



Intelligenza artificiale e Difesa italiana: sfide e opportunità

ANDREA GRILLO, ALESSANDRO MARRONE E MICHELE NONES

L'intelligenza artificiale (IA) è sempre più pervasiva anche nel mondo della difesa, presentando opportunità in termini di efficacia ed efficienza ma anche sfide quanto a sicurezza e controllo politico-militare. Da un lato, strumento per rafforzare deterrenza e difesa, trovando le principali aree di applicazione nel potenziamento delle capacità di Isr, nell'accelerazione ed efficacia dei sistemi di comando e controllo, nonché nel miglioramento della logistica e dell'addestramento. Dall'altro lato, l'IA è un potente strumento anche nelle mani degli avversari, con un effetto moltiplicatore che va dall'impiego dei sistemi autonomi alle campagne di manipolazione dell'informazione su larga scala. In prospettiva, essa costituisce inoltre una tecnologia fondamentale per la transizione verso sistemi automatizzati e progressivamente più autonomi, con implicazioni operative, organizzative ed etiche di ampia portata. Tale trasformazione complessiva impone, dunque, una riflessione più ampia sul livello di ambizione nazionale rispetto allo sviluppo, all'acquisizione e all'integrazione delle capacità di IA, nonché sul significato di sovranità tecnologica. L'adozione dell'IA nella Difesa italiana non rappresenta soltanto l'introduzione di una nuova tecnologia, ma una trasformazione strutturale del modo in cui le Forze armate osservano il contesto operativo, prendono decisioni e conducono le operazioni.

Executive summary	p. 2
1. Introduzione: l'approccio Nato all'IA	4
2. IA ed equipaggiamenti militari	7
3. IA e comando e controllo	11
4. IA e difesa cyber	15
5. IA e gestione delle risorse umane	17
6. La strategia della Difesa in materia di IA	19
Conclusioni	22
Acronimi	26

Andrea Grillo è ricercatore nel programma "Difesa, sicurezza e spazio" dell'Istituto Affari Internazionali (IAI). **Alessandro Marrone** è responsabile del programma "Difesa, sicurezza e spazio" dello IAI. **Michele Nones** è vicepresidente vicario dello IAI. Un ringraziamento a Silvia Maragno e Christian Labriola, tirocinanti nel programma "Difesa, sicurezza e spazio" per il prezioso supporto nella realizzazione dello studio.

Questo studio è stato preparato per il seminario a porte chiuse "Artificial intelligence e difesa italiana. Quo vadis?" organizzato dallo IAI a Roma il 23 giugno 2026 con il supporto di Accenture, ed è stato rivisto alla luce del dibattito ivi svoltosi.



Executive summary

L'intelligenza artificiale (IA) è divenuta in pochi anni una tecnologia abilitante e pervasiva per la difesa. L'approccio Nato all'IA si è strutturato lungo una traiettoria che coniuga la necessità di preservare il vantaggio tecnologico-militare dell'Alleanza con un forte impegno verso l'uso responsabile di tali tecnologie come delineato nella NATO's Artificial Intelligence Strategy del 2021, aggiornata poi nel 2024, la quale fissa un quadro politico-normativo comune, a beneficio di interoperabilità, coesione e rispetto del diritto internazionale, anche al fine di mitigare la frammentazione tra gli Alleati.

Allo stato attuale, la funzione primaria dell'IA sul campo di battaglia non è l'*"autonomous lethality"*, ma piuttosto l'intelligence. Veicoli autonomi assistiti dall'IA svolgono principalmente la funzione di intelligence, sorveglianza e ricognizione (*Intelligence, surveillance and reconnaissance, Isr*) a lungo e medio raggio per migliorare la *situational awareness*, contribuendo alla creazione di un quadro operativo comune (*common operational picture*), e per la correzione del tiro (*artillery fire-correction*). Uno degli ambiti più importanti dello sviluppo dell'IA, oltre l'intelligence militare, è l'identificazione della minaccia o *targeting*. L'obiettivo è accelerare il riconoscimento di oggetti, veicoli o comportamenti, riducendo il tempo tra osservazione e valutazione con sistemi IA specializzati, i quali in attività di rilevamento di cambiamenti e anomalie (*change and anomaly detection*), già superano le capacità umane in termini di velocità, accuratezza, affidabilità e quindi minore rischio di errore. Per permettere ciò, è tuttavia necessario che gli equipaggiamenti, così come i dati da essi prodotti, siano connessi e interoperabili. In questa prospettiva gli assetti ed equipaggiamenti legacy vanno riconsiderati come possibili sensori, effettori o comunque nodi di una *"kill web"* abilitata dall'IA, resa possibile attraverso la loro connessione in rete e software IA. Un limite da tenere in considerazione anche nello sviluppo di assetti di futura generazione è tuttavia rappresentato dalla capacità di generazione, accumulo e distribuzione di energia elettrica che le capacità computazionali dell'IA richiedono. Tra i maggiori benefici dell'integrazione dell'IA direttamente a bordo dei sistemi militari c'è poi la manutenzione predittiva (*predictive maintenance*), che consente di superare i tradizionali modelli basati su scadenze fisse o sull'intervento successivo al guasto e di abbassare i costi. Allo stesso modo, l'analisi predittiva dello stato delle piattaforme e dei consumi consente di efficientare la gestione della catena di approvvigionamento e della logistica in generale, anche attraverso l'utilizzo di droni dotati di IA.

La proliferazione in tutti i domini di sistemi senza equipaggio per Isr ha trasformato il moderno campo di battaglia in un ambiente sempre più digitalizzato e trasparente, saturato di sensori capaci di raccogliere in tempo reale enormi quantità di dati a supporto delle operazioni. Un tale flusso informativo eccede la capacità umana di ricevere e valutare gli input e quindi di produrre output. Per garantire la superiorità informativa è necessario quindi delegare tali funzioni alla capacità computazionale dell'IA, la quale è in grado di gestire questo carico cognitivo, filtrando, ordinando e sintetizzando il flusso informativo proveniente da fonti diverse così da renderlo realmente fruibile e utilizzabile dall'operatore o operatrice. In questo modo, l'IA si inserisce direttamente a sostegno della superiorità di comando, velocizzando il ciclo decisionale, dalla raccolta e analisi degli input al suggerimento di opzioni, priorità e alternative di risposta, lasciando all'essere umano la scelta finale. L'IA si presenta quindi come uno strumento di supporto al decisore militare o politico, piuttosto che come suo sostituto. Questo approccio del *human-in-the-loop* appare il più compatibile con un impiego operativo responsabile dell'IA, per cui l'obiettivo non è l'autonomia assoluta del sistema, ma una superiorità decisionale fondata sulla maggiore velocità del ciclo di valutazione e ingaggio. L'IA si dimostra inoltre estremamente utile nell'attività di controllo dell'operazione militare a supporto di una migliore gestione da parte dei vari livelli di comando della complessità dell'operazione, contribuendo alla mitigazione del caos della battaglia e alla rilevazione e valutazione degli scostamenti dal piano originario. In questo ambito, l'obiettivo principale dell'uso dell'IA è infatti migliorare la capacità di osservare, orientarsi, decidere e agire (*Observe, orient, decide, act*, ciclo Ooda) in modo più rapido e accurato rispetto all'avversario, garantendo un vantaggio decisionale, nel rispetto delle normative vigenti. Una delle



sfide più rilevanti rimane, infatti, il confronto con avversari che non condividono il medesimo approccio normativo e operativo della Nato all'impiego dell'intelligenza artificiale in ambito militare, e risultano quindi più veloci e con meno limitazioni.

Il controllo effettivo sulle capacità di un sistema IA dipende inoltre dalla possibilità di sviluppare, addestrare e governare in maniera autonoma il modello, inserendovi i vincoli etico-giuridici e le dottrine che ne modellano il funzionamento. Da qui emerge il tema della sovranità tecnologica, che riguarda non soltanto l'algoritmo in sé, ma anche il controllo sui dati utilizzati per l'addestramento e sulle infrastrutture necessarie al suo funzionamento. L'efficace addestramento del modello presenta infatti due principali difficoltà: la necessità di enormi volumi di dati digitalizzati, affidabili, accessibili e interoperabili che presuppone una profonda digitalizzazione dei dataset rilevanti della Difesa italiana; e la disponibilità di infrastrutture adeguate a soddisfare l'elevata capacità computazionale ed energetica richiesta.

La progressiva digitalizzazione dei processi rappresenta quindi il prerequisito fondamentale per l'adozione dell'IA: gli applicativi non possono funzionare efficacemente senza dataset completi, aggiornati e sistematicamente digitalizzati. Ciò, tuttavia, rende sempre più centrale la cybersecurity per garantirne l'integrità. L'IA, infatti, funge da acceleratore e moltiplicatore della minaccia cyber, abbassando la soglia d'accesso da parte degli avversari e consentendo anche ad attori meno sofisticati di sviluppare capacità offensive significative. L'impiego dell'IA offre al tempo stesso importanti vantaggi difensivi, permettendo agli analisti di concentrarsi su un numero ridotto di eventi rilevanti grazie a sistemi di filtraggio automatico e identificazione delle anomalie. Costituendo la velocità l'elemento distintivo di questo dominio, con tempi di reazione che si misurano in millisecondi, l'intervento umano rischia giocoforza di rappresentare un collo di bottiglia e quindi uno svantaggio piuttosto che un vantaggio. L'IA offre inoltre un vantaggio in chiave di difesa attiva e contrattacco in termini di individuazione delle vulnerabilità avversarie e generazione di payload malevoli, ma in Italia la normativa vigente preclude purtroppo questo tipo di attività alla Difesa a svantaggio della sicurezza cyber dei sistemi militari e civili. La generazione di codice offensivo è infatti importante anche in termini difensivi, permettendo l'addestramento sia dei modelli sia degli operatori attraverso l'utilizzo di ambienti simulati in cui è possibile riprodurre scenari operativi e attacchi realistici.

L'efficace adozione e integrazione di sistemi basati sull'IA nella Difesa italiana richiede quale condizione essenziale la formazione e aggiornamento del personale militare rispetto alla nuova modalità organizzativa e operativa, necessari al fine di assicurarne un uso responsabile, efficace ed efficiente. La prima sfida riguarda il personale che nelle diverse articolazioni della Difesa sarà in varia misura impegnato nella definizione e adattamento degli algoritmi IA come strumenti al servizio del decisore, nel rapporto con fornitori privati di soluzioni IA, nel procurement, manutenzione o logistica di assetti che sono abilitati dall'IA, piuttosto che nella stessa governance dell'IA prevista dalla recente strategia della Difesa al riguardo. Tale personale ha bisogno di maggiori e più approfondite competenze Stem. La seconda sfida riguarda il complesso di ufficiali e sottoufficiali che useranno l'IA a livello strategico, operativo e tattico, e devono quindi essere maggiormente formati per mantenere una adeguata capacità di valutazione delle informazioni fornite, degli scenari proposti e delle opzioni suggerite, così da prendere decisioni consapevoli e mediamente migliori. La fiducia in tali sistemi dipenderà dalla capacità degli operatori di comprenderne i meccanismi decisionali, dove tende a sbagliare e perché, e di valutarne criticamente gli output, preservando la capacità umana di valutare, correggere e decidere e rafforzando così la cultura del comando. Parallelamente, l'IA potrebbe contribuire a migliorare la qualità del training, attraverso per esempio la costruzione di scenari, simulazioni e *wargaming* basati su realtà virtuale e aumentata, percorsi di apprendimento personalizzati con un ciclo di valutazione e feedback più efficace e continuo. L'IA potrebbe, inoltre, migliorare la gestione del personale militare italiano allocandolo in maniera più efficiente o automatizzando e delegando a essa attività ripetitive, burocratiche e a basso valore aggiunto, le cosiddette "*dull functions*", consentendo così di liberare un cospicuo numero di forze da impieghi amministrativi e concentrarle invece sull'addestramento



e su compiti operativi e decisionali.

La consapevolezza dell'ineludibilità del cambiamento in atto, rafforzata dall'evoluzione della postura della Nato e dai processi strutturali di trasformazione delle difese in atto a livello alleato, non riguarda solo l'adozione di singole capacità o assetti, ma investe l'intera architettura organizzativa e operativa della difesa. La strategia della Difesa italiana in materia di IA pubblicata a febbraio 2026 è lo strumento che il vertice politico-strategico ha adottato per colmare un ritardo e un divario accumulati nello scorso decennio rispetto ad altri Paesi, alleati e non, nello sviluppo e l'integrazione di questa tecnologia. Il livello di ambizione perseguito dalla strategia è molto elevato, con tempi di attuazione stringenti. Il documento propone quattro aree di intervento per guidare l'integrazione dell'IA all'interno delle forze armate: operazioni; contesti organizzativi; formazione, addestramento e ricerca; industria. Per mantenere una totale libertà di azione e modifica sull'algoritmo, ossia la capacità di modificarlo, alimentarlo e controllarlo, è necessario esserne proprietari. Per lo sviluppo, la validazione e manutenzione dei modelli, quindi, la strategia prevede di adottare o un approccio *"in house"*, oppure uno basato sul coinvolgimento della base industriale di riferimento, allorché vengano garantite trasparenza, spiegabilità, aggiornamento continuo, supervisione umana, interoperabilità e standardizzazione. Nell'ottica del raggiungimento dell'autonomia strategica, il documento prescrive, come requisito imprescindibile, il ricorso a una capacità di calcolo che dovrà risiedere presso infrastrutture di computazione proprietarie. Particolare attenzione viene attribuita alla gestione del dato, considerato il vero fattore abilitante dell'IA. Per questo motivo, uno degli obiettivi consiste nel superare la tradizionale frammentazione informativa tra le diverse componenti della Difesa, favorendo la condivisione dei dataset e la costruzione di standard comuni. La strategia prevede poi una revisione integrata della governance dell'IA per la Difesa a connotazione interforze articolata in Ufficio per l'IA (Uia), organo politico-strategico di coordinamento, *policy*, supervisione e verifica, e Laboratorio di IA per la Difesa (Liad), il braccio operativo che agisce in qualità di *"AI Delivery Center"* della Difesa. Il Liad si inserisce in una più ampia strategia di rafforzamento dell'ecosistema nazionale dell'innovazione nel settore della difesa e delle tecnologie dual use che mira a favorire il dialogo tra istituzioni, forze armate, università, centri di ricerca e imprese, contribuendo così alla crescita di una filiera nazionale più integrata e competitiva. La sfida per il Laboratorio sarà creare le condizioni affinché i dati della Difesa possano essere utilizzati in sicurezza per finalità di addestramento, sperimentazione e sviluppo algoritmico. Questa piattaforma sarà più efficace quanto più riuscirà a coinvolgere i giovani ufficiali, nativi digitali, e le accademie, attraverso un approccio *"bottom-up"*. In generale, anche considerata la rapidità di evoluzione della tecnologia, la strategia è concepita come uno strumento dinamico e adattabile, sviluppato attraverso un processo partecipativo e completato da un piano attuativo.

