppo proprietario evidente:** fra le nazioni analizzate solo l'Estonia e la Lettonia si affidano anche a collaborazioni esterne, ma mantengono un *focus* sullo sviluppo interno.

Circa l'80% dei Paesi analizzati punta esplicitamente a sviluppare capacità tecnologiche sovrane nel campo dell'IA.

### 2.3.3. INFRASTRUTTURE E POTENZA DI CALCOLO

La disponibilità di infrastrutture di calcolo ad alte prestazioni è considerata un motore fondamentale per lo sviluppo dell'IA:

- **Nazioni con piani per l'infrastruttura di calcolo:** Francia, Germania, Regno Unito, Stati Uniti, Russia, Cina, India, Arabia Saudita.
- **Nazioni che non hanno piani per l'infrastruttura di calcolo:** l'India e l'Arabia Saudita sono state incluse nella categoria di nazioni con piani per l'infrastruttura di calcolo. La Lettonia e la Lituania pur non avendo menzionato piani specifici, si concentrano sullo sviluppo di un solido ecosistema di dati, considerato un prerequisito.

Quasi il 60% delle nazioni ha piani specifici e investimenti dedicati al potenziamento delle infrastrutture di calcolo.



### 2.3.4. GESTIONE DEI TALENTI

Attrarre, formare e trattenere specialisti in IA è una priorità comune. Le nazioni stanno implementando programmi specifici, borse di studio e politiche di immigrazione per costruire un solido capitale umano.

**Nazioni con iniziative per i talenti:** Francia (c.d. "Passaporto per talenti"), Germania (finanziamento per ricercatori *junior*), Regno Unito (borse di studio), Stati Uniti (programmi di sviluppo e scambio), Finlandia (NDU), Estonia (*AI Leap*), Lettonia, Lituania, Russia (sostegno agli sviluppatori), Cina (incentivi per il rientro), India (programmi di formazione come CSPAI), Arabia Saudita (programmi di formazione specializzata).

### 2.3.5. FOCUS SULLA FORMAZIONE E LA RICERCA

L'IA è una tecnologia che ha stimolato in modo evidente gli investimenti in ambito internazionale. Paesi come Stati Uniti, Regno Unito, Francia, Cina e Russia sono in prima linea, ma anche altri attori come Germania, Giappone, Arabia Saudita, Spagna, Canada, Turchia, Ucraina, Israele, Grecia, Belgio e Paesi Nordici hanno dimostrato un chiaro e crescente interesse.

L'analisi degli approcci nazionali sull'IA in ambito militare ha messo in evidenza che la formazione e la professionalizzazione del capitale umano siano ritenute fondamentali. Nello specifico:

- molti Paesi, inclusi il Regno Unito, la Finlandia e la Grecia, investono molto nella riqualificazione del personale in servizio per dotarsi di un *basket* di risorse umane in possesso di adeguato *background* tecnico-professionale. Questo approccio si accompagna alla volontà di incrementare l'"IA literacy" a ogni livello;
- un numero crescente di Paesi sta adottando un approccio che include anche il personale civile e i *partner* industriali per creare un ecosistema di competenze più resiliente.

### 2.3.6. CENTRALIZZAZIONE DI COMPETENZE E RESPONSABILITÀ

La ricognizione svolta indica che la tendenza principale per adottare ed integrare sistemi di IA in ambito militare, probabilmente per ridurre i rischi e i costi, è quella di affidarsi a strutture già esistenti.

Tuttavia, un numero crescente di Paesi creano all'interno della Difesa nuove unità dedicate (non necessariamente militari) per accelerare l'innovazione, anche se soggetti a conflitti di competenza e frammentazione. Per tale motivo, Paesi come gli Stati Uniti (con la DIU), il Regno Unito (con il DAIC) e la Francia (con l'AMIAD), la Russia (con Technopolis) e la Turchia (con SAYZEK) hanno istituito uno specifico centro di eccellenza/laboratorio quale elemento di raccordo e aggregazione di idee, per acquisire competenze nonché per avviare iniziative rivolte allo sviluppo e alla realizzazione di soluzioni basate sull'IA.

### 2.3.7. PARTNERSHIP CIVILE-MILITARE

La *partnership* civile-militare, sebbene con diverse declinazioni e attraverso diversi modelli (figure 3 e 4), assume importanza strategica a carattere generale, venendo descritta come la principale leva di innovazione. Si va dal modello di fusione sistemica cinese, all'ecosistema di *startup* e all'osmosi di talenti nell'approccio israeliano, fino al modello ucraino basato su contributi privati e volontari che ha dimostrato un'incredibile agilità.

### 2.3.8. TEMI ETICI E USO RESPONSABILE DELL'IA

Per quanto riguarda i temi etici legati allo sviluppo, all'adozione e all'impiego dell'IA nella Difesa, si registra che, mentre la maggior parte dei Paesi, in particolare quelli europei, pongono l'accento sui temi etici e sull'uso responsabile, attraverso un approccio "umano-centrico" in cui l'IA è un supporto e non un sostituto, alcuni Stati, spinti anche da esigenze operative, si orientano verso lo sviluppo di sistemi di IA che possano agire in modo autonomo.

### 2.3.9. CONSIDERAZIONI FINALI

Dalla disamina degli elementi sopra illustrati, emergono nettamente quali prerequisiti essenziali:

- la disponibilità di **infrastrutture abilitanti**;
- lo sviluppo e il mantenimento dei "**talenti**"<sup>43</sup>;
- la necessità di dotarsi di una **struttura in grado di supportare l'autonomia strategica operativa in ambito IA**.

43 Considerati parte integrante dell'infrastruttura "critica" della Difesa in materia di IA.

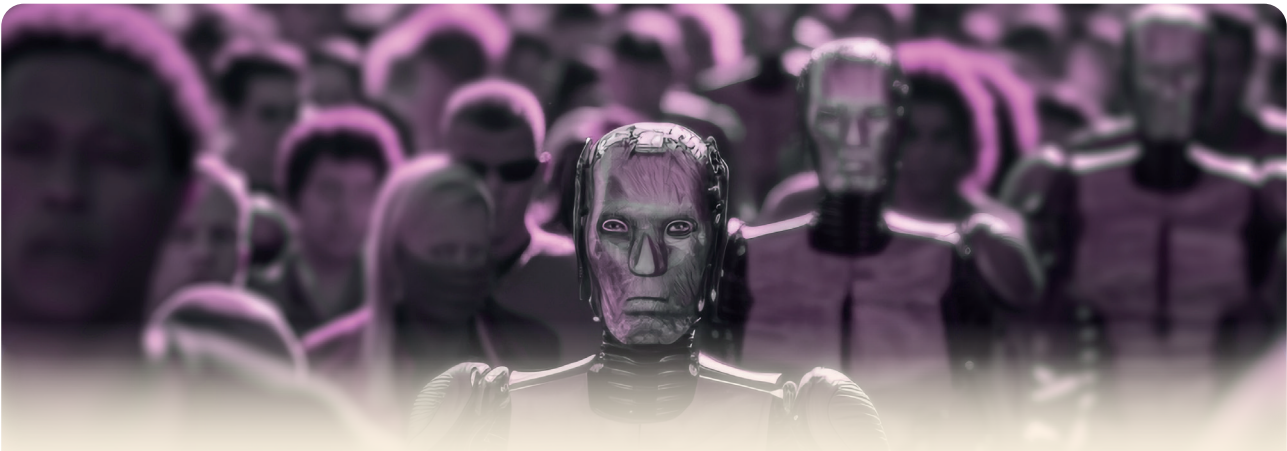
#### MODELLI DI COLLABORAZIONE CIVILE-MILITARE

L'innovazione nell'IA per la difesa non avviene in isolamento. Le nazioni stanno esplorando diversi modelli di *partnership* per unire le competenze del settore civile, accademico e militare. Questi approcci riflettono le culture strategiche e gli ecosistemi tecnologici specifici di ogni paese.



Figura 3 – Modelli collaborazione civile-militare





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

| Modello               | Punti di forza                                                                                           | Punti di debolezza                                                                   | Esempi                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------|
| <b>TRIPLA ELICA</b>   | 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 |
| <b>REVOLVING DOOR</b> | Scambio continuo di talenti e idee, rapida innovazione, forte cultura tecnologica                        | Dipendenza da un unico bacino di talenti, possibili carenze di personale militare    | Israele                                   |
| <b>TOP-DOWN</b>       | Coordinamento centralizzato, obiettivi chiari, mobilitazione di risorse su larga scala.                  | Poca flessibilità, mancanza di competitività, rischio di "pensiero unico".           | Cina, Russia, Iran                        |
| <b>OPEN DOOR</b>      | Risposta agile a bisogni specifici, riduzione della burocrazia, sfruttamento del <i>crowd sourcing</i> . | Poca flessibilità, mancanza di competitività, rischio di "pensiero unico".           | Ucraina                                   |
| <b>SILO</b>           | Maggiore sicurezza e compartimentazione, autonomia decisionale.                                          | Nessuna sinergia con il settore civile, obsolescenza tecnologica, spreco di risorse. | Canada                                    |

**Figura 4** – Punti di forza vs debolezza dei modelli collaborazione civile-militare







# 03

## L'IA PER LA DIFESA: CONTESTI DI INTERESSE

L'IA non è semplicemente un'opzione, ma una necessità strategica. Solo un approccio olistico potrà dare il giusto valore alla tecnologia in esame trasformandola in vantaggio competitivo sostenibile nel tempo

In questo capitolo si individuano gli scenari di impiego dell'IA più paganti negli ambiti di interesse della Difesa, a iniziare da quello operativo, essenza stessa del Comparto, passando da quello organizzativo, che avvicina l'istituzione a una grande *corporate*; quello formativo, essenziale per generare ed espandere la conoscenza della tecnologia, per giungere al rapporto con l'industria, in cui è ricercato un approccio più proattivo a vantaggio dell'intero Sistema Paese. L'esercizio, direttamente ancorato ai due pilastri abilitanti delle infrastrutture e competenze descritti in precedenza, è funzionale a tracciare in fase attuativa una *roadmap* che preveda:

- **nel breve periodo (entro 1 anno):** un'azione decisa sulle condizioni abilitanti fondamentali quali la *governance*, lo sviluppo delle infrastrutture, il potenziamento delle competenze, l'ottimizzazione dei processi, nonché l'abbattimento degli ostacoli normativi, organizzativi e gestionali che potrebbero limitare l'efficacia della strategia;
- **nel medio termine (entro 2 anni):** lo sviluppo e l'introduzione graduale di applicazioni IA nei settori operativi considerati prioritari, con l'obiettivo di potenziare la capacità decisionale, informativa e operativa;
- **nel lungo termine (entro 3 anni):** l'adozione diffusa dell'IA in ogni ambito della Difesa, a supporto delle attività militari, dalla pianificazione strategica alla condotta tattica, tanto sul territorio nazionale quanto all'estero, ricercando un vantaggio sostenibile attraverso un più solido tessuto *Defence Tech* nazionale.