1. Introduzione: l'approccio Nato all'IA

L'intelligenza artificiale (IA) è divenuta in pochi anni una tecnologia abilitante e pervasiva anche per la difesa, in particolare negli Stati Uniti che contano al riguardo su una leadership tecnologica e industriale nel campo civile, ma anche nei Paesi europei che avvertono la necessità di sfruttare le opportunità e mitigare i rischi di questo fattore cruciale per la sicurezza nazionale. Di conseguenza, la Nato ha sviluppato un approccio all'IA lavorando sui necessari cambiamenti a partire dal piano dottrinale. Dal 2021 l'IA, insieme ai sistemi autonomi e alle tecnologie quantistiche, è stata progressivamente integrata nel quadro più ampio delle tecnologie emergenti e dirompenti (*emerging and disruptive technologies*, Edt)¹ e nella riflessione sull'adattamento dell'architettura di deterrenza e difesa alleata al contesto tecnologico in rapida evoluzione².

¹ Si veda la strategia "Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies" citata in: Nato, *Innovation and Technology Adoption*, 8 luglio 2026, <https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies>.

² Ibid.



Conseguentemente, la Nato guarda all'IA sia come un'opportunità sia come fonte di rischi sistemici. Da un lato, strumento per rafforzare deterrenza e difesa, trovando le principali aree di applicazione nel potenziamento delle capacità di intelligence, sorveglianza e ricognizione (*Intelligence, surveillance and reconnaissance*, Isr), nell'accelerazione ed efficacia dei sistemi di comando e controllo (C2), nonché nel miglioramento della logistica e dell'addestramento (*training*)³. Dall'altro lato, l'IA è un potente strumento anche nelle mani degli avversari, con un effetto moltiplicatore che va dall'impiego dei sistemi autonomi alle campagne di manipolazione dell'informazione su larga scala.

L'approccio Nato all'IA si è, infatti, strutturato lungo una traiettoria che coniuga la necessità di preservare il vantaggio tecnologico-militare dell'Alleanza con un forte impegno verso l'uso responsabile di tali tecnologie (*Responsible AI*, Rai)⁴. In questo quadro, la Nato vede quindi sé stessa come piattaforma di scambio di informazioni e *best practices*, anche al fine di mitigare la frammentazione derivante dai diversi livelli di maturità tecnologica degli Alleati⁵, in particolare visto il divario tra gli Stati Uniti e il resto dell'Alleanza, e preservare l'interoperabilità alla base delle proprie operazioni di coalizione. Nel fare ciò, si pone come "attore responsabile" (*responsible actor*)⁶ "ensuring that its values, ethical stances as well as moral commitments will remain central"⁷, stabilendo sei principi di uso responsabile (*Principles of Responsible Use: lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, bias mitigation*)⁸ già nella sua prima strategia IA del 2021⁹. La priorità era anzitutto fissare un quadro politico-normativo comune, a beneficio di interoperabilità, coesione e rispetto del diritto internazionale, capace di orientare, senza comprometterne la sovranità, l'adozione dell'IA da parte degli Alleati, i quali ancora non disponevano di una specifica strategia militare in materia¹⁰. Tuttavia, i sei principi vengono spesso criticati per essere "troppo vaghi per funzionare da vincolo autentico"¹¹ e per la loro mancanza di concretezza¹², richiedendo indicazioni dettagliate che risultano difficili da fornire a causa della diversità di valutazioni etiche e minacce percepite, nonché delle differenti capacità infrastrutturali degli Alleati¹³. Di nuovo, gli Stati Uniti rappresentano un caso unico, con uno scontro tra l'amministrazione Trump e fornitori di soluzioni IA per la difesa sui limiti di quest'ultima, avvenuto tra febbraio e marzo 2026.

In questo contesto di varietà di approcci tra alleati si inserisce il Data and AI Review Board (Darb) della Nato, composto da delegati dei 32 Paesi membri, il quale rappresenta il braccio operativo della strategia e ha il compito di rendere operativi i sei principi attraverso lo sviluppo di strumenti pratici e standard di certificazione per un'IA responsabile¹⁴. Inoltre, il Board guida e supervisiona l'attuazione responsabile dell'IA nelle strutture di tutta l'Alleanza, fungendo contestualmente da forum di confronto tra industria, governi

³ EU Institute for Security Studies, *The EU, NATO and Artificial Intelligence. New Possibilities for Cooperation?*, novembre 2019, <https://www.iss.europa.eu/sites/default/files/EUISSFiles/EU%20NATO%20AI%20-%20Report.pdf>.

⁴ Reynolds, Ian e Yasir Atalan, "Calibrating NATO's Vision of AI-Enabled Decision Support", in *CSIS Commentaries*, 8 luglio 2024, <https://www.csis.org/node/111392>.

⁵ Nato, *Summary of NATO's Revised Artificial Intelligence (AI) Strategy*, 10 luglio 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>.

⁶ Onderco, Michal, "Navigating the AI Frontier: Insights from the Ukraine Conflict for NATO's Governance Role in Military AI", in *Journal of Strategic Studies*, vol. 48, n. 3 (2025), p. 602-626 a p. 608, <https://doi.org/10.1080/01402390.2025.2463451>.

⁷ Gilli, Andrea, "Preparing for 'NATO-mation': the Atlantic Alliance toward the Age of Artificial Intelligence", in *NDC Policy Briefs*, n. 4 (febbraio 2019), <https://www.ndc.nato.int/?p=4792>.

⁸ 1) Lawfulness (AI must comply with national and international law), 2) Responsibility and Accountability (human oversight and accountability must be ensured), 3) Explainability and Traceability (AI systems must remain transparent and verifiable), 4) Reliability (AI must be safe, secure, and tested for defined use cases), 5) Governability (AI must allow human control and intervention in case of unintended behaviour), 6) Bias Mitigation (efforts must minimise bias in AI systems and data sets).

⁹ Nato, *Summary of the NATO Artificial Intelligence Strategy*, 22 ottobre 2021, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy>.

¹⁰ Onderco, Michal, "Navigating the AI Frontier", cit., p. 608.

¹¹ "Too vague to function as a genuine constraint". Ibid., p. 604.

¹² Waldrip, Brian, "NATO Updates AI Strategy and Includes Emphasis on AI Safety", in *CAIP Opinions*, 16 luglio 2024, <https://www.centraipolicy.org/work/nato-updates-ai-strategy-and-includes-emphasis-on-ai-safety>.

¹³ Reynolds, Ian e Yasir Atalan, "Calibrating NATO's Vision of AI-Enabled Decision Support", cit.

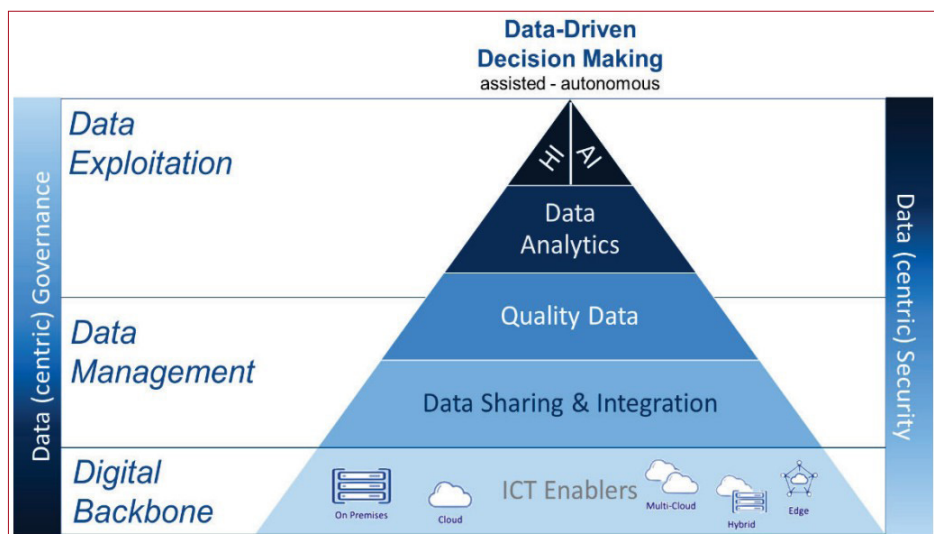
¹⁴ "Practical Responsible AI toolkits" e "Responsible AI certification standards". Si veda Nato, *Innovation and Technology Adoption*, cit.



e mondo accademico¹⁵. Tuttavia, la mancanza di meccanismi di *enforcement* rende complesso lo sviluppo di standard comuni, mentre i sei principi si scontrano con ampie differenze nell'adozione pratica a seconda della leadership e delle culture politiche e militari dei singoli paesi. Il nodo principale della Responsible AI sembra rimanere la necessità di conciliare il vantaggio strategico e operativo che l'IA conferisce allo strumento militare con l'esigenza di garantire un'"appropriata interazione uomo-macchina"¹⁶.

In ogni caso, lo sviluppo senza precedenti e l'ampia disponibilità di potenti tecnologie IA hanno obbligato la Nato ad accelerarne lo sviluppo e la diffusione nel ventaglio delle proprie capacità. La pubblicazione della *Revised Artificial Intelligence Strategy* nel 2024, solamente tre anni dopo la prima, mira a gestire la rapida evoluzione tecnologica, con particolare attenzione all'IA generativa e agli strumenti informativi potenziati dall'IA, con lo scopo di contrastare le interferenze e le campagne di disinformazione avversarie¹⁷. La nuova strategia dedica inoltre particolare attenzione alla qualità dei dati utilizzati per l'addestramento dei modelli e all'impiego dei dati generati con l'IA da parte degli operatori umani. Ricalcando l'impegno per i sei principi, la *Data Exploitation Framework Policy* mira a garantire un uso responsabile dei dati in linea con i valori dell'Alleanza, avendo come primo obiettivo strategico l'*empowerment* della persona e un approccio all'utilizzo dei dati "incentrato sull'utente e guidato"¹⁸. È lo Allied Command Transformation che porta avanti lo sforzo per migliorare il modo in cui i dati vengono gestiti e utilizzati nelle strutture Nato, al fine di sfruttare l'IA in tutti i domini, organizzando *wargaming* e formazione, e supportando gli sforzi di standardizzazione.

Figura 1 | NATO data-driven decision-making pyramid



Fonte: Nato, *Data Centric Reference Architecture for the Alliance. Version 2, 2025*,
[https://nhqc3s.hq.nato.int/apps/public/AC322-D\(2025\)0056-Data_Centric_Reference_Architecture_v2.pdf](https://nhqc3s.hq.nato.int/apps/public/AC322-D(2025)0056-Data_Centric_Reference_Architecture_v2.pdf)

I principali ostacoli tecnici alla padronanza dell'IA da parte dell'Alleanza concernono l'interoperabilità tra gli Alleati e lo sviluppo di data set e standard comuni per consentire operazioni di coalizione, poiché un processo decisionale più rapido non deriva unicamente dall'integrazione dell'IA nelle operazioni, ma richiede anche

¹⁵ Nato, *NATO's Data and Artificial Intelligence Review Board*, 13 ottobre 2022, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/10/13/natos-data-and-artificial-intelligence-review-board>.

¹⁶ "Appropriate human-machine interaction". Nato, *Summary of the NATO Artificial Intelligence Strategy*, cit.

¹⁷ Nato, *Summary of NATO's Revised Artificial Intelligence (AI) Strategy*, cit.

¹⁸ "User-focused and leader-driven approach". Nato, *Summary of NATO's Data Exploitation Framework Policy*, 23 novembre 2022, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/11/23/summary-of-natos-data-exploitation-framework-policy>.



la risoluzione di problemi di coordinamento, il miglioramento della qualità dei dati, l'addestramento dei modelli e l'adozione di processi condivisi per la definizione degli standard¹⁹. In quest'ottica, la Nato intende assumere un ruolo centrale nella gestione e integrazione dei dati dell'Alleanza attraverso l'organizzazione del database, con l'obiettivo di garantire un accesso pieno e condiviso alle informazioni (*availability*) preservando al contempo l'integrità (*integrity*) e la protezione da accessi o divulgazione non autorizzate (*confidentiality*) dei dati²⁰. A questo scopo, per dotarsi della capacità di integrare, analizzare e rendere interoperabili grandi volumi di dati provenienti da fonti eterogenee e diversi domini operativi, nell'ambito dello Allied Command Operations, la Nato ha recentemente scelto la piattaforma Maven Smart System di Palantir²¹. La decisione, attraverso un processo di procurement di soli sei mesi, riflette la volontà di accelerare la trasformazione digitale e l'urgenza di mantenere il vantaggio tecnologico dell'Alleanza²². La scelta conferma inoltre la dipendenza alleata da fornitori statunitensi di soluzioni IA.

2. IA ed equipaggiamenti militari

In campo occidentale e dalla fine della Seconda Guerra Mondiale, l'evoluzione tecnologica nel settore della difesa ha risposto a due esigenze complementari: da un lato aumentare l'efficacia operativa delle forze in combattimento, in termini di potenza di fuoco, mobilità, velocità, coordinamento e precisione, potenziandone le capacità sia difensive che offensive; dall'altro ridurre i costi umani limitando l'esposizione al rischio del combattente, in linea con il valore attribuito dalle società occidentali alla vita del singolo individuo, obiettivo perseguito attraverso la graduale diminuzione della presenza umana sul campo di battaglia e l'estensione progressiva della distanza dal punto di ingaggio²³. L'integrazione dell'IA negli equipaggiamenti militari, siano essi da combattimento terrestri, aerei o navali, di supporto logistico, di protezione individuale o di comando, controllo, comunicazioni, computer, intelligence, sorveglianza e ricognizione (*Command, control, communications, computers, intelligence, surveillance and reconnaissance, C4Isr*), concorre al conseguimento di entrambi questi obiettivi e si pone quindi in linea con sviluppi tecnologici e dottrinali precedenti.

Allo stato attuale, in ambito militare, la funzione primaria dell'IA sul campo di battaglia non è l'"*autonomous lethality*"²⁴, ma piuttosto l'intelligence. Tale tecnologia assolve infatti principalmente funzioni di gestione ed elaborazione dei dati, consentendo la raccolta, aggregazione, integrazione, analisi e diffusione delle informazioni, e quindi del supporto decisionale all'operatore umano, caricandosi così di un importante carico cognitivo²⁵. Va inoltre sottolineato che solo l'impiego di questa tecnologia consente ormai un efficace e tempestivo utilizzo della massa di informazioni oggi disponibili sulla base di sensori dedicati e banche dati costantemente aggiornate grazie al moltiplicarsi delle fonti di informazione (si veda al riguardo il capitolo tre). Anche laddove le capacità tecnologiche lo consentirebbero, stante le informazioni pubbliche disponibili, il suo impiego in modalità pienamente autonome sul campo di battaglia non è ancora avvenuto. Infatti, sebbene la direzione sia quella di andare verso l'eliminazione dell'essere umano dalla prima linea (*First Line of Troops*, Flot) in favore di una robotizzazione della stessa (*First Line of Robots*, Flor)²⁶, ad oggi veicoli autonomi assistiti dall'IA hanno svolto principalmente la funzione di Isr a lungo e

¹⁹ Reynolds, Ian e Yasir Atalan, "Calibrating NATO's Vision of AI-Enabled Decision Support", cit.

²⁰ Intervista del 2 febbraio 2026 (1).

²¹ Intervista del 2 febbraio 2026 (2).

²² "NATO Deploys Advanced AI System in Landmark Defence Technology Shift", in *EU Today*, 15 aprile 2025, <https://eutoday.net/nato-deploys-advanced-ai-system>.

²³ Interviste del 2 febbraio 2026 (1) e dell'11 febbraio 2026.

²⁴ King, Anthony, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence", in *Journal of Global Security Studies*, vol. 9, n. 2 (giugno 2024), articolo ogae009, <https://doi.org/10.1093/jogss/ogae009>.

²⁵ International Institute for Strategic Studies, "Big Data, Artificial Intelligence and Defence", in *The Military Balance 2018*, 14 febbraio 2018, p. 10-13 a p. 2, https://www.inss.org.il/private/wp-content/uploads/sites/3/2018/03/Chapter-I-Part-II_-Big-data-artificial-intelligence-and-defence_-IISS.pdf.

²⁶ International Institute for Strategic Studies, "Big Data, Artificial Intelligence and Defence", cit., p. 3.



medio raggio per migliorare la *situational awareness*, contribuendo alla creazione di un quadro operativo comune (*common operational picture*), e per la correzione del tiro (*artillery fire-correction*)²⁷. Il conflitto russo-ucraino ha accelerato i progressi di adozione e sviluppo di queste tecnologie specialmente nell'ambito della navigazione in ambienti in cui è assente il segnale Gps (*GPS-denied*) e delle operazioni coordinate in sciame, entrambe abilitate dall'IA²⁸. Nel medesimo contesto, veicoli terrestri senza equipaggio (*Unmanned ground vehicles*, Ugv) dotati di software basato sull'IA sono stati inoltre utilizzati per operazioni di sminamento, migliorandone l'efficienza e preservando al contempo la sicurezza delle forze²⁹. L'urgenza di far fronte a un notevole squilibrio di forze umane a favore della Russia ha obbligato l'Ucraina a sviluppare, integrare e dispiegare in modo estremamente rapido sul campo nuove tecnologie senza pilota basate sull'IA, e per questo creare *ex novo* unità esclusivamente dedicate alla loro integrazione nelle operazioni, come le Unmanned Systems Forces³⁰. Per questo motivo, l'integrazione dell'IA nei droni – siano essi veicoli terrestri, aeromobili (*Unmanned aerial vehicles*, Uav) e veicoli sottomarini (*Unmanned underwater vehicles*, Uuv) – è oggi una delle aree di sviluppo più rapide. Ne costituisce un esempio, difficilmente immaginabile fino a poco tempo fa, un'operazione militare condotta ad aprile 2026 senza il dispiegamento di forze sul terreno, ma esclusivamente mediante veicoli senza equipaggio controllati a distanza e conclusasi con la resa delle forze russe e la presa della posizione³¹. L'impiego di questi sistemi in oltre 22.000 missioni ad alto rischio³² ha consentito di ridurre significativamente l'esposizione del personale ucraino al combattimento, contribuendo a salvare migliaia di vite³³.

Uno degli ambiti più importanti dello sviluppo dell'IA, oltre l'intelligence militare, è l'identificazione della minaccia o *targeting* (*Automatic target recognition*, Atr)³⁴. L'obiettivo è accelerare il riconoscimento di oggetti, veicoli o comportamenti, riducendo il tempo tra osservazione e valutazione con sistemi IA specializzati, i quali, in attività di rilevamento di cambiamenti e anomalie (*change and anomaly detection*), già superano le capacità umane in termini di velocità, accuratezza, affidabilità e quindi minore rischio di errore³⁵. La medesima metodologia IA utilizzata per incrementare la velocità di analisi dei dati Isr è alla base dell'accelerazione e miglioramento del ciclo di *targeting*, dall'identificazione dell'obiettivo al suo ingaggio³⁶: nel corso degli ultimi anni questa tecnologia ha così già ridotto drasticamente la tempistica del ciclo "sensor-to-shooter".

Tuttavia, per permettere l'aggregazione e l'analisi dei dati provenienti dal campo di battaglia per abilitare tali capacità, è necessario che tutti gli equipaggiamenti siano connessi e che vi sia piena interoperabilità dei dati stessi. Per sfruttare appieno le capacità dell'IA è infatti necessario costruire un ambiente operativo integrato nel quale sensori, piattaforme, sistemi d'arma e reti di C2 operano come un unico ecosistema connesso nel cloud a loro supporto, anche nella prospettiva di operazioni multi-dominio (*multi-domain operations*) e di coalizione (Nato)³⁷. L'interoperabilità, in questo contesto, è riferita al dato che deve essere compatibile, aggregabile, confrontabile e utilizzabile da tutti i sistemi d'arma, dove l'informazione raccolta da ogni sensore presente su qualsiasi piattaforma può arrivare in tempo reale al sistema d'arma migliore

²⁷ Bondar, Kateryna, "Understanding the Military AI Ecosystem of Ukraine", in *CSIS Reports*, 12 novembre 2024; <https://www.csis.org/node/113242>; interviste dell'11 febbraio e del 2 marzo 2026.

²⁸ Bondar, Kateryna, "Understanding the Military AI Ecosystem of Ukraine", cit.

²⁹ Ibid.

³⁰ Ibid.

³¹ Kottasová, Ivana et al., "'Robots Don't Bleed': Ukraine Sends Machines into the Battlefield in Place of Human Soldiers", in *CNN*, 20 aprile 2026, <https://www.cnn.com/2026/04/20/europe/robots-ukraine-battlefield-drones-intl-cmd>.

³² Dato aggiornato ad aprile 2026.

³³ Kottasová, Ivana et al., "'Robots Don't Bleed'", cit.

³⁴ Processo di selezione e ingaggio dei bersagli in modo efficace, minimizzando al contempo i danni collaterali. Intervista del 2 febbraio 2026 (1).

³⁵ Intervista del 19 febbraio e 2 febbraio 2026 (1).

³⁶ Ciclo del targeting: *target identification, acquisition, navigation and guidance*.

³⁷ Calcagno, Elio (a cura di), "Taking Multi-Domain Operations from Theory to Practice", in *Documenti IAI*, n. 26|01 (febbraio 2026), <https://www.iai.it/en/node/21507>.



(*any sensor, best shooter*)³⁸, permettendo così in teoria il passaggio dall'odierna “kill chain” a una “kill web” più efficace. Tuttavia, un collo di bottiglia rispetto allo sviluppo di tale architettura è rappresentato dalla disponibilità di banda necessaria a sostenere il trasferimento continuo di enormi quantità di dati raccolti sul campo di battaglia verso il cloud³⁹. Assume quindi una crescente rilevanza l'integrazione di capacità di *edge computing* direttamente a bordo delle piattaforme finalizzate a massimizzare la capacità di processamento in locale, consentendo sia di ridurre la quantità dei dati da trasferire sia di ridurre la dipendenza dal cloud e aumentarne così l'autonomia operativa.

In questa prospettiva gli assetti ed equipaggiamenti legacy vanno reconsiderati come possibili sensori, effettori o comunque nodi di una “kill web” abilitata dall'IA e adattata alla nuova realtà del campo di battaglia. Nell'ottica della progressiva riduzione della presenza dell'essere umano dalla prima linea e della proliferazione di sensori e attuatori, l'aggiornamento di piattaforme non più in grado di garantire adeguati livelli di protezione del personale militare né un'efficace capacità operativa deve necessariamente passare attraverso processi di robotizzazione, connessione e integrazione di capacità autonome o remotizzate (*Internet of Military Things*), anche attraverso un cambiamento della funzione dello stesso mezzo⁴⁰. La non interoperabilità tra assetti *legacy* e di nuova generazione potrebbe quindi venire superata attraverso la loro connessione in rete e l'impiego di software IA, permettendo così l'integrazione di piattaforme eterogenee per età, capacità funzionale, livello tecnologico e dominio operativo all'interno di un'unica architettura operativa multi-dominio⁴¹. Un limite all'effettiva integrazione di capacità autonome in assetti di vecchia generazione è tuttavia rappresentato dalla capacità di generazione, accumulo e distribuzione di energia elettrica. L'integrazione di sensori, effettori, sistemi di comunicazione e capacità computazionali determina infatti un incremento significativo del fabbisogno energetico delle piattaforme per cui queste non sono state tuttavia originariamente progettate e che rappresenta quindi un vincolo strutturale a questa trasformazione.

Lo stesso vincolo è però da tenere in considerazione anche nello sviluppo di assetti di futura generazione, per i quali l'obiettivo e sfida sarà l'integrazione di capacità IA “edge” nei sistemi d'arma e nelle piattaforme tali da ridurre la dipendenza dalla connettività e dal cloud per l'espletamento delle loro missioni⁴². Scenari operativi potrebbero infatti imporre a tali piattaforme di operare in ambienti in cui la connessione a infrastrutture cloud o nodi C2 è negata o degradata, e di essere comunque in grado di mantenere autonomia decisionale, capacità di elaborazione locale e continuità operativa.

Tra i maggiori benefici dell'integrazione dell'IA direttamente a bordo dei sistemi militari c'è la manutenzione predittiva (*predictive maintenance*), che consente di superare i tradizionali modelli manutentivi basati su scadenze fisse o sull'intervento successivo al guasto. Attraverso l'analisi dei dati provenienti da sensori a bordo e l'impiego di algoritmi predittivi di *machine learning*, i sistemi abilitati dall'IA sono infatti in grado di identificare anomalie, degradi e andamenti ricorrenti, prevedendo quando potrebbero verificarsi dei guasti, abbassando così i costi di manutenzione e sostituzione e permettendo la pianificazione puntuale delle forniture delle parti di ricambio⁴³. Infatti, parallelamente, l'IA ha assunto un ruolo crescente anche nell'ottimizzazione della logistica militare, caratterizzata da complessità, forte dispersione geografica, scala continentale se non globale e la necessità di adattamento continuo a dinamiche operative e fattori poco prevedibili. In questo contesto, l'analisi predittiva dello stato delle piattaforme e dei consumi consente

³⁸ Intervista del 2 febbraio 2026 (1).

³⁹ Intervista dell'11 febbraio 2026.

⁴⁰ Intervista del 2 febbraio (1) e dell'11 febbraio 2026.

⁴¹ Calcagno, Elio (a cura di), “Taking Multi-Domain Operations from Theory to Practice”, cit.

⁴² Intervista dell'11 febbraio 2026.

⁴³ Gaire, Utsav Sharma, “Application of Artificial Intelligence in the Military: An Overview”, in *Unity Journal*, vol. 4, n. 1 (2023), p. 161-174, <https://www.researchgate.net/publication/368557872>; Aburass, Sanad et al., “Artificial Intelligence in the Global Military and Weapon Industry”, in *Jordan Scientific Journal*, vol. 2, n. 1 (2025), p. 36-60, <https://jsj.ju.edu.jo/ojs351/index.php/jsj/en/article/view/14>; International Institute for Strategic Studies, “Big Data, Artificial Intelligence and Defence”, cit.



di efficientare la gestione della catena di approvvigionamento e il trasporto logistico. Quest'ultimo può anche beneficiare di Ugv abilitati dall'IA, ai fini sia di efficientamento che di riduzione del rischio per il personale militare in teatro operativo. Più in generale, l'IA può fornire un grande valore aggiunto in termini di velocizzazione delle procedure per tutto quello che riguarda la gestione del procurement e degli equipaggiamenti in servizio, per i quali è però indispensabile registrare il reale stato di efficienza e prontezza operativa se si vuole sfruttare il potenziale dell'IA, ad esempio quanto a manutenzione predittiva, logistica militare e relative infrastrutture. Se si vuole ottenere una maggiore e migliore adozione dell'IA per tali funzioni, il divario tra rappresentazione formale (normativa), rappresentazione digitale (i.e. il dataset) e realtà operativa dovrebbe essere eliminato, in quanto se il sistema IA viene alimentato con dati non accuratamente e funzionalmente rappresentativi della realtà, il supporto decisionale prodotto sarà inevitabilmente distorto con effetti dannosi sull'efficienza delle stesse Forze armate⁴⁴.

A fronte di benefici diffusi in termini di capacità operative e funzioni di supporto, manutenzione e logistica, l'integrazione di capacità IA *"edge"* nei sistemi militari comporta, come precedentemente accennato, un ulteriore incremento dei requisiti computazionali e quindi energetici a bordo della piattaforma, condizionando i nuovi equipaggiamenti in termini di volume, alimentazione e produzione di energia elettrica, peso, bassa osservabilità e segnatura termica⁴⁵. La capacità computazionale nelle piattaforme è andata aumentando di generazione in generazione, per esempio da Tornado a EuroFighter a F-35, e aumenterà ancora di più con piattaforme di nuova generazione come il Gcap, dove questi tipi di *trade-off* dovranno essere tenuti in considerazione⁴⁶. Già oggi, infatti, alcuni singoli sistemi d'arma della Difesa italiana, in particolare quelli in dotazione ad Aeronautica e Marina, sono fortemente digitalizzati, più di quanto non lo sia la stessa struttura complessiva delle Forze armate quanto ad esempio a comando e controllo. In una certa misura, singole piattaforme o sistemi di sistemi rilevano già la realtà a partire dai propri sensori e dai dati che vengono condivisi, e la confrontano con le proprie banche dati interne. Queste ultime devono quindi essere continuamente aggiornate e complete, per permettere all'IA di operare in maniera efficace. Nel caso degli F-35, il lavoro di aggiornamento del patrimonio di dati viene fatto oggi da soggetti statunitensi, ma per il Gcap dovrebbe essere un compito della difesa italiana per il quale occorrerà attrezzarsi per tempo. L'obiettivo dovrebbe essere disporre di librerie dinamiche all'interno dell'architettura cloud, aggiornabili in tempo reale e utilizzabili da tutte le piattaforme che dialogano e scambiano dati essendo connesse appunto alla stessa architettura cloud⁴⁷.