### 3.1 L'IA NEI CONTESTI OPERATIVI

Il *battlespace* contemporaneo si configura quale **ambiente estremamente complesso e intrinsecamente multi-dominio** ove la capacità di coordinare gli effetti è una chiave irrinunciabile per il successo operativo. L'attuale competizione è inoltre dominata dalla **trasparenza del campo di battaglia**, una condizione, dovuta all'elevata diffusione di sensori, che pone le FF.AA. di fronte a sfide senza precedenti e dove, di conseguenza, il successo operativo dipende sempre più dalla capacità di interpretare correttamente una massa di dati eterogenei in modo estremamente rapido ed efficace.

A rendere ancora più complessa questa dinamica si aggiunge l'**uso spregiudicato delle tecnologie**, da quelle emergenti ed estremamente costose a quelle a basso costo e di derivazione commerciale, che di fatto hanno "democratizzato" l'accesso a capacità un tempo riservate alle grandi potenze e reso, peraltro, inefficaci piattaforme più complesse e costose.

Un'altra evoluzione fondamentale è l'aumento esponenziale dell'impiego di **sistemi robotici** terrestri, aerei e marittimi. La loro integrazione sempre più profonda nel *battlespace* ha portato alla definizione di una nuova geometria della competizione, l'area robotica del campo di battaglia, ove tali piattaforme svolgono i compiti più rischiosi e pericolosi.

Parallelamente, l'informazione si è evoluta in un'arma a tutti gli effetti. La c.d. **cognitive warfare**, condotto tramite campagne di disinformazione, *fake news* e la creazione di *deepfake*, è diventato un elemento onnipresente.

Infine, tutti questi *trend* sono accelerati dall'elevata **digitalizzazione del conflitto**, che ha reso il processo decisionale radicalmente più rapido e quasi scientifico, allontanandosi dall'approccio basato maggiormente sull'intuizione e sull'esperienza del Comandante.

Nel contesto descritto, **l'IA non è semplicemente un'opzione, ma una necessità strategica**. Solo un approccio olistico, che tenga conto dei numerosi aspetti da essa sottesi, potrà dare il giusto valore alla tecnologia in esame trasformandola in vantaggio competitivo sostenibile nel tempo. Lo scopo del presente paragrafo è traghettare il futuro dell'IA in ambito operativo al fine di tracciare i settori prioritari su cui focalizzare l'attenzione.





### 3.1.1. LE OPZIONI DI IMPIEGO DELL'IA NELLA PIANIFICAZIONE E NELLA VALUTAZIONE DEGLI EFFETTI NON CINETICI

L'impiego dell'IA nel processo di **pianificazione** delle operazioni rappresenta un elemento di assoluta centralità per assicurare la superiorità informativa in ambito operativo. Grazie alle sue capacità, l'IA consente di automatizzare l'elaborazione di una grande mole di dati, permettendo così una valutazione dinamica e tempestiva dei possibili scenari operativi. Questo processo di "*decision augmentation*" fornisce un supporto strategico irrinunciabile, consentendo di selezionare l'opzione operativa più bilanciata a valle di una rigorosa analisi di rischi, benefici e opportunità. In tale ambito, anche uno strumento "tradizionale" quale il **wargaming**<sup>44</sup>, può essere enormemente potenziato dall'IA, superando i limiti dei tradizionali scenari statici e predefiniti ed evolvendo in *adaptive wargaming*<sup>45</sup>.

Un particolare cenno lo merita la **valutazione degli effetti non cinetici**<sup>46</sup>, che rivestono un ruolo sempre più cruciale negli attuali scenari di impiego. L'integrazione di soluzioni basate sull'IA ha potenziato in modo significativo la capacità di pianificare, coordinare e valutare con precisione tali effetti, consentendo l'individuazione di vulnerabilità sistemiche nonché target cognitivi e informativi strategici. Si tratta dunque di una capacità che va prioritariamente presidiata e potenziata per gli aspetti di monitoraggio e previsione.

- .....
- 44 È uno strumento di analisi che, attraverso la rappresentazione di simulazioni complesse realizzate da esperti del settore, è in grado di fornire un fondamentale contributo ai processi decisionali, alla sperimentazione e validazione di idee, concetti e soluzioni dottrinali, alla formazione.
- 45 L'IA potrà creare simulazioni dinamiche in cui le forze avversarie reagiscono e si adattano in tempo reale alle decisioni e alle azioni delle forze amiche, contribuendo a generare un'infinità di varianti di scenario in cui esplorare, in chiave predittiva, altrettante scelte operative.
- 46 Comprendono l'insieme delle azioni volte a influenzare volontà, percezioni e capacità decisionali dell'avversario, senza ricorrere direttamente all'uso della forza. Tra i principali ambiti d'impiego si annoverano la **manipolazione informativa**, **l'influenza psicologica**, **la guerra elettronica** e **le operazioni cibernetiche**, finalizzate a compromettere la coesione interna, la capacità di reazione e le infrastrutture critiche.



UNA DIFESA CHE  
INTEGRA L'IA IN  
OGNI FASE DELLE  
OPERAZIONI,  
RICERCANDO LA  
SUPERIORITÀ  
DECISIONALE,  
L'INCREMENTO  
DI EFFICIENZA  
ED EFFICACIA E  
LA PROTEZIONE  
DELLE FORZE



### 3.1.2 LE PROSPETTIVE DI IMPIEGO FUTURO DELL'IA NELLA CONDOTTA DELLE OPERAZIONI

Il Ministro della Difesa e i vertici Militari dovranno essere in grado di accedere con immediatezza alle pertinenti informazioni operative, amministrative, tecniche e logistiche operative relative agli assetti delle FF.AA. in operazioni e addestramento, tanto in Patria quanto all'estero, al fine di disporre di una *picture*, multi-livello (politico-strategico-operativo-tattico), multi-dominio e multi-dimensione, finalizzata a supportare i decisori politici e militari nei vari contesti in cui il Dicastero Difesa dovrà operare.

Al riguardo, l'adozione di sistemi di IA nella **Difesa integrata del territorio**<sup>47</sup> consentirà di monitorare e migliorare la *situational awareness*, facilitata da sistemi di valutazione ed *early warning* integrati dalla capacità di rilevamento di anomalie elettromagnetiche sul territorio nazionale.

Per gestire la complessità delle **Multi-Domain Operations** (MDO) e della multi-dimensionalità, la sola capacità di elaborazione e analisi umana non risulta più sufficiente. Nell'ambito operativo, l'IA potrà trovare la massima espressione e impiego nelle fasi di analisi, comprensione e orientamento, lasciando ai Comandanti, ai vari livelli, la responsabilità delle successive fasi di decisione e di azione, essendo potenzialmente in grado di scalare l'efficacia e l'efficienza di ogni *Joint Function*<sup>48</sup>, risultando altresì irrinunciabile per la *Stability Policing* e i compiti di Polizia militare.

Nell'ambito del **Comando e Controllo** e nel processo di *decision-making*, l'IA può offrire un contributo decisivo non ponendosi quale sostituto ma come acceleratore delle capacità umane. La sua funzione principale sarà quella di integrare la quantità esponenziale di dati provenienti dalle molteplici fonti e supportare il decisore – anche ai livelli più bassi – nell'apprezzamento della situazione<sup>49</sup>, nella gestione del campo di battaglia, nella valutazione degli effetti cinetici e non cinetici delle azioni e nella pianificazione e gestione logistica delle forze a lui assegnate. Sfruttando l'analisi predittiva sarà possibile prefigurare scenari futuri, valutare gli esiti attesi delle diverse scelte operative e identificare i potenziali rischi, in modo tale da fornire al decisore un serie di possibili opzioni per conseguire gli effetti desiderati ovvero risolvere situazioni critiche. Si tratta di un **settore ad alta priorità**, in quanto funzionale a conseguire la superiorità decisionale.

L'**intelligence** è fondamentale per anticipare le minacce, comprendere gli avversari e supportare le operazioni militari. L'IA è il motore dell'info-valorizzazione trasformando una mole ingestibile di dati in "*intelligence operativa*" e risultando essenziale per l'integrazione di fonti multiple<sup>50</sup>, correlare dati apparentemente non collegati, anticipare le intenzioni degli avversari e rafforzare la sicurezza dell'intero ciclo *intelligence*.

L'IA può contribuire alla **manovra** attraverso il supporto di piattaforme robotiche e il loro coordinamento. Proprio

47 In tale ambito, l'infrastruttura capillare delle articolazioni territoriali dell'Arma dei Carabinieri costituisce un asset strategico che moltiplica la capacità di risposta flessibile e multidimensionale alle minacce ibride.

48 C2, *Intelligence, Manoeuvre, Fires, Information, Force Protection, Civil and Military Cooperation, Sustainment*. AJP-3, *Allied Joint Doctrine For The Conduct Of Operations, Edition C Version 1*.

49 Inclusa la Space Situational Awareness, che non può prescindere dall'acquisire un'adeguata capacità di conoscere la posizione dei satelliti artificiali e determinarne potenzialità ed eventuali pericoli per gli assetti spaziali nazionali e/o alleati derivanti da manovre ostili.

50 Quali l'intelligence umana (HUMINT), dei segnali (SIGINT), delle comunicazioni (COMINT), delle emissioni (ELINT), delle analisi di segnali e "firme" fisiche o chimiche di un oggetto o fenomeno (MASINT), dei dati geografici e geospaziali combinati con immagini e altre fonti (GEOINT), delle immagini (IMINT) e delle fonti aperte (OSINT).



gli *Autonomous Weapon Systems (AWS)*<sup>51</sup>, che includono quelli specificamente progettati per l'impiego di forza letale (*Letal AWS*), pongono sfide significative, anche dal punto di vista etico. L'applicazione tattica più attuale e dirompente dell'IA, tuttavia, è lo *swarming*, ovvero il coordinamento di sciame di sistemi senza pilota che agiscono in modo collaborativo per sopraffare le difese, saturare un'area di interesse o generare dilemmi operativi.