L'acquisizione di tecnologia IA si scontra inoltre con un più ampio limite strutturale del sistema di procurement italiano, originariamente concepito per piattaforme complesse tradizionali – come fregate, carri o velivoli – caratterizzate da relativa stabilità tecnologica e dei requisiti operativi, e quindi da lunghi cicli di sviluppo, acquisizione e aggiornamento. In tale sistema, i costi elevati di ricerca e sviluppo nonché di produzione richiedono una certa massa critica per assicurare economie di scala, pianificazione di lungo periodo e certezza delle produzioni. L'attuale sistema di procurement opera, infatti, su orizzonti temporali tendenzialmente di alcune decine di anni, che tuttavia risultano oggi rigidi e incompatibili con i ritmi dell'innovazione tecnologica legata all'IA. Il rischio è che definendo il requisito oggi, questo si traduca, dopo i diversi anni necessari al procurement, in una capacità tecnologica già superata, a fronte di aumenti

⁴⁴ I dati presenti nel dataset, e quindi il dataset stesso, non sono la realtà, ma una rappresentazione digitale della realtà: un mondo sintetico. La fase di sviluppo e successiva alimentazione del dataset attraverso la digitalizzazione delle informazioni e dei dati, dalla creazione dell'ontologia alla classificazione e organizzazione dei dati stessi, porta già con sé un certo tipo di decisione soggettiva sulla rappresentazione della realtà. Quest'ultima, oltre ad essere accurata, dovrebbe essere quindi funzionale allo scopo del sistema che si sta creando.

⁴⁵ Intervista dell'11 febbraio 2026.

⁴⁶ Murgia, Nicolò et al., "Le nuove frontiere della propulsione aeronautica tra sfide tecnologiche, sostenibilità ambientale e sicurezza nazionale", in *Documenti IAI*, n. 25|12 (ottobre 2025), <https://www.iai.it/it/node/20667>; Marrone, Alessandro (a cura di), "The New Partnership among Italy, Japan and the UK on the Global Combat Air Programme (GCAP)", in *Documenti IAI*, n. 25|03 (marzo 2025), <https://www.iai.it/it/node/19737>.

⁴⁷ Intervista del 23 febbraio 2026.



di costo che non corrispondono a un aumento di valore. In altri contesti, si è cercato di affrontare la sfida di velocizzare il procurement militare con iniziative quali l'Unmanned Systems Forces ucraina o la statunitense Transforming in Contact (TiC)⁴⁸, che permettono di accelerare la sperimentazione, validazione e distribuzione alle brigate, in un ciclo di adozione della nuova tecnologia più rapido.

Una delle difficoltà principali nel procurement di sistemi di IA o dotati di IA riguarda inoltre i criteri alla base della loro certificazione e omologazione. A differenza dei sistemi tradizionali, il cui comportamento è deterministico⁴⁹ e quindi prevedibile quando sottoposti a test identici e ripetibili, quelli basati sull'IA operano attraverso modelli probabilistici e inferenze statistiche, con la conseguenza che i risultati dei test possono variare nel tempo e non vi è piena prevedibilità del risultato⁵⁰. Il problema assume una rilevanza ancora maggiore con l'entrata in servizio, in quanto la loro efficacia nel tempo dipende dalla disponibilità di dati continuamente aggiornati e da processi costanti di addestramento dei modelli in scenari operativi reali⁵¹. Ciò contribuisce tra l'altro a spiegare anche il loro rapido sviluppo negli ultimi anni, favorito dalla disponibilità di *sandbox*⁵² reali, fornite dalla guerra in Ucraina e in Medio Oriente, e di enormi quantità di dati. In questo senso, i sistemi dotati di IA tendono a migliorare progressivamente attraverso l'impiego operativo, rendendo la verifica delle prestazioni un processo continuo lungo l'intero ciclo di vita del sistema piuttosto che una fase limitata al collaudo iniziale. Tale caratteristica collide tuttavia con gli attuali strumenti di procurement e contrattualizzazione della difesa, i quali risultano quindi largamente inadatti per acquisire tale tecnologia.

Infine, da notare come una delle prime applicazioni dell'IA potrebbe essere collegata alla digitalizzazione della stazione appaltante, per portare a un aumento dell'efficienza e della produttività molto significativo a parità di risorse umane⁵³, aiutando così il processo complessivo di procurement anche a favore della stessa introduzione dell'IA nella difesa. Ci sono già iniziative in cantiere al riguardo, che potrebbero rappresentare progetti pilota e buone prassi per una introduzione più ampia dell'IA negli aspetti gestionali delle Forze armate, dal personale al procurement alle infrastrutture militari.

3. IA e comando e controllo

L'efficacia delle operazioni militari è fortemente influenzata dal livello di superiorità informativa e quindi dal sistema di comando e controllo. La proliferazione in tutti i domini di sistemi senza equipaggio per Isr ha trasformato il moderno campo di battaglia in un ambiente sempre più digitalizzato e trasparente, saturato di sensori capaci di raccogliere in tempo reale enormi quantità di dati a supporto delle operazioni. Un tale flusso informativo eccede la capacità umana di ricevere, classificare, assorbire, analizzare, valutare gli input e quindi di produrre output⁵⁴. Per garantire la superiorità informativa delle Forze armate italiane è necessario quindi delegare tali funzioni alla capacità computazionale dell'IA, la quale è in grado di gestire questo carico cognitivo, filtrando, ordinando e sintetizzando il flusso informativo proveniente da fonti diverse (in primis tramite algoritmi di *sensor fusion*) così da renderlo realmente fruibile e utilizzabile

⁴⁸ Transforming in Contact (TiC) è un'iniziativa dello US Army che mira ad accelerare l'introduzione di nuove tecnologie, come droni, AI e robotica, direttamente a disposizione dei soldati impiegati in unità pronte al combattimento. Essa consente di testare rapidamente tali tecnologie, raccogliere il feedback degli utilizzatori e apportare modifiche durante le esercitazioni addestrative, favorendo così un'adozione più rapida delle nuove capacità operative. Anderson, Bradley e Kathryn Bailey "Transforming in Contact", in *Army AL&T*, agosto 2024, p. 36-43, https://www.army.mil/article/278935/transforming_in_contact.

⁴⁹ Ovvero, a un determinato input corrisponde un output prevedibile.

⁵⁰ Intervista del 2 febbraio (1) e del 2 marzo 2026.

⁵¹ Intervista del 19 febbraio 2026.

⁵² Una sandbox è un'area geografica o un ambiente controllato in cui si testano tattiche, tecnologie, sistemi d'arma o procedure operative.

⁵³ Intervista del 19 febbraio 2026.

⁵⁴ Marton, Imrich et al., *The Future of Drones: Strategic Interregnum*, Bratislava, Adapt Institute, dicembre 2025, <https://www.adaptinstitute.org/?p=13868>.



dall'operatore o operatrice⁵⁵. Il controllo umano sullo strumento è assicurato dalla possibilità, per il fruitore, di accedere direttamente ai dati e alle immagini e video elaborati dal sistema IA, verificandone e validandone le valutazioni.

In questo modo, l'IA si inserisce direttamente a sostegno della superiorità di comando, velocizzando il ciclo decisionale, dalla raccolta e analisi degli input al suggerimento di opzioni, priorità e alternative di risposta, lasciando all'essere umano la scelta finale. La superiorità di comando riguarda infatti la capacità di prendere decisioni efficaci in tempi compatibili con la velocità del conflitto contemporaneo. In tale contesto, l'IA si presenta come uno strumento di supporto al decisore militare o politico, piuttosto che come suo sostituto. Questo approccio del *human-in-the-loop* (Hitl) appare il più compatibile con un impiego operativo responsabile dell'IA, per cui l'obiettivo non è l'autonomia assoluta del sistema, ma una superiorità decisionale fondata sulla maggiore velocità del ciclo di valutazione e ingaggio. Nel ciclo di *Target Evaluation and Weapon Assignment* (Tewa), per esempio, il sistema non decide in autonomia se ingaggiare, ma contribuisce a determinare, ottimizzando l'utilizzo delle risorse secondo un'allocazione efficiente, quale sia l'assetto più adatto all'ingaggio (*best shooter*) suggerendo opzioni all'autorità designata (*target engagement authority*), cui rimane in capo la decisione (principio di *accountability*)⁵⁶. Si tratta di una forma di integrazione dell'IA che rafforza il C2 senza trasferire alla macchina la facoltà di aprire il fuoco, ma assistendo il decisore politico e militare nella valutazione delle informazioni e nell'individuazione delle possibili linee d'azione⁵⁷.

L'IA si dimostra inoltre estremamente utile nell'attività di controllo dell'operazione militare (la cosiddetta fase condotta) a supporto della gestione da parte del comandante della complessità dell'operazione, contribuendo, in ultima istanza, a evitare il fuoco amico (*blue on blue*). In questa fase, in cui risulta difficile esercitare l'attività di controllo a causa della dinamicità e dell'estensione dell'operazione moderna composta da azioni materiali e immateriali in domini diversi, l'IA contribuisce alla mitigazione del caos della battaglia e alla rilevazione e valutazione degli scostamenti dal piano originario, anche al fine di meglio valorizzare l'autonomia decisionale locale e il comando decentrato. L'IA sarebbe infatti in grado di supportare l'esercizio della funzione di controllo, mediante il monitoraggio continuo dell'intero dispositivo multi-dominio attraverso il flusso ascendente di informazioni verso il comando, nonché di accelerare ed efficientare la gestione del flusso discendente di informazioni verso le forze sul campo, contribuendo a selezionare e prioritizzare le informazioni loro necessarie in un contesto di capacità di banda limitata⁵⁸.

Il nodo circa la collocazione dell'intervento umano nel processo decisionale – il suddetto Hitl, oppure *human-on-the-loop* (Hotl) o *human-out-of-the-loop* (Hootl) – è alla base di riflessioni etiche e giuridiche riguardo la responsabilità delle azioni militari, per esempio con riguardo all'uso di sistemi d'arma letali autonomi (*Lethal autonomous-weapons systems*, Laws)⁵⁹. L'obiettivo dell'IA è infatti migliorare la capacità di osservare, orientarsi, decidere e agire (*Observe, Orient, Decide, Act*, ciclo Ooda) in modo più rapido e accurato rispetto all'avversario, garantendo un vantaggio decisionale, nel rispetto delle normative vigenti – e.g. diritto internazionale umanitario (principio di *lawfulness*)⁶⁰. Ad oggi, l'approccio ucraino e Nato è stato quello di mantenere la decisione d'ingaggio e valutazioni strategiche sotto il controllo umano (Hitl),

⁵⁵ International Institute for Strategic Studies, "Big Data, Artificial Intelligence and Defence", cit., p. 3.

⁵⁶ Intervista del 2 febbraio 2026 (1) e (2).

⁵⁷ Rashid, Adib Bin et al., "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges", in *International Journal of Intelligent Systems*, 2023, articolo 8676366, <https://doi.org/10.1155/2023/8676366>; Vold, Karina, "Augmenting Military Decision Making with Artificial Intelligence", in *Cambridge Forum on AI: Law and Governance*, vol. 1 (2025), articolo e48, <https://doi.org/10.1017/cfl.2025.10022>.

⁵⁸ Intervista del 12 giugno 2026.

⁵⁹ International Institute for Strategic Studies, "Big Data, Artificial Intelligence and Defence", cit., p. 4.

⁶⁰ Intervista dell'11 febbraio 2026; Borchert, Heiko et al. (a cura di), *The Very Long Game: 25 Case Studies on the Global State of Defense AI*, Cham, Springer, 2024, <https://doi.org/10.1007/978-3-031-58649-1>; Jensen, Benjamin e Yasir Atalan, "The Pentagon's AI Problem Isn't Algorithms, It's Evaluation", in *CSIS Commentaries*, 19 dicembre 2025, <https://www.csis.org/node/120004>.



nonché la possibilità da parte dell'operatore di intervenire sulle funzioni autonome e di sovrascriverne le decisioni (principio di *governability*)⁶¹. Va, tuttavia, tenuto presente che in molti casi l'operatore umano avrà un arco di tempo molto limitato per prendere le decisioni, sotto la pressione degli eventi e della minaccia, e questo potrebbe portare ad affidarsi maggiormente alle opzioni raccomandate dall'IA.

In questo contesto, una delle sfide più rilevanti rimane il confronto con avversari che non condividono il medesimo approccio normativo e operativo all'impiego dell'intelligenza artificiale in ambito militare. Da un lato la Nato, già con la suddetta strategia IA del 2021 e i sei principi, e un gruppo ancora più ampio di Paesi con la Dichiarazione politica sull'uso militare responsabile dell'IA e dell'autonomia⁶² presentata dagli Stati Uniti al vertice sull'uso responsabile dell'IA in ambito militare (*Responsible AI in the Military Domain*, Reaim) dell'Aia del 2023, hanno cercato di promuovere standard condivisi per un uso responsabile dell'IA. Dall'altro lato, attori come Russia e Cina non hanno aderito a tali iniziative, mantenendo una posizione di maggiore ambiguità nella demarcazione tra supporto e autonomia nell'uso della forza da parte dell'IA⁶³. In una prospettiva storica più ampia, con lo sviluppo di sistemi d'arma sempre più sofisticati e con la maggiore capacità di *data fusion*, il confine tra intervento umano e automazione⁶⁴ ha continuato a variare, e l'IA sposta semplicemente più in avanti il punto in cui si inserisce la decisione umana all'interno del processo decisionale.

Il controllo effettivo sulle capacità di un sistema IA dipende inoltre dalla possibilità di sviluppare, addestrare e governare in maniera autonoma il modello. Da qui emerge il tema della sovranità tecnologica, che riguarda non soltanto l'algoritmo in sé, ma anche il controllo sui dati utilizzati per l'addestramento e sulle infrastrutture necessarie al suo funzionamento⁶⁵.

Lo sviluppo dell'algoritmo in maniera autonoma, oppure il suo *fine tuning* per attagliare il modello alle specifiche esigenze militari accettando però un grado di dipendenza tecnologica, rappresentano il principale ambito in cui può esercitarsi un effettivo controllo sovrano sul sistema⁶⁶. In tal modo si possono inserire i vincoli etici e/o giuridici, le dottrine che ne modellano il funzionamento⁶⁷, garantendo così trasparenza dell'algoritmo (principio di *explainability*) e tracciabilità delle valutazioni del sistema (principio di *traceability*).

L'efficace addestramento del modello presenta due principali difficoltà: la necessità di enormi volumi di dati e la disponibilità di infrastrutture adeguate a soddisfare l'elevata capacità computazionale e energetica richiesta⁶⁸. Il buon funzionamento di un sistema IA dipende in primo luogo dalla qualità e dalla quantità dei dati sui quali viene addestrato, il che presuppone una profonda digitalizzazione dei dataset rilevanti della difesa ai fini dell'IA, resi omogenei e fruibili sulla base di un alto livello di qualità del dato, nonché la capacità

⁶¹ Bondar, Kateryna, "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare", in *CSIS Reports*, marzo 2025, <https://www.csis.org/node/114918>.

⁶² Stati Uniti, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, 16 febbraio 2023, <https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy>.

⁶³ Ibid.; Javadi, Mahmoud e Michal Onderco, "What Does Global Military AI Governance Need?", in *ELN Commentaries*, 2 febbraio 2024, <https://europeanleadershipnetwork.org/?p=21545>.

⁶⁴ Automazione e autonomia non coincidono. Un sistema automatizzato esegue una funzione predefinita secondo regole stabilite dall'uomo, mentre un sistema autonomo è in grado di percepire l'ambiente, elaborare informazioni e prendere decisioni con un grado variabile di indipendenza. Un sistema d'arma automatico, automatizza l'ingaggio del bersaglio una volta attivato dall'operatore, ma non decide autonomamente se iniziare l'azione. Un sistema d'arma autonomo, invece, sarebbe capace di selezionare, identificare e ingaggiare bersagli senza intervento umano diretto nel ciclo decisionale.

⁶⁵ Intervista del 23 febbraio 2026.

⁶⁶ Ad oggi i paesi con un modello Llm di base nazionale sembrano essere Usa, Cina, Russia e Francia. Intervista del 19 febbraio e del 2 febbraio 2026 (1).

⁶⁷ Ad oggi dottrine e modalità di ingaggi non fanno ancora parte del patrimonio conoscitivo dell'IA, per cui l'approccio Hitl rimane necessario. Intervista dell'11 febbraio, del 19 febbraio e del 3 marzo 2026.

⁶⁸ Intervista del 23 febbraio 2026.



di prevenire manipolazioni o contaminazioni esterne⁶⁹. Con riferimento ai dati, anche i meccanismi di addestramento hanno un ruolo centrale: impiegare *large language models* (Llm) per generare dati sintetici o feedback utilizzati nell'addestramento di altri Llm può accelerare e rendere più efficiente il processo automatizzandolo, ma introduce anche rischi legati alla possibile propagazione di errori e bias già presenti nel modello generatore e alla riduzione del controllo sulla qualità e sulla provenienza del dataset⁷⁰. O ancora, approcci basati sull'addestramento permanente del modello IA distribuito su assetti diversi produrrebbero una proliferazione di modelli divergenti, perché addestrati su dati eterogenei, con il risultato di generare sistemi che rispondono in modo diverso agli input esterni⁷¹. Per tali ragioni è per molti aspetti preferibile un modello di addestramento periodico e centralizzato, in cui un ente responsabile, il proprietario dell'infrastruttura o un'autorità designata coordina l'addestramento e il conseguente aggiornamento del modello. In tale contesto, la difesa italiana è indietro circa la sua completa digitalizzazione e popolazione del dataset, e non dispone attualmente di piena autonomia infrastrutturale in termini di modello, cloud e *High performance computing* (Hpc) nazionali⁷².

Presupposto essenziale per lo sviluppo dell'IA per il C2 militare è quindi la costruzione del dataset al livello interforze, che deve quindi passare per la digitalizzazione e l'interoperabilità trasversale dei dati tra le diverse Forze armate⁷³. La difesa italiana, nonostante l'uso di alcune piattaforme complesse e altamente digitalizzate, nel complesso è stata storicamente caratterizzata da una limitata propensione alla digitalizzazione delle informazioni⁷⁴. Lo stato della digitalizzazione non è omogeneo tra Forze armate, né tra ambienti più specialistici, come per esempio l'intelligence che fa uso di strumenti avanzati di analisi dati, e il resto dello strumento militare⁷⁵.

L'IA rappresenta quindi un abilitatore trasversale per tutte le piattaforme connesse, configurandosi come uno strumento unificante del sistema informativo e dell'architettura operativa interforze e in prospettiva di coalizione⁷⁶. Se da un lato questo comporta un aumento dell'efficienza, dall'altro comprime l'autonomia delle singole Forze armate, che non possono più operare attraverso sistemi chiusi, spesso duplicati, in favore di un ruolo necessariamente più forte dello Stato Maggiore della Difesa, producendo effetti in tutti i domini, indipendentemente dai rapporti gerarchico-funzionali. In questa prospettiva, accanto al cambiamento della dimensione tecnologica, l'efficace adozione dell'IA nelle Forze armate italiane beneficerebbe anche dall'adeguamento del quadro normativo e organizzativo della difesa, già modificato con la riforma Di Paola sulla struttura dei vertici, verso un'ulteriore progressiva centralizzazione e rafforzamento dello Stato

⁶⁹ È essenziale lavorare sulla qualità del dato. I meccanismi di pulizia del dato possono anch'essi essere assistiti dall'IA, ad esempio tramite modelli che confrontano risultati, scartano deviazioni e mantengono una maggiore coerenza del dataset. Intervista dell'11 febbraio e del 13 febbraio 2026.

⁷⁰ I dati costituiscono il fondamento su cui un sistema IA apprende e opera, elaborandoli per produrre risultati utili all'utente. Nel caso degli Llm, il modello non elabora direttamente il significato delle parole, bensì rappresentazioni numeriche di token testuali. Essi apprendono regolarità statistiche nelle sequenze linguistiche, utilizzando per prevedere il token successivo e generare testi coerenti. Per gli esseri umani le parole rimandano a una realtà conosciuta attraverso l'esperienza e il contesto, mentre gli Llm non possiedono tale esperienza e quindi per il modello le parole rappresentano solo parole, non corrispondendo a nient'altro. Esse sono solo un mezzo che consente al modello IA di manipolare la sua "realtà" – fatta esclusivamente di parole – per fornirci un risultato coerente dal punto di vista linguistico. Tuttavia, poiché un Llm non dispone di un'esperienza diretta del mondo reale né di un meccanismo di verifica delle proprie affermazioni rispetto alla realtà esterna, i contenuti generati possono risultare fattualmente inesatti o errati. Per questa ragione, durante il training, se una quota eccessiva dei dati di addestramento è costituita da contenuti sintetici generati da altri Llm, il modello può degradare progressivamente la qualità delle informazioni generate. Tale fenomeno è noto in letteratura come collasso del modello. Intervista del 19 febbraio 2026; Shumailov, Ilia et al., "AI Models Collapse when Trained on Recursively Generated Data", in *Nature*, vol. 631 (2024), p. 755-759, <https://doi.org/10.1038/s41586-024-07566-y>; Wyllie, Sierra et al., "Fairness Feedback Loops: Training on Synthetic Data Amplifies Bias", in *FACCT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, giugno 2024, p. 2113-2147, <https://doi.org/10.1145/3630106.365902>.

⁷¹ Intervista del 2 febbraio 2026 (1).

⁷² Ibid.

⁷³ Intervista del 23 febbraio 2026.

⁷⁴ Ibid.

⁷⁵ Ibid.

⁷⁶ Intervista del 16 gennaio 2026.



Maggiore della Difesa – nelle funzioni di coordinamento, pianificazione, definizione di linee guida, policy, standard e strategie e C2 – al fine di garantire coerenza ed evitare frammentazioni eccessive.

Oltre che sul piano tattico e operativo, anche su quello organizzativo il supporto dell'IA ai processi decisionali e di pianificazione ha come prerequisito fondamentale l'accesso a informazioni digitalizzate e organizzate in dataset completi e sistematicamente aggiornati quanto personale, infrastrutture, mezzi e relativo stato operativo, al fine di ottimizzare l'impiego delle risorse umane e materiali⁷⁷.

Poiché la preparazione di dataset adeguati richiede una semplificazione e digitalizzazione delle Forze armate, esso solleva interrogativi rilevanti in termini di accesso, governance e titolarità delle informazioni, ed espone inevitabilmente a rischi di cybersicurezza. Rappresentando il dominio cyber il principale vettore di attacco contro sistemi digitali, lo sviluppo delle capacità IA e cyber deve necessariamente procedere in sinergia.

4. IA e difesa cyber

In Italia, l'approccio alla cybersicurezza si sta progressivamente strutturando secondo una logica interministeriale e interforze. La creazione dell'Agenzia per la cybersicurezza nazionale (Acn) rappresenta il tentativo di costruire un perimetro cyber nazionale più organico e centralizzato. Tuttavia, il processo è ancora in fase di consolidamento e permane una significativa frammentazione organizzativa. In particolare, nonostante la presenza del Comando Operazioni in Rete (Cor) a vocazione interforze, il settore cyber della difesa continua a vedere una certa duplicazione di strutture e competenze tra le diverse Forze armate⁷⁸. Se infatti il Cor gestisce il nucleo centrale dell'infrastruttura digitale della difesa (Difenet), le singole diramazioni decentralizzate rimangono in capo alle rispettive Forze armate⁷⁹. Nonostante, quindi, l'informazione costituisca il vero centro di gravità dell'IA e del dominio cyber, tale frammentazione genera dispersione informativa e rallenta il coordinamento operativo, minandone l'efficacia.

In un contesto che vede l'Italia primo obiettivo per numero di attacchi cyber subiti in Europa e quarta al livello mondiale, con il 10 per cento di tutti gli attacchi registrati a livello globale⁸⁰, e in cui attori statali come Russia, Cina, Iran e Corea del Nord intraprendono azioni di guerra ibrida⁸¹, un ulteriore elemento di debolezza della struttura operativa italiana in materia di cybersicurezza riguarda il limite, imposto per legge, alle capacità difensive cui le Forze armate e in particolare il Cor devono attenersi. Vi è una consapevolezza istituzionale diffusa circa la necessità di riconoscere lo spazio cyber come dominio "di interesse nazionale per la difesa e la sicurezza dello Stato"⁸² e di rafforzare il perimetro della cybersicurezza nazionale, come esplicitato nel non-paper sulla guerra ibrida del ministro della Difesa Guido Crosetto che punta peraltro a istituire una *cyberforce* dedicata, definita "Arma Cyber"⁸³, dotata anche del potere di intraprendere operazioni offensive e di contro-attacco. Tuttavia, resta l'assenza, ad oggi, del mandato legale per sviluppare capacità di difesa attiva, e men che meno offensive o di contrattacco, il che continua a limitare significativamente la capacità della Difesa di operare efficacemente nel dominio cyber⁸⁴.

⁷⁷ Interviste dell'11 febbraio e del 23 febbraio 2026.

⁷⁸ Intervista del 13 febbraio 2026.

⁷⁹ Ibid.

⁸⁰ International Trade Administration, *Italy Country Commercial Guide: Cybersecurity*, aggiornamento al 3 febbraio 2026, <https://www.trade.gov/country-commercial-guides/italy-cybersecurity>.

⁸¹ Ministero della Difesa, *Il contrasto alla guerra ibrida: una strategia attiva*, novembre 2025, https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf.

⁸² Ibid.

⁸³ Ibid.; Tessari, Paola, "Il contrasto alla guerra ibrida, nuova priorità della difesa italiana", in *Affari Internazionali*, 16 dicembre 2025, <https://www.affarinternazionali.it/?p=115482>.

⁸⁴ Intervista del 13 febbraio 2026.



Inoltre, i più recenti sviluppi dell'IA nel dominio cyber alimentano crescenti preoccupazioni circa le sue potenziali implicazioni per la sicurezza nazionale. Emblematico, al riguardo, è il caso dei modelli più avanzati sviluppati da Anthropic, che hanno suscitato timori in merito al loro possibile impiego per l'identificazione di vulnerabilità e la conduzione di azioni *cyber offensive*, per cui l'azienda ha dovuto sospendere l'utilizzo a tutti i suoi clienti dopo che Washington ha imposto restrizioni alla loro diffusione e commercializzazione⁸⁵. In questo contesto di costante progresso tecnologico, l'IA funge infatti da acceleratore e moltiplicatore della minaccia cyber, abbassando la soglia d'accesso da parte degli avversari e consentendo anche ad attori meno sofisticati di sviluppare capacità offensive significative⁸⁶. A maggior ragione, dato l'impatto dell'IA nel dominio cyber, ambiente di per sé caratterizzato da assenza di confini geografici, difficoltà di attribuzione, velocità e continua evoluzione delle tecniche avversarie, una postura difensiva esclusivamente passiva è insufficiente a garantire la sicurezza delle infrastrutture digitali della difesa e delle infrastrutture critiche civili⁸⁷. L'attuale quadro normativo italiano e il suo forte orientamento etico sono elementi che limitano la capacità operativa, soprattutto rispetto ad attori che adottano approcci meno vincolati da norme o principi di responsabilità. In questo senso, le esercitazioni Nato costituiscono un'opportunità importante per l'Italia, che possiede maggiori vincoli normativi rispetto ad altri Paesi partner, per testare almeno in quel contesto le proprie capacità cyber⁸⁸.

L'impiego dell'IA offre al tempo stesso enormi vantaggi difensivi, permettendo agli analisti di concentrarsi su un numero ridotto di eventi rilevanti grazie a sistemi di filtraggio automatico e identificazione delle anomalie⁸⁹. Costituendo la velocità l'elemento distintivo di questo dominio, con tempi di reazione che si misurano in millisecondi, l'intervento umano rischia giocoforza di rappresentare un collo di bottiglia e quindi uno svantaggio piuttosto che un vantaggio⁹⁰. L'IA offre un vantaggio in chiave di difesa attiva e contrattacco in termini di individuazione delle vulnerabilità avversarie e generazione di *payload* malevoli. Tuttavia, i modelli di IA commerciali sono spesso soggetti a vincoli etici e tendono quindi a limitare la produzione diretta di codice offensivo⁹¹. In tale cornice, il preposizionamento, la preparazione delle risorse e responsabilità per rispondere, e la presenza persistente nelle reti avversarie sono essenziali, attraverso per esempio l'identificazione preventiva di minacce e target⁹². Da notare infine che la generazione di codice offensivo è importante anche in termini difensivi, permettendo l'addestramento sia dei modelli sia degli operatori attraverso l'utilizzo di *cyber range*, ambienti simulati in cui è possibile riprodurre infrastrutture critiche, scenari operativi e attacchi realistici appunto per finalità di addestramento e sperimentazione⁹³.