L'IA aumenta drasticamente la velocità di ingaggio, la precisione e la verifica dell'efficacia del fuoco. In particolare, i sistemi basati su IA possono riconoscere, selezionare e tracciare particolari obiettivi suggerendo il migliore effetto. Ciò riduce drasticamente il *"sensor to shooter link"*<sup>52</sup> e contribuisce in modo netto alla superiorità decisionale e di ingaggio.

L'IA è un abilitante fondamentale nella gestione dell'**ambiente informativo** e per la *cognitive warfare* poiché con l'aumento della connettività, le identità digitali e le comunità virtuali assumeranno un'importanza crescente, configurandosi come spazi di interazione e partecipazione sempre più influenti ma potenzialmente manipolabili. Al riguardo, l'IA offrirà strumenti sempre più sofisticati per analizzare e rilevare campagne di disinformazione e *deepfake* avversari ovvero identificare potenziali vulnerabilità da sfruttare.

L'IA è divenuta un *asset* fondamentale per la **protezione delle Forze** e delle infrastrutture offrendo capacità avanzate che superano le limitazioni dei metodi tradizionali. Ciò, oltre a rendere più efficiente la sorveglianza delle infrastrutture, appare estremamente efficace per contrastare minacce quali:

- quelle portate attraverso lo spettro elettromagnetico e il dominio *cyber*;
- droni piccoli e difficili da rilevare, anche in sciame;
- missili balistici e ipersonici.

L'IA può inoltre migliorare l'efficacia delle operazioni di **Civil-Military Cooperation (CIMIC)**. Strumenti di analisi evoluti possono fornire un ausilio strategico nel valutare le aree bisognose di intervento e le dinamiche locali cui porre attenzione, contribuendo in modo determinante alla gestione delle crisi, al miglioramento delle operazioni di supporto e dell'eventuale uso della forza nonché alla prevenzione dei conflitti.

Il **sostegno logistico** è il settore in cui l'IA ha raggiunto grande maturità e può offrire soluzioni concrete per ridurre i costi, accelerare flussi e funzioni e migliorare la prontezza operativa attraverso la c.d. manutenzione predittiva, l'ottimizzazione della catena dei rifornimenti, recuperi e sgomberi, che potranno avvenire attraverso i canali più sicuri e veloci e sfruttando tecnologie che minimizzano la necessità di operatori umani.

L'attuale scenario geopolitico internazionale, infine, richiede alla Difesa di prepararsi a scenari di stabilizzazione a lungo termine di aree territoriali eterogenee. In tale contesto, si rivela essenziale disporre di un efficace sistema di *Early Warning* e l'utilizzo di strumenti di analisi predittiva per anticipare potenziali focolai di instabilità e ottimizzare le attività di **Polizia Militare** e **Stability Policing**.

51 I sistemi d'arma autonomi sono quelle piattaforme che, una volta attivate, possono selezionare e ingaggiare obiettivi senza ulteriore intervento di un operatore. Si tratta, ad esempio, di droni o piattaforme senza pilota, anche in sciame, ormai diventati una componente centrale delle operazioni militari.

52 Il moderno approccio si basa sul concetto di *any sensor, right decisor, best shooter*, significando che un dato proveniente da qualsiasi sensore, opportunamente valorizzato, è alla base di una decisione assunta al giusto livello per un ingaggio che sfrutta la migliore soluzione disponibile, operante in qualsiasi dominio.



La sfera operativa militare mira dunque a sfruttare l'IA per il supporto alla pianificazione, la superiorità decisionale, la velocità d'ingaggio e la protezione multi-dominio.

In tale contesto si prefigurano le seguenti linee d'azione:



**Ufficio per l'IA:**

- definisce l'indirizzo generale contenente i *policy frameworks* strategici;
- è garante di un robusto quadro etico e legale, essenziale per la condotta di operazioni in coalizione;
- è preposto al monitoraggio per assicurare il rigoroso rispetto dei principi etici e normativi nell'impiego operativo dell'IA.



**Laboratorio di IA per la Difesa (LIAD):**

agisce come *AI Delivery Center* per:

- creare, trasformare, sperimentare e rendere operative le soluzioni di IA in base ai requisiti operativi generati dalle articolazioni tattiche.
- realizzare progetti operativi in maniera rapida e scalabile e che siano funzionali e rispondenti ai requisiti di sicurezza sul campo, mirando al vantaggio strategico.





## 3.2. L'IA NEI CONTESTI ORGANIZZATIVI

Questo paragrafo individua le priorità di intervento, evitando duplicazione di sforzi e tendendo alla massima interoperabilità, per incrementare efficacia ed efficienza e orientare la risorsa umana verso compiti ad alto valore aggiunto.

### 3.2.1. L'IA A SUPPORTO DELLA PRODUTTIVITÀ INDIVIDUALE

Il ruolo dell'IA a supporto della produttività individuale nell'ambito del lavoro di *staff* rappresenta il primo passo ineludibile per generare rapidamente efficienza nel comparto della Difesa. L'obiettivo primario è dotare il personale di strumenti intelligenti che, pur non sostituendo le competenze umane, ne amplifichino l'efficacia, snellendo le tempistiche e alleggerendo il carico di compiti ripetitivi e a basso valore aggiunto.

L'acquisizione ovvero lo sviluppo di un **Large Language Model** (LLM) della Difesa, specificamente addestrato su una vasta gamma di documentazione interna, appare come pre-requisito imperativo. Le sue funzionalità, integrate da IA generativa, contribuirebbero in modo determinante a una più efficiente gestione della conoscenza interna, garantendo un supporto fondamentale nella creazione di bozze di documenti e contenuti multimediali, analisi e sintesi di documenti ed estrazione di informazioni, garantendo una rigorosa coerenza terminologica, la qualità dei risultati, la riduzione dei margini di errore e il risparmio di tempo, orientabile così all'analisi critica.

Tale LLM garantirebbe capacità strategiche, come ad esempio:

- **integrazione informativa** multi-livello: sintesi avanzata di conoscenze provenienti da fonti eterogenee, operante trasversalmente su tutti i livelli decisionali (politico, strategico, operativo e tattico);
- **supporto decisionale adattivo**: *framework* analitici e esperienze di supporto alle decisioni calibrati sulle esigenze specifiche di ciascun livello di comando;
- **mitigazione del rischio**: riduzione delle vulnerabilità derivanti dalla frammentazione e compartimentazione dei dati nelle strutture organizzative;
- **analisi in tempo reale di scenari complessi**: capacità di valutazione dinamica in ambienti operativi ad alta complessità;
- **generazione automatizzata di infografiche**: generazione di infografiche interattive e visualizzazioni *mission-oriented* a supporto della consapevolezza del quadro di situazione;
- **interoperabilità dei sistemi**: integrazione nativa con architetture e piattaforme esistenti e future;
- **capacità di edge computing**: implementazione su dispositivi a risorse limitate, inclusi apparati tattici disconnessi o a connettività intermittente, quali dispositivi mobili *rugged*;
- **vantaggio strategico**: efficacia accresciuta nei processi di pianificazione e condotta delle operazioni.

È importante sottolineare il valore strategico di tale iniziativa, che costituirebbe un *asset* strategico critico per l'autonomia tecnologica nazionale, articolato in:

- **integrazione di dati specialistici**: incorporazione di dati classificati e strutturati del settore difesa, compresa la realizzazione di *knowledge graph* specializzati per requisiti operativi militari;
- **ecosistema nazionale di innovazione**: sviluppo di un polo di eccellenza composto da *team* dedicati alla ricerca applicata e alla collaborazione attiva con il personale militare operante in contesti operativi.



Sulla base di questo, sarà poi possibile implementare ulteriori azioni, come:

- dotarsi di strumenti di **supporto alla gestione degli incontri di lavoro**, come la trascrizione, il riassunto e la traduzione automatica al fine di velocizzare la preparazione di documenti e report;
- implementare **chatbot specialistici** che, rispondendo in tempo reale alle domande, fungano da *advisor* su aree tematiche di interesse;
- adottare strumenti per la **gestione efficiente dei flussi comunicativi** che permettano di implementare filtri intelligenti, individuare priorità, proporre lo smistamento delle pratiche in base a temi e contesto, liberando così il personale da una gestione manuale e spesso dispersiva dei flussi.

### UNA DIFESA CHE SFRUTTA PIENAMENTE L'IA PER MIGLIORARE PRODUTTIVITÀ E PROCESSI, LIBERANDO RISORSE PER COMPITI AD ALTO VALORE AGGIUNTO

Non sottacendo i rischi presenti al livello descritto, quali la **sicurezza dei dati** come priorità assoluta, la **spiegabilità** (*explainability*)<sup>53</sup> e la **fiducia** (*trust*)<sup>54</sup>, è **fondamentale sottolineare che il giudizio umano non deve mai risultare eclissato**.

#### 3.2.2. L'IA A SUPPORTO DELL'UTENZA

L'implementazione dell'IA per supportare direttamente il personale e gli utenti esterni alle piattaforme della Difesa rappresenta una linea strategica fondamentale per migliorare la qualità dei servizi e l'efficienza complessiva percepita. L'obiettivo è superare le complessità burocratiche e informative attraverso un ecosistema di "strumenti intelligenti" che forniscano assistenza immediata, continuativa e personalizzata, basata sul linguaggio naturale.

Per trasformare la semplice informazione in azione, questo sistema di interazione dovrà essere integrato con strumenti di **Robotic Process Automation** (RPA)<sup>55</sup> che permetteranno all'IA di navigare tra moduli, compilare campi, avviare procedure e inoltrare richieste. Un'evoluzione del modello descritto potrà prevedere l'impiego di strumenti di **Agentic IA**, in grado di risolvere problemi complessi e non strutturati. Per garantire la sicurezza e la personalizzazione dei servizi è, tuttavia, essenziale l'integrazione con un sistema di **identità digitale** forte e sicuro che consenta l'autenticazione, l'accesso in modo sicuro ai dati personali e la gestione delle pratiche in modo personalizzato e conforme alle norme in vigore.

53 L'*explainability* è un insieme di processi e metodi che consentono agli utenti umani di comprendere e considerare affidabili i risultati e gli *output* generati.

54 Può condurre a un uso sub-ottimale della tecnologia quando eccessiva ovvero ridotta.

55 Questi ultimi consentono all'IA di non limitarsi a rispondere, ma di eseguire direttamente azioni concrete in nome e per conto dell'utente, previa la sua autorizzazione



La capacità dell'IA di apprendere continuamente da nuove interazioni e da nuovi documenti assicura, infine, che il sistema si evolva nel tempo, migliorando costantemente la qualità del supporto fornito.