Come accennato in precedenza, la progressiva digitalizzazione dei processi rappresenta il prerequisito fondamentale per l'adozione dell'IA: senza dataset completi, aggiornati e sistematicamente digitalizzati, gli applicativi non possono funzionare efficacemente⁹⁴. Vista la continua evoluzione della minaccia cyber e il ruolo che l'IA gioca al riguardo, la protezione di questi dati non si realizza attraverso la chiusura al mondo

⁸⁵ Dey, Mrinmay et al., "Anthropic Disables Top-Tier AI Models after US Order Limiting Foreign Access", in *Reuters*, 13 giugno 2026, <https://www.reuters.com/technology/us-blocks-foreign-access-anthropics-most-advanced-ai-models-axios-reports-2026-06-13>; Chia, Osmond, "Anthropic Says US Lifts Export Ban on Its Advanced AI Tools", in *BBC*, 1 luglio 2026, <https://www.bbc.com/news/articles/cdr42623e1do>.

⁸⁶ Kabir, Md Humayun et al., "A National-Scale AI-Driven Cyber Defense Framework for Protecting U.S. Critical Infrastructure Against Nation-State Attacks", in *Journal of Computer Science and Technology Studies*, vol. 8, n. 6 (2026), p. 94-107, <https://al-kindipublishers.org/index.php/jcsts/article/view/12628>; Kshetri, Nir, "Transforming Cybersecurity with Agentic AI to Combat Emerging Cyber Threats", in *Telecommunications Policy*, vol. 49, n. 6 (2025), articolo 102976, <https://doi.org/10.1016/j.telpol.2025.102976>; Intervista del 13 febbraio 2026.

⁸⁷ Intervista del 13 febbraio 2026.

⁸⁸ Ibid.

⁸⁹ Il triage automatico classifica gli alert come benigni, sospetti o critici e ha accuratezza superiore al 99 per cento. Braccioli, Marco, "Come l'IA ha trasformato la difesa di Washington", in *Airpress*, n. 175, marzo 2026; Intervista del 13 febbraio 2026.

⁹⁰ Intervista del 2 marzo 2026.

⁹¹ Intervista del 13 febbraio 2026.

⁹² Ibid.

⁹³ Interviste del 13 febbraio e del 2 febbraio 2026 (2).

⁹⁴ Interviste dell'11 febbraio e del 23 febbraio 2026.



digitale e al cloud, bensì mediante una valutazione del rischio. Questa si basa su un'analisi costi-benefici delle misure di mitigazione che tenga conto di risorse e tempo disponibili, nonché di vantaggi e svantaggi derivanti dall'impiego o no delle tecnologie digitali. La sovranità digitale deve conciliarsi con la capacità di valorizzare le informazioni come risorsa operativa, trasformandole in un fattore di vantaggio tramite l'IA, e garantendone al contempo l'integrità, disponibilità e difesa dagli avversari. In questa prospettiva, l'efficacia del modello dipende dalla condivisione dei dati e dalla loro interoperabilità, accettando un livello strutturalmente inevitabile di rischio.

Il rischio zero non esiste, né nel caso in cui la decisione ricada in capo all'essere umano né quando essa sia affidata a sistemi di IA. Parimenti, non è possibile assicurare un livello di sicurezza tale da escludere in modo assoluto il rischio di manipolazione (*poisoning*) o esfiltrazione dei dati, siano essi digitali o fisici. Tale rischio, perciò, può e deve essere mitigato, riducendone l'impatto a un livello accettabile, senza però compromettere e sacrificare i benefici derivanti dall'impiego di tecnologie come l'IA, la cui assenza ridurrebbe significativamente la capacità operativa delle Forze armate. La tecnologia, in questo senso, non elimina il rischio di perdita di dati o di errore nel processo decisionale, ma permette di ridurli, grazie alla possibilità di fondare le decisioni su una maggiore quantità di informazioni a disposizione, aumentandone quindi al contempo qualità e rapidità. Il tutto richiede però una formazione adeguata del personale militare.

5. IA e gestione delle risorse umane

L'efficace adozione e integrazione di sistemi basati sull'IA nella difesa richiede quale condizione essenziale la formazione e l'aggiornamento del personale militare rispetto alla nuova modalità organizzativa e operativa. Questa rappresenta oggi una delle principali sfide della Difesa italiana, poiché riguarda la costruzione di un ecosistema organizzativo e culturale consapevole del funzionamento dei sistemi IA. La comprensione a grandi linee dei principi di funzionamento dell'IA, una forma quindi di "alfabetizzazione" rispetto a tale tecnologia, è necessaria al fine di aumentare la consapevolezza del personale delle Forze armate sulle azioni da attuare per assicurarne un funzionamento responsabile, efficace ed efficiente. La sfida in questo ambito è duplice.

La prima sfida riguarda il personale che nelle diverse articolazioni della Difesa sarà in varia misura impegnato nella definizione degli algoritmi, nel rapporto con fornitori privati di soluzioni IA, nel procurement, manutenzione o logistica di assetti che sono abilitati dall'IA, piuttosto che nella stessa governance dell'IA prevista dalla strategia della Difesa (vedasi capitolo sei). Tale personale ha bisogno di maggiori e più approfondite competenze scientifiche avanzate (*Science, technology, engineering and mathematics*, Stem). Padroneggiare il funzionamento dell'IA consentirebbe agli operatori di comprendere, plasmare e governare gli algoritmi come uno strumento al servizio del decisore, permettendogli al contempo di comprendere i limiti, i bias e le logiche di funzionamento dei sistemi dotati di IA. Entrambe le sfide costituiscono per la Difesa anche l'opportunità di orientare la formazione a diffondere una più solida cultura tecnologica e un approccio maggiormente orientato all'innovazione, di cui beneficerebbe tutto lo strumento militare⁹⁵.

La seconda sfida riguarda il complesso di ufficiali e sottoufficiali che useranno l'IA per prendere decisioni al livello strategico, operativo e tattico, e devono quindi essere maggiormente formati per mantenere una adeguata capacità di valutazione delle informazioni fornite, degli scenari proposti e delle opzioni suggerite, così da prendere decisioni consapevoli e mediamente migliori. Ciò richiede sia una solida formazione di base, in particolare nelle accademie militari, sia un periodico aggiornamento professionale per un impiego adeguato ed efficace dell'IA. La fiducia in tali sistemi dipenderà dalla capacità degli operatori di comprenderne i meccanismi decisionali, dove tende a sbagliare e perché, e di valutarne criticamente gli output. Nonostante

⁹⁵ Interviste dell'11 febbraio e del 2 febbraio 2026 (2).



la tentazione di attribuire alla macchina una superiorità decisionale automatica, è necessario preservare la capacità umana di valutare, correggere e decidere. La formazione deve dunque rafforzare la cultura del comando, non indebolirla, evitando che gli operatori divengano meri esecutori delle indicazioni prodotte dalla macchina e che abbiano la forza e la legittimità di andare anche contro le linee d'azione proposte per esempio da un sistema di C2 alimentato dall'IA. La responsabilità della decisione ultima deve restare umana, poggiando sulla comprensione delle capacità e dei limiti dell'IA. In questo contesto, emerge una crescente attenzione alla dimensione cognitiva del conflitto odierno, nella quale le attività di disinformazione e controinformazione sono strumenti attraverso cui gli avversari cercano di influenzare percezioni, decisioni e consenso politico⁹⁶. Oltre ai domini tradizionali, infatti, la Difesa è oggi chiamata a operare in uno spazio che comprende dimensioni digitali, cibernetiche, informative e cognitive, nelle quali infrastrutture critiche, flussi informativi e percezioni pubbliche assumono un'importanza crescente⁹⁷. La capacità di distinguere informazioni affidabili da contenuti poco attendibili rappresenta una difficoltà concreta all'interno delle Forze armate come della società italiana di cui fanno parte e in cui sono immersi, dove la consapevolezza delle implicazioni strategiche dell'IA non è uniformemente diffusa⁹⁸. L'avvento dell'IA rafforza ulteriormente l'esigenza di una formazione equilibrata tra discipline ingegneristiche, insegnamenti militari e corsi umanistici, a indirizzo filosofico, con l'obiettivo di sviluppare consapevolezza e capacità di discernimento. L'iniziativa dell'Esercito di aggiornare la sua offerta formativa per la futura classe dirigente con un corso in scienze strategiche a indirizzo filosofico, introducendo temi quali l'etica delle tecnologie, il dual-use, il rapporto tra conoscenza naturale e digitale, riflette la consapevolezza che l'esercizio del comando non richieda soltanto competenze tecniche, ma anche capacità di pensiero critico, ragionamento autonomo e interpretazione della complessità, evitando la formazione di semplici esecutori e favorendo invece la capacità di valutare criticamente informazioni e ordini e di prendere decisioni⁹⁹. Piuttosto che trasmettere competenze legate a singoli strumenti IA destinati a evolversi rapidamente, che pure sono necessarie, la formazione mira a sviluppare le capacità cognitive di ragionamento necessarie per porre le domande corrette, valutare criticamente i risultati prodotti dagli algoritmi (*critical thinking*) e quindi mantenere il controllo decisionale umano.

La formazione del personale militare rispetto all'IA deve comunque confrontarsi con la gestione delle risorse umane nella Difesa, comprese le progressioni di carriera. In Italia, a causa di vincoli normativi circa organici e pensionamenti, il raggiungimento delle posizioni apicali avviene mediamente con sei-sette anni di ritardo rispetto ad altri Paesi Nato, il che incide direttamente sulla capacità di cogliere e integrare l'innovazione tecnologica, che tende fisiologicamente a ridursi con l'età¹⁰⁰. Il meccanismo di rotazione degli incarichi e più in generale la gestione di risorse umane non favorisce inoltre al momento percorsi specializzanti sulla stessa funzione o aspetto della difesa, e questo rende difficile la formazione e l'aggiornamento di specialisti dove servono, e in particolare di specialisti di IA. In termini organizzativi, la capacità istituzionale di identificare per tempo le figure destinate a occupare determinati incarichi e provvedere quindi alla loro preparazione, sia essa di carattere specialistico o generalista, assume un'importanza crescente.

Mentre la formazione del personale per una migliore adozione dell'IA è una sfida, viceversa l'introduzione dell'IA a supporto del sistema formativo delle Forze armate è un'opportunità. Di fatto rientrano tra le priorità dell'Esercito la digitalizzazione della formazione, l'alfabetizzazione all'uso dell'IA, nonché la dronizzazione della forza armata¹⁰¹. L'IA potrebbe, infatti, contribuire a migliorare la qualità del training, attraverso per esempio la costruzione di scenari, simulazioni e *wargaming* basati su realtà virtuale e

⁹⁶ Intervista del 26 maggio 2026 (1).

⁹⁷ Intervista del 26 maggio 2026 (2).

⁹⁸ Intervista del 2 febbraio 2026 (2).

⁹⁹ "Filosofia ai militari, accordo tra Accademia e Università di Modena", in *Ansa*, 16 dicembre 2025, https://www.ansa.it/sito/notizie/cronaca/2025/12/16/filosofia-ai-militari-sara-in-un-percorso-di-scienze-strategiche_857e755f-c047-4e82-8a57-3d341d016077.html.

¹⁰⁰ Intervista del 2 febbraio 2026 (2).

¹⁰¹ Intervista del 26 maggio 2026 (1).



aumentata, migliori e più aggiornate esercitazioni cyber, percorsi di apprendimento personalizzati con un ciclo di valutazione e feedback più efficace e continuo grazie al supporto dell'IA¹⁰². Sempre nell'ambito del training, quest'ultima consente inoltre lo sviluppo di strumenti di pianificazione e simulazione delle conseguenze delle scelte operative che rafforzano il pensiero critico e la capacità di operare sotto pressione, migliorando le competenze decisionali, di comando e di pianificazione a lungo termine¹⁰³. Inoltre, l'introduzione di strumenti digitali e IA a supporto della didattica destinati sia a docenti che allievi contribuisce al processo di alfabetizzazione all'IA in tutti i percorsi formativi.

Il possibile supporto dell'IA a una migliore gestione del personale militare riguarda l'efficienza della sua allocazione tramite l'opportunità di automatizzare e delegare all'IA le attività ripetitive, burocratiche e a basso valore aggiunto, le cosiddette “*dull functions*”, consentendo di liberare un cospicuo numero di forze da impieghi amministrativi e concentrarle invece sull'addestramento e su compiti operativi e decisionali¹⁰⁴. Ciò a sua volta migliorerebbe la loro formazione e crescita professionale in senso più ampio. Tra queste “*dull functions*” amministrative rientra anche la stessa gestione delle risorse umane. Un sistema IA potrebbe supportare l'assegnazione degli incarichi e la distribuzione del personale a condizione di disporre di un dataset digitale completo, sistematicamente aggiornato e strutturato secondo criteri chiari di classificazione, tagging e organizzazione delle informazioni, relativo alle dotazioni organiche e fondato su dati che riflettano l'effettiva realtà operativa e non valori teorici definiti dalla normativa e riportati nelle tabelle ordinarie. Come precedentemente sottolineato per gli equipaggiamenti militari, in una gestione delle risorse umane supportata dall'IA, il divario tra rappresentazione formale e realtà operativa dovrebbe essere eliminato se si vuole evitare la distorsione del supporto fornito dall'IA, che diventa altrimenti inutile o dannoso. La trasformazione digitale richiede pertanto che il mondo digitalizzato coincida con quello reale, superando una consolidata cultura organizzativa e gestionale italiana in cui la dimensione formale tende spesso a prevalere sulla situazione operativa effettiva.

6. La Strategia della Difesa in materia di IA

Al di là delle differenti sensibilità istituzionali e organizzative, appare ormai diffusa la percezione che l'IA non costituisca un fenomeno transitorio, bensì una trasformazione strutturale destinata a ridefinire il funzionamento delle organizzazioni pubbliche e private, comprese le Forze armate. La consapevolezza dell'ineludibilità del cambiamento in atto, rafforzata dall'evoluzione della postura della Nato e dai processi strutturali di trasformazione delle difese in atto a livello alleato, non riguarda solo l'adozione di singole capacità o assetti, ma investe l'intera architettura organizzativa e operativa della difesa. La rapidità dell'innovazione tecnologica, l'evoluzione delle minacce e la crescente integrazione tra dimensione fisica, digitale e cognitiva impongono infatti una revisione delle competenze, dei processi e dei modelli organizzativi in essere. Da questa consapevolezza, diffusa sia ai vertici sia nei livelli operativi della Difesa, è derivata l'esigenza di sviluppare una visione strategica nazionale capace di orientare priorità e investimenti, al fine di evitare che iniziative frammentate e non coordinate producano risultati limitati rispetto alla portata delle trasformazioni in atto¹⁰⁵.