### 3.2.3. L'IA A SUPPORTO DEI PROCESSI STRUTTURATI

L'impiego dell'IA nell'ambito dei macro-processi della Difesa rappresenta il passaggio dal supporto individuale all'ottimizzazione strategica su larga scala, con l'obiettivo di trasformare l'efficienza e la capacità decisionale dell'intera organizzazione. A questo livello, gli strumenti operano su vasti insiemi di dati strutturati e non e, per tale motivo, i modelli di IA e di *Business Intelligence* diventano catalizzatori per la riorganizzazione dei processi strategici del comparto.

Tra i vari ambiti, è opportuno evidenziare:

- **Human Resources (HR):** è un settore che prevede un impatto radicale e trasformativo dell'IA, ove risulti compatibile col perimetro normativo di riferimento. Un'area cruciale è la selezione e il reclutamento, dove l'IA può supportare l'identificazione di profili di interesse attraverso l'analisi dei curricula e delle competenze dei candidati. Altri ambiti di applicazione sono la gestione della formazione e delle carriere in modo personalizzato, il supporto alla gestione e impiego del personale o al ricollocamento dei militari che si apprestano a lasciare il servizio attivo;
- **Logistica e Supply Chain:** la logistica, come già visto per le operazioni, è uno dei campi in cui l'IA può generare i maggiori benefici in termini di efficienza e risparmi. Un sistema di gestione intelligente della logistica può analizzare dati storici, climatici e operativi per prevedere la domanda di rifornimenti in modo estremamente accurato, consentendo di ottimizzare scorte, percorsi e spazi, ridurre i costi di stoccaggio e, in genere, minimizzare gli errori umani e i rischi anche in contesti critici. L'introduzione dei **Digital Twin**<sup>56</sup> (gemelli digitali), poi, eleva questo processo a un nuovo livello, consentendo un'analisi che, unita al più ampio uso di sensori, abilita la c.d. **manutenzione predittiva** e la **gestione energetica intelligente**<sup>57</sup>;
- **Amministrazione e finanza:** l'IA offre un vasto potenziale per l'automazione dei processi amministrativi e finanziari, tradizionalmente ad alta intensità di lavoro e a elevato rischio di errore umano. L'IA può supportare il monitoraggio dei flussi, della gestione di bilancio e l'individuazione di anomalie, gestire la classificazione e l'archiviazione di documenti e stimare l'andamento delle spese a supporto della pianificazione finanziaria;
- **Sicurezza:** ancorché non catalogabile come processo strutturato, l'IA non è solo uno strumento di supporto, ma un elemento centrale e irrinunciabile per efficientare il controllo e la sicurezza, sia fisica sia informatica. Nel primo caso, i sistemi intelligenti<sup>58</sup> possono identificare repentinamente comportamenti anomali e attivare le procedure di allarme, nel secondo, l'IA può rilevare e anche bloccare proattivamente le minacce cibernetiche automatizzando le attività di sorveglianza, analisi e difesa.

56 Un *Digital Twin* è una replica virtuale di un *asset* – anche un'infrastruttura – che simula in tempo reale il suo stato, le sue prestazioni e il suo comportamento.

57 Non solo riferita alle infrastrutture, ma anche a sistemi e piattaforme. L'IA si rivela fondamentale per suggerire strategie di risparmio, individuare anomalie o ottimizzare i consumi in modo dinamico.

58 Esempio principe sono i sistemi intelligenti di videosorveglianza che analizzano automaticamente i flussi video, verificando in tempo reale dati biometrici e altre informazioni riferite a persone e oggetti.



L'utilizzo dell'IA nei contesti organizzativi deve essere focalizzata a supportare la produttività individuale e l'ottimizzazione dei processi strutturati (logistica, risorse umane, amministrazione):



**Ufficio per l'IA:**

quale organo di alto profilo, garantisce un coordinamento unitario e autorevole delle tematiche IA, assicurando la funzione di **coerenza strategica** nell'uso efficiente delle risorse, nel definire i *capability targets* e nel garantire l'ottimizzazione e la coerenza programmatica.



**Laboratorio di IA per la Difesa (LIAD):**

- aggrega idee e competenze per **sviluppare soluzioni tecnologiche** che supportano l'utenza e la **produttività individuale** (ad esempio, l'implementazione di LLM della Difesa);
- favorisce l'integrazione dell'IA per ottimizzare i processi strutturati nelle funzioni di supporto come risorse umane, finanza e logistica.



### 3.3 IA, FORMAZIONE, ADDESTRAMENTO E RICERCA

L'IA nel settore della Difesa rappresenta una delle sfide e opportunità più significative del nostro tempo che, come visto, necessita della disponibilità di un'infrastruttura tecnologica idonea e risorse umane, sia militari sia civili, adeguatamente formate. Ciò richiede rapidi interventi (*upskilling e reskilling*) nel corso delle diverse fasi formative con l'obiettivo di superare il divario generazionale esistente, assicurare la continuità operativa del comparto Difesa, sviluppare una base di conoscenza generalista<sup>59</sup> per promuovere un uso etico e responsabile delle nuove applicazioni e prevenire il consolidarsi di *bias*. Tale fase non può essere disgiunta da un potenziamento delle competenze trasversali (*soft skills*) necessarie a far acquisire un *mindset* digitale e a mantenere l'essere umano al centro di questa nuova fase di trasformazione. La formazione, quindi, è un perno determinante attorno a cui ruota l'efficace implementazione dell'IA nella Difesa ed è un fattore abilitante per la disponibilità di personale in possesso di un *background* tecnico-professionale di adeguato livello qualitativo. È essenziale, dunque, dotarsi di un **modello formativo capace di adeguarsi rapidamente** ai cambiamenti e di fornire contenuti erogabili in forma *blended* a distanza per far fronte a esigenze di autoformazione e formazione adattiva personalizzata<sup>60</sup>, ricorrendo a metodologie interattive e coinvolgenti e superando le barriere linguistiche. Potenziando le proprie capacità formative, la Difesa intende investire sul fattore umano, fornendo gli strumenti necessari per sostenerne la motivazione all'aggiornamento e alla crescita professionale.



Immagine generata con AI

<sup>59</sup> È auspicabile accrescere la consapevolezza dei limiti e dei rischi correlati all'uso dell'IA e delle sfide etiche e legali legate all'applicazione del DIU e del Diritto nazionale e internazionale penale.

<sup>60</sup> Perseguibile attraverso il ricorso ad applicazioni di IA in grado di modellare i contenuti e il ritmo di studio in base alle capacità di ogni singolo discente.



### 3.3.1. FORMAZIONE ALL'IA

Per conseguire tutti gli obiettivi, è necessario prevedere che il personale del Dicastero prenda parte a momenti formativi periodici che permettano di accrescere la c.d. alfabetizzazione all'IA<sup>61</sup>, che deve essere strutturata nel tempo, diffusa<sup>62</sup> e attagliata ai bisogni dell'utenza, in un *framework* che consenta di:

- comprendere i concetti fondamentali dell'IA (**dimensione cognitiva**);
- utilizzare le tecnologie IA in modo efficace (**dimensione operativa**);
- valutare in modo critico gli output (**dimensione critica**);
- comprendere le norme e le questioni etiche<sup>63</sup> (**dimensione etico-normativa**).

Sarà necessario, inoltre, far acquisire un set di *soft skills* che permetta di sviluppare il *mindset* digitale necessario ad operare in ambienti di lavoro misti (uomo-macchina) e multidisciplinari, altamente tecnologici e in continua evoluzione. La definizione delle figure professionali d'interesse e il quadro di conoscenze, abilità e competenze da perseguire sarà indispensabile per poter progettare nuovi percorsi formativi o adeguare quelli già in atto. **Relativamente ai leader, dovranno essere preparati ad assumere decisioni complesse in scenari ibridi dove l'essere umano rimane l'attore centrale in un ecosistema sempre più automatizzato, garantendo l'uso efficace, efficiente e responsabile dell'IA<sup>64</sup>.**

In ultimo, occorre definire un *framework* che garantisca la continuità dei contenuti erogati nelle diverse fasi formative<sup>65</sup> che consenta di attrarre, formare e trattenere talenti e perseguire l'autonomia strategico-operativa della Difesa.

### 3.3.2. FORMAZIONE CON L'IA

L'impiego dell'IA da parte degli studenti di ogni ordine e grado è ormai una realtà consolidata nonostante i rischi correlati all'uso della IA generativa<sup>66</sup>.

L'IA offre d'altra parte anche l'opportunità di introdurre modelli di insegnamento che vanno decisamente nella direzione opposta, rendendo sostenibile la personalizzazione del processo formativo alle esigenze di ogni singolo studente. I momenti formativi sull'IA dovranno quindi insegnare a docenti e discenti come impiegare al meglio l'IA in relazione al proprio ruolo e a supporto alla formazione/auto-formazione, acquisendo competenze specifiche e sul corretto uso di questi nuovi assistenti allo studio ovvero alla ricerca e produzione ed erogazione dei contenuti. L'impiego attivo dell'IA generativa, inoltre, ha accelerato l'obsolescenza di molti metodi di verifica, rendendo necessaria l'integrazione di attività atte a dimostrare la reale padronanza degli strumenti cognitivi appresi.

61 *AI Literacy*.

62 Significando che, nel rispetto dei minimi requisiti di standardizzazione, l'erogazione dei corsi in esame potrà essere periferizzata sul territorio compatibilmente con le esigenze delle FF.AA.

63 Con particolare riferimento a trasparenza e spiegabilità, equità, responsabilità, sicurezza e *privacy*.

64 **Evitando di riporre scarsa fiducia negli strumenti a causa della non spiegabilità dei sistemi IA (*black box*) o di affidarsi in modo eccessivo e acritico (*automation bias*), incorrendo in un'errata percezione della responsabilità e, peggio, nella perdita di competenze (*skill atrophy*) e di pensiero critico o nella dipendenza dall'IA.**

65 Iniziale, intermedia e avanzata. L'offerta formativa dovrà tener conto dell'evoluzione del settore dell'IA, dei *feedback* dei frequentatori, delle esigenze formative conseguenti alla definizione dei profili professionali d'interesse per la Difesa e di eventuali nuovi bisogni provenienti dall'area operativa.

66 Vanno dalla diffusione di *bias* cognitivi e disinformazione a scenari più allarmanti di pigrizia cognitiva e perdita delle capacità di pensiero critico.



La nuova didattica richiede, pertanto, applicazioni di IA dedicate e costantemente aggiornate, un *data lake*<sup>67</sup> unico della "conoscenza militare" e il potenziamento della capacità di creare ed erogare contenuti aggiornati e sempre fruibili che consentano di rendere agili ed efficaci i processi di apprendimento durante tutta la carriera e i percorsi di *reskilling* e *upskilling* mediante sistemi evoluti che implementino un *recommender system*<sup>68</sup>.

**UNA DIFESA CHE CONSIDERA FORMAZIONE E ADDESTRAMENTO QUALI PILASTRI STRATEGICI PER VALORIZZARE IL CAPITALE UMANO, USANDO L'IA QUALE SUPPORTO DI UN MODELLO EVOLUTO ED EFFICACE**

### 3.3.3. IA E ADDESTRAMENTO

La Difesa dovrà progressivamente modificare la propria organizzazione per rispondere a crescenti esigenze di cooperazione umano-macchina. **Ai nuovi leader militari sarà richiesto di gestire una forza lavoro mista, dover assumere decisioni sempre più complesse, esaminare grandi volumi di informazioni, impiegare sistemi d'arma performanti e governare l'utilizzo di sistemi autonomi.**

È, quindi, necessario ampliare la gamma di attività addestrative che consentano di rafforzare la capacità di decidere e agire con un approccio sistemico, in quanto abilità non innate e addestrabili anche attraverso il ricorso alla simulazione. L'IA offre ottime opportunità per migliorare la qualità dei sistemi di **simulazione** e rendere più realistiche e coinvolgenti le attività addestrative.

In tale quadro, si ritiene necessario accrescere le possibilità di condurre esercitazioni multidominio e interagenzia, o con partner operanti in aree geografiche diversificate, utilizzando tecnologie di simulazione<sup>69</sup>, realtà virtuale, *gamification*<sup>70</sup> e *wargaming*. Inoltre, l'implementazione di sistemi di *augmented reality* e tecnologie immersive, per la creazione di ambienti realistici che permettano l'apprendimento esperienziale in situazioni complesse e dinamiche senza rischi fisici, eleverà la qualità dell'addestramento.

Questo permetterà di identificare aree di miglioramento e di incrementare le prestazioni in modo più rapido ed economico e di poter valutare l'efficacia delle procedure applicabili in uno specifico contesto attraverso *feedback* immediati.

67 Archivio digitale centralizzato per grandi volumi di dati nel loro formato nativo (i.e. senza doverli prima strutturare o trasformare) che permette di memorizzarli, gestirli e tracciare le modifiche effettuate, fungendo da deposito per progetti e collaborazioni.

68 Ossia suggeriscano i corsi da frequentare per acquisire le competenze necessarie per ricoprire un incarico e, viceversa, le persone più adatte a ricoprire una posizione organica sulla base delle competenze acquisite.

69 Individuando soluzioni che consentano di integrare/federare le piattaforme di simulazione disponibili e/o di prevederne una unica per l'intero comparto.

70 Questa metodologia sfrutta l'IA per applicare elementi e meccaniche tipiche dei giochi contesti formativi non ludici. L'obiettivo è rendere l'addestramento più coinvolgente e motivante, capitalizzando la naturale propensione umana al gioco per affinare le capacità cognitive, decisionali e di squadra.



### 3.3.4. IA E RICERCA

In un contesto altamente competitivo, congestionato e dinamico, occorre rendere possibile la virtuosa interazione di tutti gli *stakeholders* disponibili in ambito nazionale, al fine di generare valore di cui l'intero Sistema Paese possa beneficiare. Risulta, pertanto, determinante accrescere la qualità della ricerca di base e tecnologica nel settore per generare conoscenza e capacità proprietarie, ridurre la dipendenza tecnologica da attori esterni e ricercare nicchie di eccellenza in cui il Sistema Paese possa vantare una supremazia.

Nell'ambito della formazione, addestramento e ricerca, l'obiettivo è quello di sviluppare una cultura dell'IA, formare il personale e potenziare i sistemi addestrativi.



#### Ufficio per l'IA:

- definisce le politiche per rendere coerenti e sinergiche le iniziative di formazione e ricerca;
- seguendo un approccio trasparente, sicuro e responsabile, indirizza la definizione di *guardrail* etici che devono essere rispettati nella ricerca e sviluppo dei prodotti.



#### Laboratorio di IA per la Difesa (LIAD):

funge da polo di eccellenza ed orchestratore per:

- sviluppare la ricerca di base e tecnologica;
- aggregare competenze, generare conoscenza e capacità proprietarie per il trasferimento dei risultati della ricerca alla Difesa;
- sviluppare, in sinergia con il mondo accademico e industriale, un c.d. *Defence AI Skills Framework* al fine di attrarre, reclutare, formare e trattenere profili altamente specializzati (talenti), definendo al contempo nuove carriere specialistiche.



### 3.4. IA E INDUSTRIA

L'IA sta, di fatto, trasformando processi produttivi, modelli organizzativi e servizi, con aziende e istituzioni che ripensano attività e decisioni intorno a strumenti intelligenti. L'Italia può giocare un ruolo di primo piano non solo nel digitale civile, ma anche nella Difesa, trasformando l'IA in un fattore strategico per competitività, sicurezza e autonomia tecnologica. Il presente paragrafo si pone proprio l'obiettivo di individuare le principali direttrici strategiche attraverso cui potenziare **il ruolo di guida della Difesa** nel panorama IA nazionale non solo verso le grandi *corporate*, che rappresentano l'eccellenza, ma anche e soprattutto **verso spin off, start-up e PMI innovative** e ad alto potenziale tecnologico. Solo attraverso questo cambio di paradigma la Difesa potrà contribuire attivamente alla crescita dell'ecosistema "Defense Tech" e, di conseguenza, a potenziare il tessuto tecnologico del Sistema Paese.



Immagine generata con AI



### 3.4.1. LO SCOUTING TECNOLOGICO QUALE LEVA STRATEGICA

La capacità della Difesa di assumere un ruolo di guida nel settore dell'IA non può prescindere da una profonda e aggiornata conoscenza del panorama tecnologico nazionale e internazionale. È necessario, dunque, un approccio proattivo e strutturato di **scouting tecnologico**, che consenta di identificare e comprendere le tendenze emergenti e le innovazioni dirompenti.

La conoscenza, in questo contesto, non è un semplice *asset*, ma il vero e proprio punto di partenza per una strategia di innovazione efficace e mirata che superi le tradizionali logiche di *"technology push"* e *"demand pull"* in favore di un modello di collaborazione biunivoco e sinergico con l'industria.

Per conseguire l'obiettivo proposto occorre avviare una serie di azioni strutturate e, in particolare:

- **rivedere la governance IA in ambito Difesa**, al fine di individuare l'organismo o gli organismi che avranno il compito di mappare e aggiornare costantemente il panorama tecnologico nazionale, europeo e NATO;
- **incrementare le collaborazioni strategiche** con l'ecosistema dell'innovazione, sia potenziando i legami con università e centri di ricerca, sia creando sinergie strutturali con **incubatori, acceleratori e venture capital fund**, osservatori privilegiati attraverso cui avere una visione diretta sulle tecnologie di frontiera ed esercitare un'azione di indirizzo degli investimenti privati verso aree di interesse strategico, facendo leva sul **Laboratorio di Intelligenza Artificiale per la Difesa (LIAD)**;
- **espandere i "sensori" sul territorio nazionale** per interagire in modo proattivo con i distretti tecnologici, i parchi scientifici e le comunità di ricerca;
- sviluppare uno strumento digitale che funga da **"Osservatorio IA"** e contribuisca a creare una mappa dinamica e aggiornata del panorama tecnologico nazionale e internazionale, identificando tendenze emergenti, aree di ricerca promettenti e *player* rilevanti, fornendo così una solida base di conoscenza in base a cui orientare lo sviluppo tecnologico;
- **espandere le relazioni esterne attraverso eventi specifici** quali *"startup day"*, hackathon o *call* tecnologiche dedicate all'IA, mettendo così in contatto diretto i decisori della Difesa con gli altri soggetti dell'ecosistema nazionale dell'innovazione.

Tra i benefici dell'approccio appena citato si possono citare il **rafforzamento della domanda**, che si avvantaggerebbe di una più solida conoscenza delle soluzioni disponibili, l'**anticipazione** e l'**adattamento** derivante dalla precoce intercettazione delle tecnologie ancora in fase di sviluppo e il concreto **supporto a ulteriori iniziative nel campo dell'innovazione** ritenute di interesse.

**UNA DIFESA FARO DI INNOVAZIONE, PRONTA A GUIDARE LO SVILUPPO DI UN ECOSISTEMA DEFENSE TECH COMPETITIVO E A VALORIZZARE LE REALTÀ ALTAMENTE INNOVATIVE SUL TERRITORIO NAZIONALE**



### 3.4.2. L'INNOVAZIONE QUALE LEVA STRATEGICA PER AMPLIARE LA BASE INDUSTRIALE DI RIFERIMENTO

La Difesa, per rimanere all'avanguardia in un contesto tecnologico in rapida evoluzione, deve prendere una serie di azioni proattive che stimolino l'espansione della base industriale di riferimento, in modo da affiancare ai grandi *player* industriali tradizionali nuove realtà, come *start-up* e *spin-off* accademici, che sono spesso i veri motori dell'innovazione dirompente. Per raggiungere questo obiettivo, la Difesa deve agire come un **catalizzatore**, implementando azioni concrete volte a ridurre le barriere burocratiche e a creare un ecosistema di fiducia e collaborazione, con benefici per l'intero sistema Paese.



Immagine generata con AI



Al riguardo, occorrerà:

- **potenziare la comunicazione e incrementare la visibilità di bisogni, sfide tecnologiche e opportunità presenti nella Difesa.** Il primo passo per attrarre l'innovazione, in sostanza, è far sapere all'ecosistema di riferimento che la Difesa è un partner potenziale e interessato a nuove soluzioni. La creazione di una **piattaforma dedicata**, facilmente accessibile a tutti e che illustri aree di interesse e opportunità<sup>71</sup> è un'azione cruciale;
- **incrementare gli strumenti di intercettazione delle soluzioni di interesse**, in modo che strumenti *solicited*<sup>72</sup>, più agili e mirati, diventino in modo predominante il ponte diretto e agile tra le esigenze operative della Difesa e le capacità tecnologiche del settore privato, come fatto con successo nel Polo Nazionale della dimensione Subacquea (PNS);
- **sfruttare strutture e metodologie più agili** per l'avvio di progetti pilota e sperimentazioni. LIAD assumerà il ruolo chiave di *AI Delivery Center*, supportato dalle strutture già esistenti quali i Centri di sperimentazione delle FF.AA.;
- **sostenere l'innovazione attraverso opportuni finanziamenti** mirati e utilizzando strumenti innovativi di supporto a *start-up* e PMI a basso carico burocratico-amministrativo<sup>73</sup>, promuovendo un approccio al *procurement* basato sul concetto di *good enough*, che privilegi il tasso di innovatività della proposta rispetto a un'eccessiva, tardiva e dispendiosa ricerca della perfezione;
- **dotarsi di incubatori e acceleratori** attraverso cooperazioni con partner strategici che possano supportare l'innovazione nell'ambito di una *governance* ben definita.