¹⁰² Intervista del 2 febbraio 2026 (2); Gaikwad, Rupali Rajesh e Aparna Sanjay Choudhary, “Integrating Artificial Intelligence into Military Education: Opportunities, Challenges, and Future Directions”, in *Journal of East-West Thought*, vol. 15, n. 1 (marzo 2025), p. 1317-1330, <https://jetjournal.us/index.php/journals/article/view/756>.

¹⁰³ Gaikwad, Rupali Rajesh e Aparna Sanjay Choudhary, “Integrating Artificial Intelligence into Military Education”, cit.; Dumitrașcu, Veronica, “Involvement of Youth in Political Life. A Vector of Democratic Resilience”, in *Proceedings of the 20th International Scientific Conference Strategies XXI*, 28 marzo 2024, p. 73-79, <https://www.researchgate.net/profile/Veronica-Dumitrascu-2/publication/380571261>.

¹⁰⁴ Intervista dell'11 febbraio 2026.

¹⁰⁵ Intervista del 26 maggio 2026 (2).



La Strategia della Difesa italiana in materia di IA pubblicata a febbraio 2026¹⁰⁶ è lo strumento che il vertice politico-strategico ha adottato per colmare un ritardo e un divario accumulati nello scorso decennio rispetto ad altri Paesi, alleati e non, nello sviluppo e nell'integrazione di questa tecnologia – un divario cui la stessa Strategia fa riferimento. La Strategia mira a dotare il Paese di una visione sistemica e di lungo periodo riguardo l'IA, capace di individuare priorità, orientare gli investimenti e definire obiettivi misurabili, evitando la frammentazione delle iniziative che spesso caratterizza il *modus operandi* italiano e favorendo una maggiore coerenza tra indirizzo politico e attuazione operativa. Con l'obiettivo di un'integrazione rapida, sistemica e sistematica dell'IA negli ambiti formativo, organizzativo e operativo, il livello di ambizione perseguito dalla Strategia è molto elevato, con tempi di attuazione stringenti, scadenze a uno, due e tre anni, che devono “necessariamente allinearsi al ritmo evolutivo di questa tecnologia”. L'obiettivo, comune ad altri aspetti della politica di difesa italiana portata avanti dal Governo di Giorgia Meloni e in particolare dal ministro della Difesa Guido Crosetto¹⁰⁷, è il conseguimento dell'autonomia strategica e della sovranità tecnologica.

Quest'ultimo obiettivo implica il mantenimento del controllo dell'IA durante tutto il ciclo di vita, attraverso un approccio al suo utilizzo che sia responsabile, etico e in linea con i principi del diritto internazionale umanitario. La piena autonomia gestionale dei modelli, dall'addestramento alla più generica comprensione dell'algoritmo, rappresenta una condizione necessaria per assicurare in modo consapevole il mantenimento della piena responsabilità umana sulle tecnologie impiegate. Per mantenere una totale libertà di azione e di modifica sull'algoritmo, ossia la capacità di modificarlo, alimentarlo e controllarlo, è necessario esserne proprietari¹⁰⁸. Per lo sviluppo, la validazione e la manutenzione dei modelli la Strategia prevede quindi di adottare un approccio “*in house*” oppure uno basato sul coinvolgimento della base industriale di riferimento, allorché vengano garantite “trasparenza e spiegabilità dei modelli, aggiornamento continuo, supervisione umana, interoperabilità e standardizzazione”¹⁰⁹. Sempre nell'ottica del raggiungimento dell'autonomia strategica, il documento prescrive, come requisito imprescindibile, il ricorso a una capacità di calcolo che dovrà risiedere presso infrastrutture di computazione proprietarie.

Particolare attenzione viene attribuita alla gestione del dato, considerato il vero fattore abilitante dell'IA: i dati devono essere raccolti, organizzati e resi fruibili e interoperabili affinché possano generare valore operativo. Per questo motivo, uno degli obiettivi consiste nel superare la tradizionale frammentazione informativa tra le diverse componenti della Difesa, favorendo la condivisione dei dataset e la costruzione di standard comuni¹¹⁰.

Al fine dello sviluppo della sovranità tecnologica nel settore IA, la Strategia individua quali assetti abilitanti le risorse umane qualificate (i cosiddetti talenti), i dati, gli algoritmi, la capacità di calcolo proprietaria (Hpc e *quantum computing*), e le reti sicure. Di conseguenza propone quattro aree di intervento per guidare l'integrazione dell'IA all'interno delle Forze armate: 1) operazioni, 2) contesti organizzativi, 3) formazione, addestramento e ricerca, 4) industria.

La Strategia invoca poi una revisione integrata della governance dell'IA per la Difesa articolata in un Ufficio per l'IA (Uia), organo politico-strategico di coordinamento, *policy*, supervisione e verifica, e un Laboratorio di IA per la Difesa (Liad), il braccio operativo che agisce in qualità di “*AI Delivery Center*” della Difesa. La scelta di istituire un'unità dedicata all'interno della Difesa per accelerare l'innovazione IA riflette un approccio

¹⁰⁶ Ministero della Difesa, *IA e Difesa. Strategia della Difesa in materia di intelligenza artificiale*, Edizione 2026, febbraio 2026, <https://www.difesa.it/primopiano/strategia-della-difesa-in-materia-di-intelligenza-artificiale/90297.html>.

¹⁰⁷ Si veda al riguardo, tra gli altri: Marrone, Alessandro, “Meloni's Defence Policy: Adjusting the Balance Sheet to Crises”, in *IAI Commentaries*, n. 26|16 (marzo 2026), <https://www.iai.it/en/node/21914>.

¹⁰⁸ Intervista del 2 marzo 2026.

¹⁰⁹ Ministero della Difesa, *IA e Difesa*, cit., p. 17.

¹¹⁰ Ibid., p. 37.



diffuso in un numero crescente di Paesi, rispetto ai quali la strategia fornisce un'utile analisi delle buone prassi e degli approcci ai quali ispirarsi. Il Liad, polo infrastrutturale di eccellenza, si inserisce in una più ampia strategia di rafforzamento dell'ecosistema nazionale dell'innovazione nel settore della difesa e delle tecnologie dual-use che mira a favorire il dialogo tra istituzioni, Forze armate, università, centri di ricerca e imprese, contribuendo così alla crescita di una filiera nazionale più integrata e competitiva. Questo ricalca il già operativo Polo Nazionale della Dimensione Subacquea, e agirebbe come aggregatore di competenze, *liaison* con il mondo industriale e accademico per costruire un ecosistema “*Defence Tech*” e favorire soluzioni innovative e il trasferimento dei risultati della ricerca alla Difesa¹¹¹. In questa prospettiva, il Laboratorio non rappresenta soltanto una struttura tecnica, ma anche uno strumento di governance dell'innovazione della Difesa. Concepito come uno strumento di coordinamento, sperimentazione e sviluppo delle capacità nazionali nel settore, il Liad nasce dalla consapevolezza che la sfida dell'adozione dell'IA non possa essere affrontata attraverso iniziative isolate da parte delle singole Forze armate, ma richieda invece una logica di sistema a favore della condivisione di competenze, infrastrutture, dati e soluzioni tecnologiche. Questo si configurerebbe come un ambiente virtuale comune nel quale sviluppatori, ricercatori, militari e partner industriali possono collaborare alla realizzazione di applicativi e servizi di interesse per l'intera Difesa¹¹². Il Laboratorio punta infatti a costruire un patrimonio condiviso di conoscenze, strumenti e soluzioni, riducendo la frammentazione degli investimenti e favorendo economie di scala. La logica è quella di un ecosistema aperto, nel quale quanto sviluppato da un soggetto possa essere riutilizzato, adattato e migliorato da altri, per obiettivi specifici o Forze armate diverse, accelerando il ciclo dell'innovazione e aumentando la reattività complessiva del sistema.

La disponibilità di dati classificati, sensibili o comunque difficilmente accessibili rappresenta uno degli assetti distintivi della Difesa e il principale fattore abilitante per lo sviluppo di applicativi IA militari specializzati. La sfida consisterà nel rendere accessibili ai sistemi IA, in modo coerente con le rispettive esigenze funzionali, i silos informativi stratificatisi nel tempo in applicazione del principio del “*need to know*”, superando la frammentazione del patrimonio informativo che ne è derivata¹¹³. Il valore aggiunto del Liad non risiede pertanto soltanto nella sua infrastruttura tecnologica che permette la collaborazione, ma nella capacità di mettere a disposizione delle migliori competenze del Paese i dati della Difesa¹¹⁴. In questo contesto, la sfida per il Laboratorio sarà creare le condizioni affinché tali dati possano essere utilizzati in sicurezza per finalità di addestramento, sperimentazione e sviluppo algoritmico.

Questa piattaforma sarà più efficace quanto più riuscirà a coinvolgere i giovani e le accademie, attraverso un approccio “*bottom-up*”. Mentre ad oggi le generazioni al vertice della Difesa hanno assistito alla trasformazione digitale, non essendone nativi, i futuri ufficiali e comandanti vivono e si formano in un contesto in cui il digitale costituisce già una componente naturale dell'ambiente personale, professionale e operativo. Per i giovani gli strumenti digitali, l'IA e l'automazione non rappresentano tecnologie emergenti da comprendere dall'esterno, bensì strumenti con cui interagiscono quotidianamente durante il proprio percorso formativo. Le nuove generazioni mostrano una maggiore predisposizione a sperimentare, apprendere e integrare strumenti digitali nei processi decisionali e organizzativi, contribuendo a ridurre le resistenze culturali che spesso accompagnano i processi di innovazione. Tale dinamica è particolarmente evidente nelle scuole di formazione della Difesa, dove crescono le iniziative, i progetti e le sfide legate alla programmazione, all'analisi dei dati e all'intelligenza artificiale¹¹⁵. La trasformazione in corso viene quindi percepita dai giovani ufficiali non come una rottura rispetto a un modello precedente, ma come una componente ordinaria del loro futuro professionale.

¹¹¹ Ibid.

¹¹² Intervista del 26 maggio 2026 (2).

¹¹³ Evento a porte chiuse del 25 giugno 2026.

¹¹⁴ Intervista del 26 maggio 2026 (2).

¹¹⁵ Terza conferenza sulle discipline Stem nella Difesa dal titolo “La sfida dell'intelligenza artificiale e la sicurezza comune”, organizzata dalla Scuola Navale Militare “Francesco Morosini” il 4 febbraio 2026.



La *governance* della difesa in materia di IA delineata dalla Strategia sarà a connotazione interforze sia al livello strategico-militare, con le aree tecnico-operativa e tecnico-amministrativa, sia al livello operativo e tattico con le loro articolazioni. Il documento indica anche la costituzione di un organo consultivo interno, composto da esperti militari e civili di etica e diritto, con il compito di promuovere l'uso responsabile dell'IA, in linea con i valori democratici al livello nazionale e internazionale.

In termini di risorse, si rimanda a una valutazione delle attuali linee di finanziamento, con particolare attenzione ai finanziamenti destinati ai “pilastri fondamentali” della formazione del personale e della digitalizzazione delle infrastrutture, e alla futura istituzione di un dedicato “Fondo per l'IA” nelle disponibilità del livello politico-strategico a sostegno dell'attuazione della strategia e dell'ecosistema IA del Paese. Nel frattempo, si indicano le limitate risorse già stanziare nel Piano Nazionale della Ricerca Militare¹¹⁶, nel Fondo Composito Difesa 2021¹¹⁷ e nel Fondo per l'attuazione dei programmi di investimento pluriennale per le esigenze della difesa nazionale¹¹⁸.

A corollario della visione strategica delineata nel documento, vengono poi definite 15 direttrici strategiche di intervento che costituiscono un quadro di riferimento preliminare per la pianificazione, il coordinamento e la valutazione dell'attuazione concreta della Strategia.

Considerata la rapidità di evoluzione della tecnologia, la Strategia è concepita come uno strumento dinamico e adattabile, sviluppato attraverso un processo partecipativo e soggetto a costanti aggiornamenti¹¹⁹. Questa si inserisce infatti tra due altri documenti strategici di indirizzo: il sopra citato non-paper sulla guerra ibrida e la Strategia Digitale della Difesa¹²⁰, anch'essa di recente pubblicazione. La Strategia sull'IA non è il punto di arrivo, ma costituisce una tappa importante di un percorso di trasformazione della difesa in direzione di un'adozione sistematica dell'IA che vedrà un altro passaggio fondamentale in un Piano Attuativo, aggiornabile nel tempo, per definire misure operative, responsabilità e *Key Performance Indicators* per il monitoraggio dell'attuazione della stessa. Il documento è previsto entro il 2026, insieme alla relativa direttiva ministeriale, e dovrebbe rappresentare un passaggio decisivo per continuare e velocizzare la trasformazione organizzativa e dei processi della Difesa in vista di un'adozione virtuosa dell'IA.

Conclusioni

L'adozione dell'IA nella Difesa italiana non rappresenta soltanto l'introduzione di una nuova tecnologia, ma una trasformazione strutturale del modo in cui le Forze armate osservano il contesto operativo, prendono decisioni e conducono le operazioni. Il principale valore aggiunto dell'IA risiede nella capacità di automatizzare processi, rafforzare la superiorità informativa e decisionale, e contribuire alla gestione della complessità rispetto sia ai domini operativi che allo sviluppo dello strumento militare. Già nel breve-medio periodo, tramite un'efficace introduzione dell'IA, la Difesa italiana può e deve ottenere significativi benefici in termini di intelligence, targeting, C2, operazioni multi-dominio, riconfigurazione di assetti *legacy*, integrazione di capacità IA “*edge*” nelle piattaforme in via di acquisizione, manutenzione predittiva e ottimizzazione della logistica, migliore e più efficiente gestione delle risorse umane e del procurement militare. In prospettiva, l'IA costituisce inoltre una tecnologia fondamentale per la transizione da sistemi automatizzati a sistemi progressivamente più autonomi, con implicazioni operative, organizzative ed etiche di ampia portata. Tale trasformazione complessiva impone, dunque, una riflessione più ampia sul

¹¹⁶ Ministero della Difesa, *IA e Difesa*, cit., p. 57.

¹¹⁷ Ibid.

¹¹⁸ Ibid., p. 58.

¹¹⁹ Intervista del 26 maggio 2026 (2).

¹²⁰ Ministero della Difesa, *Strategia digitale 2026-2030*, maggio 2026, <https://www.difesa.it/assets/allegati/strategia-digitale-della-difesa-2026-2030.2026.05.28.15.57.41.888.pdf>.



livello di ambizione nazionale rispetto allo sviluppo, all'acquisizione e all'integrazione delle capacità di IA, nonché sul significato di sovranità tecnologica.