I benefici attesi dall'approccio appena citato sono molteplici e spaziano dal significativo ampliamento del ventaglio di soluzioni tecnologiche disponibili, al rafforzamento dell'intero ecosistema tecnologico nazionale, alla riduzione di tempi, costi e rischi.

## UNA DIFESA IN GRADO DI INDIRIZZARE LE SCELTE STRATEGICHE DELL'INDUSTRIA E DI PARTECIPARE ATTIVAMENTE ALLO SVILUPPO DI SOLUZIONI INNOVATIVE

71 Nazionali e internazionali. Si tratta, ad esempio, di bandi finanziati attraverso l'*European Defence Fund* (EDF), iniziative nell'ambito dell'*Hub for European Defense Innovation* (HEDI) o quelle in seno al *NATO Defense Innovation Accelerator for North Atlantic* (DIANA).

72 Quali, ad esempio, *Challenge* tecnologiche, *Hackathon* o *Call for innovation/solutions*.

73 Tali strumenti risultano avere una cubatura finanziaria non rilevante per gli stanziamenti totali dello Stato ma di assoluto valore per le *start-up* e PMI.



### 3.4.3. POTENZIAMENTO DEL RUOLO ATTIVO DELLA DIFESA NELLE RELAZIONI CON L'INDUSTRIA

Per completare la transizione da cliente a partner strategico, la Difesa deve assumere un ruolo proattivo e di *leadership*, diventando un vero e proprio catalizzatore di innovazione per l'intero ecosistema tecnologico nazionale con la capacità di influenzare, indirizzare e co-creare il futuro tecnologico. L'obiettivo è, dunque, stabilire una relazione profonda e continua con l'industria, in cui le esigenze operative della Difesa non solo informino il mercato, ma ne guidino lo sviluppo in modo mirato.

Per conseguire l'effetto trasformativo descritto occorrerà che la Difesa agisca sulle leve strategiche di politica industriale più tradizionali e ne individui di innovative dando concretezza alle seguenti azioni:

- **definire requisiti** allo stato dell'arte che consentano aggiornamenti senza limitazioni di alcun tipo. In tal senso, un'adozione più ampia del c.d. **Modular Open System Approach (MOSA)**<sup>74</sup> è una delle azioni fondamentali, in quanto obbliga i contraenti a progettare sistemi le cui componenti siano interoperabili, sostituibili e aggiornabili con *hardware/software* prodotti da fornitori diversi. Ciò stimola la competizione e riduce il rischio di "*vendor lock in*";
- **definire standard tecnologici e criteri di certificazione chiari**, al fine di perseguire i requisiti di sicurezza e qualità auspicati e favorire lo sviluppo di soluzioni che possano trovare sbocchi anche nei mercati internazionali;
- **promuovere co-sviluppo, co-investimento e partnership strategiche** partecipando attivamente alla ricerca e sviluppo e incrementando il dialogo con l'industria;
- **sviluppare una *technology roadmap* strategica condivisa a lungo termine**<sup>75</sup> con l'industria e la comunità scientifica che permetta di allineare i rispettivi piani strategici di sviluppo riducendo l'incertezza in ottica di lungo periodo;
- **valorizzare le competenze interne e dell'industria** istituendo meccanismi di consulenza e scambio che favoriscano un flusso continuo di conoscenze.

L'approccio appena descritto è in grado di generare numerosi benefici quali la maggior **sostenibilità del vantaggio tecnologico** nel lungo periodo, il **rafforzamento della base industriale nazionale "Defense Tech"** e un miglior **allineamento delle *roadmap* di sviluppo** aziendale con le reali esigenze della e la **riduzione di tempi e costi** per l'implementazione delle soluzioni ricercate.

74 Architettura aperta e modulare.

75 *Roadmap* che riguarda i 3 anni conseguenti al rilascio della presente strategia, in coerenza con quanto asserito in precedenza.



L'area industriale mira a valorizzare l'ecosistema nazionale (incluse PMI e start-up), promuovendo *partnership* sinergiche e la sovranità tecnologica.



**Ufficio per l'IA:**

esercita un'azione di indirizzo strategico e gestisce i fondi del Dicastero per l'IA per sostenere l'attuazione della Strategia e il consolidamento di capacità sovrane.



**Laboratorio di IA per la Difesa (LIAD):**

quale *AI Delivery Center*, funge da perno per:

- implementare uno *scouting* tecnologico proattivo, strutturato ed efficiente verso le esigenze della Difesa;
- promuovere e realizzare *partnership* sinergiche con l'accademia e l'industria (incluse PMI e *start-up*) con l'obiettivo di costruire un ecosistema "*Defense Tech*" sovrano e competitivo, riducendo la dipendenza tecnologica e rafforzare l'ecosistema.

In tale frangente, stimolerà l'innovazione tecnologica nazionale semplificando l'accesso agli *asset* della Difesa (dati, capacità di calcolo).





Immagine generata con AI







# 04

In tale organizzazione dovranno essere collocate nuove entità altamente specialistiche che garantiscano il soddisfacimento dei fabbisogni della Difesa.

## FABBISOGNI E DIRETTRICI DI INTERVENTO

Da quanto precede discende in modo naturale che, ai fini dell'integrazione dell'IA all'interno del Comparto Difesa e per raggiungere i risultati ambiti, è fondamentale:

- sottoporre l'attuale organizzazione interna a una revisione organica e funzionale;
- allocare adeguate risorse (finanziarie, umane, tecnologiche e infrastrutturali) e renderle disponibili con continuità per l'attuazione dei suddetti punti;
- individuare le principali Direttrici Strategiche (DS) di intervento.

### 4.1. REVISIONE ORGANICA E FUNZIONALE

Nel quadro delineato, è essenziale disporre di una struttura di *governance* dedicata che, articolata su più livelli gerarchici, ciascuno con compiti e responsabilità specifiche ma strettamente interconnesse tra loro, sia capace di assolvere e assicurare:

- unicità di indirizzo politico e militare, in coerenza con le iniziative strategiche e le normative nazionali e internazionali;
- la gestione, il coordinamento tra i livelli istituzionali del Dicastero e verso gli organi interministeriali e internazionali, e l'esecuzione delle attività inerenti all'IA;
- la ricerca e sviluppo volta alla sovranità tecnologica di settore;
- l'adozione e l'impiego dell'IA in modo responsabile ed etico.

In tale organizzazione dovranno essere collocate nuove entità altamente specialistiche che garantiscano il soddisfacimento dei fabbisogni della Difesa, in particolare quelli con ricadute pratiche e operative, ricercando un'evoluzione migliorativa complessiva.

La visione descritta è meglio definita di seguito.



#### 4.1.1. LIVELLO POLITICO-STRATEGICO

È il livello che definisce l'indirizzo generale, le risorse e l'allineamento con gli orientamenti nazionali e internazionali. Qui, un **ufficio preposto alla coordinazione delle iniziative in ambito Intelligenza Artificiale** (c.d. **"Ufficio per l'IA" - UIA**) opererà quale organo di alto profilo dedicato all'indirizzo, alla supervisione e al monitoraggio delle tematiche connesse all'IA, garantendo un coordinamento unitario e autorevole. Esso promuoverà e sosterrà le iniziative strategiche coerenti con le esigenze del Dicastero, assicurando un presidio costante e qualificato delle attività e l'impiego efficiente dei fondi dedicati. Si occuperà, inoltre, delle relazioni interministeriali e internazionali per modellare gli sviluppi globali in linea con i valori democratici, promuovendo trasparenza, sicurezza ed uso etico e responsabile dell'IA.

Tale Ufficio coordinerà il **"Laboratorio di Intelligenza Artificiale per la Difesa" (LIAD)**<sup>76</sup> a cui verranno assegnate le funzioni di creare, trasformare, sperimentare e rendere operative, in sinergie con gli utilizzatori ultimi, le soluzioni di IA.

Con tale ambizione e in sinergia con le altre misure definite nel presente documento, il **LIAD**, lavorando ed interagendo in maniera verticale lungo tutti i livelli della Difesa, fungerà da polo di eccellenza, aggregatore di idee, interessi ed innovazione tecnologica nonché da vero e proprio **"AI Delivery Center"** della Difesa, con il compito di:

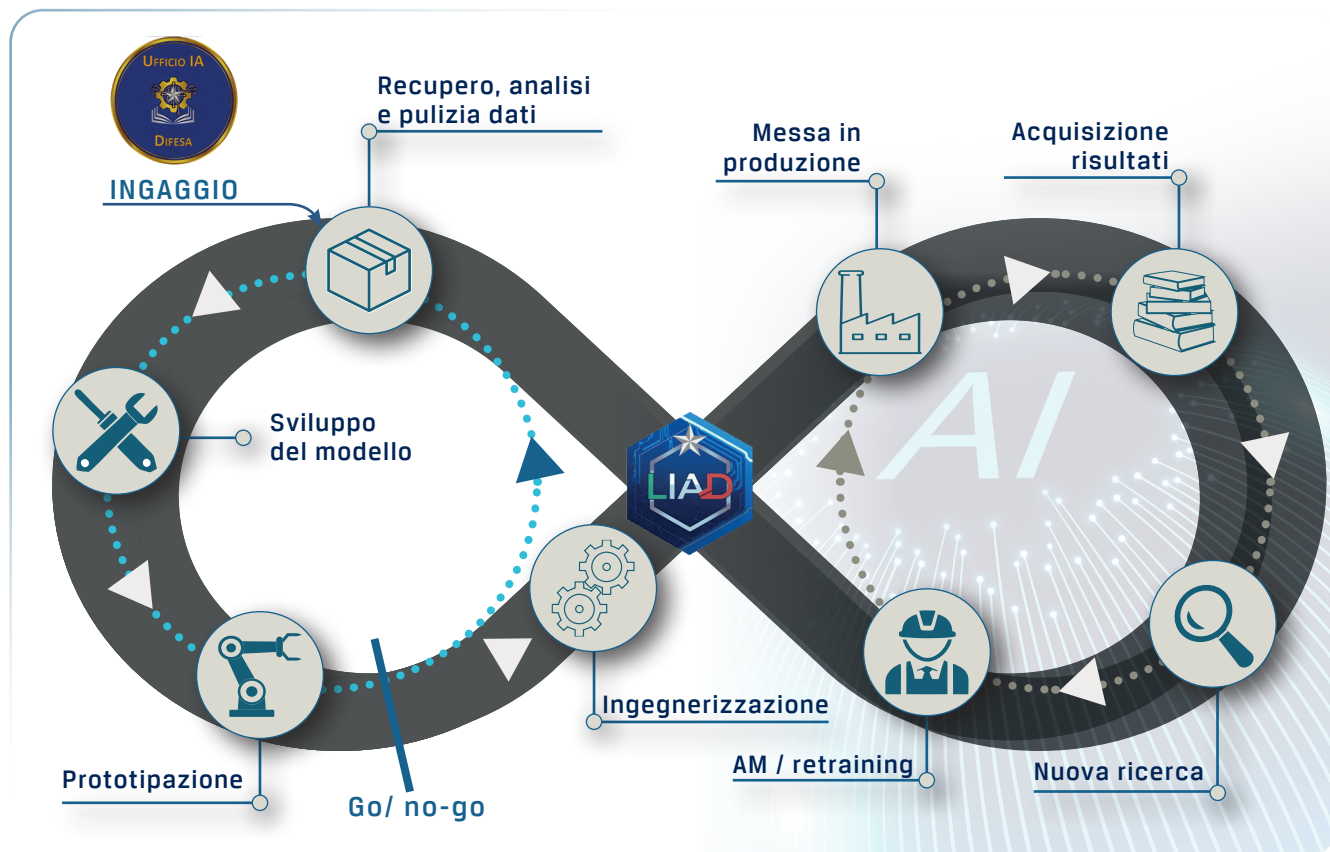
- ampliare e consolidare il patrimonio di conoscenze in materia di IA, trasferire competenze e i risultati della ricerca alla Difesa e accrescere le possibilità di accesso a fonti di finanziamento nazionali e internazionali;
- irrobustire la Difesa dal punto di vista scientifico nel panorama universitario nazionale e internazionale della ricerca nell'ambito dell'IA, attrarre, reclutare, formare e trattenere talenti;
- sviluppare l'attività di ricerca lungo le direttrici indicate dal Dicastero, con l'obiettivo di aggregare idee e iniziative rivolte allo sviluppo e realizzazione di soluzioni basate sull'IA nella Difesa;
- stimolare e sviluppare l' "ecosistema IA della Difesa" grazie alla collaborazione col mondo accademico, centri di ricerca e imprese di ogni dimensione;
- costituire una "officina" dove, con il suddetto ecosistema e sulla base delle necessità e dei requisiti della Difesa, poter realizzare soluzioni tecnologiche all'avanguardia, pienamente funzionali e rispondenti ai requisiti di sicurezza, qualità e affidabilità.

Tutto ciò, basandosi su un modello operativo *agile* e a "doppia elica"<sup>77</sup> (figura 5), rappresenta le fondamenta per creare uno sviluppo tecnologico sovrano, inclusivo e sostenibile, in linea con le priorità della Difesa e quelle nazionali, a beneficio dell'intero Sistema-Paese.

.....  
<sup>76</sup> Già citato nei precedenti capitoli.

<sup>77</sup> Modello, in linea con quello assunto da USA, Regno Unito e Francia, fondato sulla rapida ed agile interazione tra le fasi di sviluppo e *testing*.





**Figura 5** – Modello operativo agile e a "doppia elica".



#### 4.1.2 LIVELLO STRATEGICO-MILITARE

##### 4.1.2.1. **Area tecnico-operativa interforze**

In coerenza con le analoghe funzioni riferite ad altri domini/settori/ambiti, l'Area Tecnico-Operativa definisce la *policy* e garantisce la gestione e il coordinamento dei programmi, orientando le risorse verso progetti capaci di rispondere alle priorità nazionali e alle evoluzioni del contesto internazionale. Assicura la gestione in ambito formativo e addestrativo e l'integrazione dottrinale e operativa delle capacità abilitate dall'IA, attraverso le soluzioni fornite dal **LIAD**, in tutti i domini e ambienti operativi e settori che costituiscono la sfera militare.

##### 4.1.2.2. **Area tecnico-amministrativa interforze**

In linea con i definiti indirizzi strategici e di *policy*, l'area Tecnico-Amministrativa ha il ruolo di coordinare e allineare le iniziative relative alla "Ricerca e Sviluppo" e per la "Politica industriale". Assicurerà il raccordo tra le iniziative del **LIAD** e quelle intraprese in altri ambiti, favorendo sinergie e processi di collaborazione tra enti di ricerca, industria nazionale ed estera, nonché con le F.A., e collaborerà con il **LIAD** nelle fasi legate al *procurement*, assicurando il rispetto degli standard di sicurezza e qualità.

Per entrambe le suddette aree, le singole F.A. assolvono compiti di impulso e orientamento – anche in ragione delle specifiche esigenze capacitive – fungendo da anello di congiunzione tra la domanda operativa e l'offerta tecnologica attraverso le interazioni con i corrispettivi livelli. Tale ruolo è fondamentale per assicurare che lo sviluppo delle capacità IA risponda concretamente alle priorità di sviluppo capacitivo, di integrazione e di impiego multi-dominio.

#### 4.1.3. LIVELLO OPERATIVO E TATTICO INTERFORZE

A questo livello, le articolazioni avranno il compito:

- di generare e riversare al **LIAD** i requisiti operativi degli strumenti di IA necessari ad allineare le capacità militari con le esigenze imposte dagli attuali scenari geopolitici e dai relativi "*battlefield*";
- di sperimentare ed impiegare sul campo gli strumenti sviluppati, fornendo riscontro al **LIAD** per eventuali azioni correttive e migliorative;
- in collaborazione e in coordinamento con i Centri di sperimentazione, interforze e delle singole F.A., di verificare, validare e certificare i sistemi a garanzia di affidabilità in tutto il ciclo di vita.

#### 4.1.4. AREA GIURIDICA

In tale area ricadono tutte le funzioni relative a:

- predisposizione di emendamenti/nuove proposte di legge concernenti l'ambito militare;
- la diffusione di informazioni che consentano l'allineamento con le normative nazionali e internazionali<sup>78</sup>;
- l'adozione e l'impiego dell'IA in modo responsabile ed etico, grazie ad un'interazione con l'**UIA** per definire i c.d. *guardrail* etici che il **LIAD** dovrà tenere in considerazione durante il proprio operato riversandoli praticamente nei prodotti e servizi sviluppati e distribuiti.

78 In particolare per il rispetto della legislazione sulla protezione dei dati personali (i.e. Regolamento Generale sulla Protezione dei Dati – GDPR).



In tale ambito, quale funzione di supporto trasversale, sarà necessaria la costituzione di un organo consultivo interno, composto da esperti - militari e civili - di etica, di diritti fondamentali e del DIU col compito di promuovere l'uso responsabile dell'IA in ambito militare e contribuire attivamente presso i tavoli internazionali<sup>79</sup> a costruire una visione comune sull'uso militare responsabile dell'IA, allineata ai valori democratici.

La *governance* multilivello e *multi-stakeholder* così delineata intende rappresentare l'imprescindibile schema iniziale di riferimento per l'implementazione della Strategia IA della Difesa.

Pensata come un *living document*, tale strategia sarà oggetto di monitoraggio costante e di valutazioni periodiche per adeguarsi in modo tempestivo ed efficace alle esigenze emergenti, agli scenari tecnologici in continua evoluzione e alle nuove sfide che si presenteranno nel futuro.

## UNA DIFESA STRUTTURATA PER GOVERNARE EFFICACEMENTE L'EVOLUZIONE IA, IN MODO RESPONSABILE, ETICO E IN LINEA CON LE PRIORITARIE ESIGENZE DEL SISTEMA-PAESE

### 4.2. RISORSE

Sarà necessario disporre di strumenti economici sufficienti e stabilmente dedicati quale requisito imprescindibile per garantire la credibilità e l'efficacia delle azioni da intraprendere e per promuovere una reale capacità di sviluppo, sperimentazione e integrazione delle soluzioni di IA. Infatti, solo un consistente e mirato impegno in termini di risorse permette di supportare concretamente le esigenze formative, di costruzione delle infrastrutture tecnologiche, di ricerca e di innovazione e di accompagnare nel tempo il processo, fondamentale a sostenere l'autonomia strategica della Difesa e la competitività del Sistema Paese.

In questo contesto, sarà effettuata un'attenta valutazione sulla congruità delle **linee di finanziamento attualmente disponibili** al fine di verificare il loro grado di contributo al raggiungimento degli obiettivi definiti. Particolare attenzione sarà posta ai finanziamenti destinati alla **formazione** e alla **digitalizzazione**, che costituiscono i pilastri fondamentali per la crescita del capitale umano e delle infrastrutture dedicate all'IA.

Parimenti rilevanti risultano le risorse dedicate alla **ricerca scientifica e tecnologica**, inclusi gli stanziamenti previsti da uno strumento chiave quale il **Piano Nazionale della Ricerca Militare (PNRM)** e quelle assentite con la **Legge di Bilancio 2021<sup>80</sup>**, attraverso cui sono già finanziate iniziative e progetti riconducibili all'ambito delle tecnologie emergenti, tra cui quelle relative all'IA.

Parallelamente, si rende necessario istituire un **dedicato "Fondo per l'IA"**, con una adeguata dotazione iniziale e una gestione a cura della costituenda articolazione a livello strategico-politico. Tale Fondo sarà funzionale a sostenere

<sup>79</sup> ONU, NATO, UE, ecc.

<sup>80</sup> Fondo Composito Difesa 2021.



l'attuazione della presente Strategia, le numerose iniziative, sia promosse con approccio *top-down* sia originate *bottom-up*, e a promuovere il potenziamento dell'ecosistema IA del Paese e il consolidamento di capacità sovrane, assicurando un utilizzo coerente ed efficiente delle risorse finanziarie. In attesa dell'istituzione del predetto fondo finanziario, le esigenze potranno essere soddisfatte impiegando altresì le risorse affluite con il **"Fondo per l'attuazione dei programmi di investimento pluriennale per le esigenze di difesa nazionale"** ovvero con altro strumento finanziario idoneo allo scopo anche a valere sul bilancio di altri Dicasteri.

Il Fondo per l'IA, unitamente a tutte le altre linee di finanziamento, sarà oggetto di costanti rivalutazioni e adeguamenti periodici in fase di condotta poiché, in assenza di un adeguato sostegno finanziario, la Strategia rischierebbe di non poter dispiegare pienamente il proprio potenziale o, addirittura, di disattendere il raggiungimento dei risultati prefissati.