In questo contesto, la sovranità non coincide necessariamente con lo sviluppo e il possesso integrale delle tecnologie, bensì con la capacità di mantenere il controllo sui nodi decisionali e sugli elementi critici che consentono di trasformare capacità tecnologiche in capacità operative. Ciò implica la necessità di interrogarsi sulla sovranità del dato, dell'infrastruttura e dell'algoritmo, individuando quali componenti debbano necessariamente rimanere sotto controllo nazionale e quali possano invece essere acquisite attraverso partnership industriali, nazionali e/o internazionali. In molti casi, infatti, sviluppare internamente ogni componente tecnologica risulta né realistico né economicamente sostenibile.

Uno degli elementi principali in cui l'esercizio della sovranità si concretizza è il dato. La qualità dell'IA dipende direttamente dalla disponibilità di dati digitalizzati, caratterizzati, affidabili, accessibili, condivisibili e interoperabili. In Italia, in aggiunta al ritardo accumulato nella digitalizzazione della Difesa, persistono ancora ostacoli culturali e organizzativi che limitano la valorizzazione del suo patrimonio informativo. La compartimentazione eccessiva delle informazioni, spesso giustificata da esigenze di classificazione o di gestione da parte delle singole Forze armate, produce l'effetto di rendere i dati difficilmente accessibili, riducendone il loro valore operativo. La retrosia al cambiamento e la limitata cultura della gestione del dato sono tra i principali vincoli all'adozione dell'IA per la Difesa italiana. La Difesa dovrebbe, dunque, muoversi verso un adeguato livello di digitalizzazione e una solida governance dei dati, compreso il completamento e l'aggiornamento costante delle banche dati per ridurre il divario tra la realtà operativa e quella che alimenta l'IA, in modo da trarre benefici significativi per lo strumento militare.

L'evoluzione tecnologica delle principali piattaforme in dotazione alla difesa, la cui capacità computazionale è progressivamente aumentata, evidenzia già oggi questa esigenza. Alcuni sistemi in servizio risultano oggi altamente digitalizzati, spesso in misura superiore rispetto alle stesse strutture C2 delle Forze armate. Tale divario rende evidente come l'introduzione di piattaforme avanzate debba fungere da fattore trainante per la digitalizzazione dell'intero ecosistema al loro supporto, senza il quale altrimenti il beneficio della piattaforma rimane di portata limitata. L'esempio dell'F-35 dimostra come l'acquisizione di una piattaforma digitale richieda inevitabilmente l'adeguamento di tutte le capacità che la supportano. Uno degli obiettivi al riguardo dovrebbe essere quello di disporre di librerie dinamiche all'interno dell'architettura cloud, aggiornabili in tempo reale e utilizzabili da tutte le piattaforme che dialogano e scambiano dati essendo connesse appunto allo stesso cloud¹²¹.

La trasformazione tecnologica portata dall'IA richiede una revisione dei modelli organizzativi della difesa per essere pienamente sfruttata. L'emergere di un ambiente operativo caratterizzato da una crescente trasparenza del campo di battaglia rafforza ulteriormente questa esigenza. La possibilità di rilevare, elaborare e condividere informazioni in tempo reale impone un adeguamento dei processi decisionali verso cicli sempre più rapidi se si vuole restare al passo con gli avversari che sfruttano le opportunità offerte dalla tecnologia. In questo contesto, una certa frammentazione delle responsabilità rallenta oggi molti processi decisionali. Il processo di integrazione interforze appare ancora incompleto e richiederebbe un'evoluzione ulteriore, anche attraverso una razionalizzazione delle strutture che sfrutti a pieno le potenzialità dell'IA.

Inoltre, la trasformazione tecnologica dell'IA rende inadeguati gli attuali modelli di investimento e acquisizione della Difesa. Il tradizionale approccio basato su acquisizioni *una tantum*, programmi pluriennali e aggiornamenti limitati dovrebbe evolvere nella direzione di cicli di acquisizione più agili e continui, basati su una prototipizzazione rapida (*fast prototyping*) e aggiornamenti (*add-on*) incrementali durante il ciclo di vita del sistema, con l'obiettivo di allinearli a quelli dell'evoluzione della tecnologia. La

¹²¹ Intervista del 23 febbraio 2026.



regolamentazione del codice degli appalti dovrebbe prevedere una procedura più adeguata al procurement militare, e in particolare per le tecnologie dell'informazione e della comunicazione, con modelli di sviluppo più agili o *fast track* dedicati, che vedano industria e Forze armate collaborare e sperimentare i prototipi in scenari realistici che replicano il campo di battaglia (*battlefield laboratories*) per misurarne l'efficacia in operazioni e non solo dal punto di vista ingegneristico, e procedere più velocemente verso la messa in servizio. Occorrerebbe anche adeguare i criteri di omologazione e certificazione alla realtà dell'IA che opera non in modo deterministico ma attraverso modelli probabilistici e inferenze statistiche, tenendo conto che i sistemi dotati di IA tendono a migliorare progressivamente attraverso l'impiego operativo, e quindi devono essere gestiti attraverso specifici strumenti di procurement e contrattualizzazione. Al tempo stesso, la Direzione Nazionale Armamenti e in generale la Difesa dovrebbero sfruttare le potenzialità dell'IA applicandola alla digitalizzazione della stazione appaltante, con un significativo beneficio in termini di efficienza e produttività a parità di risorse umane, di cui il procurement italiano ha sempre più bisogno visto l'ammodernamento in corso dello strumento militare. Costruendo sulle buone prassi e sulle iniziative avviate, si dovrebbe procedere rapidamente all'applicazione dell'IA agli aspetti gestionali delle Forze armate, dal procurement alla logistica, dalle risorse umane alle infrastrutture militari.

In generale, l'efficacia dell'introduzione dell'IA nella Difesa dipende anche dalla disponibilità di competenze informatiche adeguate. Le nuove capacità richieste dall'IA rendono necessario rafforzare l'expertise militare nelle discipline Stem, condizione imprescindibile per integrare efficacemente l'IA nelle Forze armate. In questo ambito, la Difesa potrebbe beneficiare della costruzione di canali di collaborazione strutturati con il mondo accademico e industriale, a partire dalle università e start-up, nelle quali si concentra la gran parte dei profili legati alla ricerca e all'innovazione. Permangono, tuttavia, importanti ostacoli burocratico-amministrativi che rendono complesse tali collaborazioni. L'introduzione di modalità di reclutamento e di percorsi di carriera nella difesa più flessibili e maggiormente permeabili con il settore civile potrebbe favorire la circolazione delle competenze tra quest'ultimo e la Difesa e contribuire ad aumentare la presenza di profili specialistici Stem, in linea con un approccio "*whole-of-society*". In generale, la Difesa deve investire maggiormente sulla formazione e aggiornamento del personale militare rispetto all'IA e alle nuove modalità operative e organizzative che questa tecnologia porta con sé. A sua volta, l'IA può contribuire a migliorare il training, e le Forze armate dovrebbero sfruttare le sue potenzialità, ad esempio per quanto riguarda la costruzione di scenari, simulazioni e *wargaming*, migliori e più aggiornate esercitazioni cyber, e, in generale, il processo di alfabetizzazione all'IA in tutti i percorsi formativi.

La riflessione sull'IA investe inevitabilmente anche il piano etico e giuridico. L'IA costituisce infatti una tecnologia abilitante per la transizione da sistemi automatizzati a sistemi sempre più autonomi, ma l'impiego di questi ultimi solleva questioni rilevanti in termini di affidabilità, responsabilità, vulnerabilità informatica e controllo umano. Tra i principali rischi vi sono malfunzionamenti, criticità nell'attribuzione della responsabilità per eventuali errori, possibilità di compromissione informatica e, soprattutto, progressiva riduzione del controllo umano sull'impiego della forza. Per tale ragione permane un ampio consenso sulla necessità che la decisione finale rimanga sempre affidata alla persona in divisa, con l'IA utilizzata quale strumento di supporto a un ciclo decisionale più rapido ma non sostitutivo della responsabilità umana.

Accanto agli aspetti normativi emerge inoltre una rilevante dimensione culturale. Mentre la responsabilità dell'operatore umano viene normalmente valutata *ex post*, nel caso dell'IA l'errore probabilistico del sistema è noto *ex ante* e viene implicitamente accettato già nella fase di progettazione. Questa diversa percezione e valutazione del rischio di errore generano una significativa resistenza culturale e giuridica, più accentuata nel contesto dell'Europa continentale che in quello anglosassone, il quale è più orientato a una gestione pragmatica del rischio e dell'incertezza. Tuttavia, il mantenimento di un controllo umano sull'IA non rappresenta soltanto un requisito giuridico, ma riflette una precisa scelta di valore. Sebbene



tale approccio possa apparire più restrittivo rispetto a quello di avversari come Russia e Cina non vincolati dagli stessi principi, esso rappresenta uno degli elementi distintivi delle democrazie liberali. Non a caso la Nato ha sviluppato un approccio basato sull'uso responsabile dell'IA con i sei principi già dal 2021. In questo senso, se da un lato tali vincoli possono comportare maggiori complessità operative, dall'altro essi costituiscono precisamente i principi e i valori che le democrazie intendono difendere.

Infine, la crescente dipendenza da infrastrutture digitali necessarie anche per l'introduzione dell'IA rende indispensabile rafforzarne la resilienza rispetto alle minacce cyber. L'IA funge infatti da acceleratore e moltiplicatore della minaccia, consentendo anche ad attori meno sofisticati di sviluppare capacità offensive significative. Dato l'impatto dell'IA nel dominio cyber, una postura difensiva esclusivamente passiva è insufficiente a garantire la sicurezza delle infrastrutture digitali della difesa, e bisognerebbe quindi adeguare il quadro normativo italiano per dare mandato al Cor di compiere attività costanti di difesa attiva e di contro-attacco. Al tempo stesso, i conflitti recenti hanno dimostrato come data center e infrastrutture digitali costituiscano ormai obiettivi prioritari delle operazioni militari cinetiche e la protezione di tali infrastrutture, anche rispetto a questo tipo di attacchi, diventa pertanto parte integrante della sicurezza nazionale.

In definitiva, l'adozione dell'IA nella Difesa italiana non dipenderà principalmente dalla disponibilità della tecnologia, seppure importante, bensì dalla capacità di sviluppare un ecosistema nazionale favorevole al suo impiego. Ciò richiede interventi coordinati su governance, capitale umano, dati, infrastrutture digitali e procurement. In questo contesto, la strategia della Difesa in materia di IA non è il punto di arrivo, ma costituisce una tappa importante di un percorso di trasformazione della difesa in direzione di un'adozione sistematica dell'IA che vede un altro passaggio fondamentale nel Piano Attuativo e nella relativa direttiva ministeriale, per muovere la Difesa verso un'adozione virtuosa dell'IA.



Acronimi

Acn	Agenzia per la cybersicurezza nazionale
Atr	Automatic target recognition
C2	Comando e controllo
C4isr	Command, control, communications, computers, intelligence, surveillance and reconnaissance
Cor	Comando Operazioni in Rete
Darb	Data and AI Review Board
Difenet	Infrastruttura digitale della difesa
Edt	Emerging and disruptive technology
Flor	First Line of Robots
Flot	First Line of Troops
Gcap	Global Combat Air Programme
Hitl	Human-in-the-loop
Hootl	Human-out-of-the-loop
Hotl	Human-on-the-loop
Hpc	High performance computing
IA	Intelligenza artificiale
Isr	Intelligence, surveillance and reconnaissance
Law	Lethal autonomous-weapons system
Liad	Laboratorio di IA per la Difesa
Llm	Large language model
Nato	North Atlantic Treaty Organization
Ooda	Observe, orient, decide, act
Rai	Responsible AI
Reaim	Responsible AI in the Military Domain
Stem	Science, technology, engineering and mathematics
TiC	Transforming in Contact
Uav	Unmanned aerial vehicle
Ugv	Unmanned ground vehicle
Uia	Ufficio per l'IA
Uuv	Unmanned underwater vehicle

L'Istituto Affari Internazionali (IAI) è un think tank indipendente, privato e non-profit, fondato nel 1965 su iniziativa di Altiero Spinelli. Lo IAI mira a promuovere la conoscenza della politica internazionale e a contribuire all'avanzamento dell'integrazione europea e della cooperazione multilaterale. Si occupa di temi internazionali di rilevanza strategica quali: integrazione europea, sicurezza e difesa, spazio, economia internazionale e governance globale, energia e clima, politica estera italiana; e delle dinamiche di cooperazione e conflitto nelle principali aree geopolitiche come Mediterraneo e Medioriente, Asia, Eurasia, Africa e Americhe. Lo IAI pubblica una rivista trimestrale in lingua inglese (*The International Spectator*), una online in italiano (*AffarInternazionali*), due collane di libri (*Trends and Perspectives in International Politics* e *IAI Research Studies*) e varie collane di paper legati ai progetti di ricerca (*Documenti IAI*, *IAI Papers*, ecc.).

Via dei Montecatini, 17
I-00186 Roma, Italia

T +39 06 6976831

www.iai.it



Ultimi Documenti IAI

Direttore: **Alessandro Marrone** (a.marrone@iai.it)

ISSN 2280-6164 | DOI 10.82088/IAIdoc2607

- | | |
|-----------|--|
| 26 07 | Andrea Grillo, Alessandro Marrone e Michele Nones, <i>Intelligenza artificiale e Difesa italiana: sfide e opportunità</i> |
| 26 06 | Alessia Chiriatti and Ettore Greco, <i>Sustainable Transitions and Competitiveness: Policy Directions for the European Union and Italy</i> |
| 26 05 | Federico Castiglioni and Luca Cinciripini, <i>The Future of European Defence: Industrial Ambition, Operational Constraints and Flexible Partnerships</i> |
| 26 04 | Matteo Bursi, Federica Marconi and Alessio Sangiorgio, <i>The Reshaping of the European Economic Sovereignty</i> |
| 26 03 | Karolina Muti (ed.), <i>Lessons for Europe and Italy from Other Space Powers: The Civil-Military Interconnection</i> |
| 26 02 | Alessia Chiriatti, <i>Unlocking Strategic Potential Outside the EU: Italy-Turkey Bilateral Partnership in Defence</i> |
| 26 01 | Elio Calcagno (ed.), <i>Taking Multi-domain Operations from Theory to Practice</i> |
| 25 15 | Luca Barana, Matteo Bursi and Luca Cinciripini, <i>How to Fund European Ambitions? Opportunities and Challenges for the Next MFF</i> |
| 25 14 | Federico Castiglioni, <i>Italy, Germany and Europe in Times of Geoeconomic Disorder</i> |
| 25 13it | Karolina Muti, Andrea Grillo, Sergio Marchisio e Michele Nones, <i>La proposta di EU Space Act: una prospettiva italiana</i> |