**UNA DIFESA PRONTA A INVESTIRE IN MODO STABILE E MIRATO NELL'IA,  
SOSTENENDO IN MODO EFFICACE LA TRASFORMAZIONE DEL COMPARTO E  
L'INNOVAZIONE TECNOLOGICA**

#### 4.3. DIRETTRICI STRATEGICHE DI INTERVENTO

A corollario del quadro definito nel presente documento, sono di seguito delineate 15 DS, suddivise in 5 gruppi, che definiscono i principali ambiti di intervento verso i quali si intende orientare l'adozione e l'integrazione dell'IA nei processi, nelle capacità e nelle operazioni militari per il raggiungimento dei relativi obiettivi strategici. Esse rappresentano l'anello di congiunzione tra la visione strategica e quella che sarà l'attuazione concreta che soddisfa i fabbisogni finora descritti, costituendo un quadro di riferimento per la pianificazione, il coordinamento e la valutazione delle iniziative.

| GRUPPO                              | DENOMINAZIONE DS                                                                     | OBIETTIVO STRATEGICO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Governance<br/>e<br/>risorse</b> | <b>DS-1</b> Revisione della <i>governance</i> IA della Difesa e sostegno finanziario | Disporre di una <i>governance</i> IA chiara e solida che:<br>a) attraverso un Ufficio Centrale per l'IA, assicuri un coordinamento efficace tra i diversi livelli istituzionali, garantisca la coerenza delle iniziative ed un uso efficiente delle risorse nonché il rigoroso rispetto dei principi etici e normativi;<br>b) attraverso il Laboratorio di Intelligenza Artificiale per la Difesa presidi la creazione, trasformazione, sperimentazione e operatività delle soluzioni IA per la Difesa, agendo come "AI Delivery Center" dedicato. |



| GRUPPO                        | DENOMINAZIONE DS                                           | OBIETTIVO STRATEGICO                                                                                                                                                                                                                                                                                   |
|-------------------------------|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fattori strategici abilitanti | <b>DS-2</b> Risorse umane quali capacità abilitanti        | Disporre delle risorse umane necessarie per operare autonomamente in ambito IA, costruendo, attirando e trattenendo i talenti necessari per perseguire una superiorità tecnologica sostenibile.                                                                                                        |
|                               | <b>DS-3</b> Infrastrutture digitali                        | Garantire le fondamenta tecnologiche per l'adozione diffusa e sicura dell'IA, assicurando capacità di calcolo ad alte prestazioni (HPC), infrastrutture <i>cloud/edge</i> sovrane, reti sicure e resilienti, nonché una gestione unitaria, sicura e interoperabile dei dati come risorsa strategica.   |
| L'IA nei contesti operativi   | <b>DS-4</b> Superiorità decisionale e velocità di ingaggio | Assicurare processi di pianificazione e decisionali più rapidi, accurati e coordinati rispetto ai <i>competitor</i> , grazie all'integrazione di sensori, piattaforme C5ISR, capacità di <i>targeting AI-enabled</i> e riduzione del ciclo <i>sensor-to-shooter</i> in chiave cinetica e non cinetica. |
|                               | <b>DS-5</b> Sistemi autonomi e cooperativi                 | Sviluppare e impiegare sistemi autonomi e semi-autonomi in cui l'IA potenzi percezione, navigazione, coordinamento e capacità decisionale, mantenendo il controllo umano coerentemente agli <i>standard</i> etici e normativi nazionali e internazionali.                                              |
|                               | <b>DS-6</b> Protezione multi-dominio                       | Impiegare l'IA per prevenire, rilevare e neutralizzare minacce cibernetiche, nello spettro elettromagnetico e fisiche, incluse capacità anti-drone/sciame, garantendo protezione e continuità operativa in tutti i domini e nell'ambiente informativo.                                                 |
|                               | <b>DS-7</b> Sostenibilità operativa e logistica            | Applicare l'IA per ottimizzare logistica e manutenzione, in chiave interforze, garantendo disponibilità, prontezza e resilienza delle infrastrutture e dei sistemi IA stessi, in un'ottica di ciclo di vita completo.                                                                                  |



| GRUPPO                                           | DENOMINAZIONE DS                                                                     | OBIETTIVO STRATEGICO                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L'IA nei<br>contesti<br>organizzativi            | <b>DS-8</b> IA a supporto della produttività individuale                             | Potenziare l'adozione di strumenti di IA per migliorare la produttività individuale, snellire i flussi di lavoro di staff e liberare risorse per compiti ad alto valore aggiunto.                                                                                                                                                          |
|                                                  | <b>DS-9</b> IA a supporto dell'utenza                                                | Trasformare l'interazione del personale e degli utenti esterni con l'organizzazione attraverso un'assistenza più accurata, continua e personalizzata, rendendo i servizi di supporto più accessibili ed efficienti.                                                                                                                        |
|                                                  | <b>DS-10</b> IA a supporto dei processi strutturati                                  | Potenziare l'adozione dell'IA a supporto dei processi di lavoro della Difesa, garantendo efficienza, efficacia e migliorando l'interoperabilità tra tutte le componenti del Dicastero.                                                                                                                                                     |
| IA,<br>formazione,<br>addestramento<br>e ricerca | <b>DS-11</b> Sviluppo di una cultura dell'IA e formazione del personale della Difesa | Colmare il divario di conoscenza sull'IA, promuovere un uso etico e responsabile della tecnologia, sviluppando un <i>mindset</i> digitale in tutto il personale e creare una forza lavoro specializzata.                                                                                                                                   |
|                                                  | <b>DS-12</b> Potenziamento del Sistema Formativo tramite l'IA                        | Utilizzare l'IA come strumento per modernizzare e personalizzare i processi di insegnamento, apprendimento e ricerca, rendendoli più agili ed efficaci.                                                                                                                                                                                    |
|                                                  | <b>DS-13</b> Utilizzo dell'IA nell'addestramento                                     | Ampliare le capacità addestrative per migliorare i processi decisionali e operare in scenari complessi e ambienti ad alto rischio, anche ricorrendo alla cooperazione umano-macchina.                                                                                                                                                      |
| IA<br>e<br>industria                             | <b>DS-14</b> Potenziamento dell'ecosistema di innovazione della Difesa               | Espandere le capacità di <i>scouting</i> tecnologico al fine di intercettare con tempestività soluzioni di interesse, potenziare la comunicazione verso l'esterno e sfruttare l'innovazione quale leva strategica per favorire l'espansione della base industriale di riferimento e potenziare l'ecosistema <i>Defense Tech</i> del Paese. |
|                                                  | <b>DS-15</b> Ruolo attivo verso il comparto industriale                              | Assumere un ruolo di guida verso il comparto industriale di riferimento attraverso la definizione di standard e la condivisione di esigenze, ricercando la condivisione di expertise e un maggior allineamento delle rispettive <i>roadmap</i> di lungo termine.                                                                           |



Ai fini dell'implementazione concreta della presente Strategia, entro 3 mesi dall'approvazione del presente documento, sarà diramato un **Piano attuativo** contenente, per ciascuna delle DS, le azioni chiave, ritenute necessarie (c.d. "**misure attuative**") in ordine di **priorità**, le **responsabilità** di attuazione e gli **indicatori** (c.d. *Key Performance Indicator* - KPI) utili a monitorare lo stato di avanzamento rispetto agli obiettivi stabiliti. Tale piano attuativo sarà validato e supervisionato da un **Comitato Ordinatore** che verrà nominato dall'A.P., sentito il Capo di Stato Maggiore della difesa, contestualmente alla pubblicazione della presente Strategia.







## 04

L'adozione  
dell'IA è un  
imperativo  
strategico  
e politico  
imprescindibile  
con l'obiettivo  
di dotare il  
Ministero  
della Difesa  
di sistemi  
all'avanguardia,  
sicuri e  
resilienti per  
assicurare  
la difesa  
nazionale

# CONCLUSIONI

L'adozione dell'Intelligenza Artificiale non è più una scelta tecnologica, ma un **imperativo strategico e politico imprescindibile** per il futuro della difesa nazionale e per affrontare con efficacia le crescenti sfide geopolitiche.

La presente strategia si configura quindi come un **quadro organico e ambizioso** che definisce un percorso da adottare immediatamente e da portare a compimento in un arco temporale contenuto per l'integrazione sistemica e sistematica dell'IA nella Difesa.

Per fare questo, tale strategia, che dovrà necessariamente essere adattata alla continua evoluzione tecnologica e al contesto geopolitico, definisce un percorso modulare con **obiettivi a breve, medio e lungo termine (entro 1, 2 e 3 anni rispettivamente)**, focalizzandosi su quattro aree principali: **operazioni, contesti organizzativi, formazione e industria**.

Il documento sottolinea l'importanza di **risorse umane** specializzate e di **infrastrutture tecnologiche abilitanti** (dati, algoritmi e capacità di calcolo proprietarie), identificando **15 direttrici strategiche** per guidare gli interventi previsti.

Va sottolineato come la strategia riconosce il ruolo centrale del fattore umano, impegnandosi per un uso **etico e responsabile** della tecnologia, sempre in linea con i principi del Diritto Internazionale Umanitario. Inoltre, attraverso il potenziamento di infrastrutture critiche e la creazione di nuovi elementi di organizzazione, come l'**Ufficio per l'IA** e il **Laboratorio di Intelligenza Artificiale per la Difesa**, la Difesa intende fungere da **catalizzatore di innovazione** a vantaggio dell'intero ecosistema industriale e tecnologico nazionale e, in ultima istanza, del Sistema Paese.

Il cuore politico di questa visione risiede nell'obiettivo irrinunciabile di **conseguire l'autonomia strategica** e la **sovranità tecnologica**, riducendo le dipendenze critiche e garantendo alla Difesa e all'Italia una competitività sostenibile sul piano internazionale. Questo rafforzerà la nostra posizione come **partner credibile e proattivo** all'interno delle alleanze a cui l'Italia aderisce, come NATO e Unione Europea, e a livello globale.

Quale strumento ambizioso e pragmatico, questa strategia vuole rappresentare il **mandato decisivo** per dotare il Ministero della Difesa nel suo complesso di sistemi all'avanguardia, sicuri e resilienti, assicurando la difesa nazionale e contribuendo in modo determinante alla stabilità internazionale in un contesto di rapidi mutamenti e crescenti minacce.

**IL MINISTRO DELLA DIFESA**

On. Guido Crosetto







MINISTERO DELLA DIFESA

