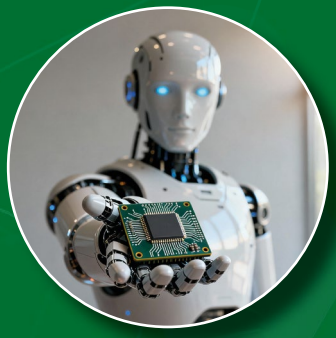
SCIENCE



TECHNOLOGY

ENGINEERING

MATHEMATICS

Le discipline STEM nella DIFESA

La sfida dell'Intelligenza Artificiale e la sicurezza comune

A cura di
Isabella RAUTI

LE DISCIPLINE STEM NELLA DIFESA

LA SFIDA DELL'INTELLIGENZA ARTIFICIALE E LA SICUREZZA COMUNE

Evento organizzato dal
Sottosegretario di Stato alla Difesa
Scuola Navale Militare " Francesco Morosini"
Venezia, 4 febbraio 2026

INDICE

Sottosegretario di Stato alla Difesa

Sen. Isabella RAUTI

Prefazione del Sottosegretario di Stato alla Difesa Sen. Isabella RAUTI

La Conferenza "Le discipline STEM nella Difesa", giunta alla sua 3^ edizione, si inserisce in un percorso ormai strutturato, promosso nell'ambito della "Settimana nazionale delle discipline scientifiche, tecnologiche, ingegneristiche e matematiche (STEM)", istituita con legge n. 187 del 24 novembre 2023. Questo nostro appuntamento annuale rappresenta un momento qualificato di riflessione, confronto e indirizzo strategico sul ruolo delle competenze STEM all'interno del sistema formativo e addestrativo della Difesa.

Fin dalla prima edizione dal titolo "Le discipline STEM nella Difesa", organizzata nel 2024 alla Scuola Militare "Teuliè" di Milano, l'iniziativa ha voluto valorizzare la formazione scientifica come leva fondamentale per affrontare le trasformazioni in atto negli scenari globali. La seconda edizione dal titolo "Le discipline STEM nella Difesa. Competenze abilitanti per gestire la complessità", ospitata nel 2025 dall'Istituto di Scienze Militari Aeronautiche di Firenze (ISMA), ha ampliato la partecipazione all'intera filiera formativa della Difesa, ponendo al centro il tema delle competenze abilitanti e della gestione della complessità.

La terza Conferenza, tenuta il 4 febbraio 2026 alla Scuola Navale Militare "Francesco Morosini" di Venezia, segna un ulteriore passo in questo percorso. Il tema scelto – "La sfida dell'Intelligenza Artificiale e la sicurezza comune" – evidenzia la centralità di una tecnologia trasversale e abilitante, destinata a incidere profondamente su tutti i domini operativi e decisionali. L'Intelligenza Artificiale è la regina delle tecnologie emergenti e rappresenta "la sfida delle sfide", integrando tutti gli strumenti più moderni, abilitando sistemi autonomi, supportando il decision making e favorendo l'interarabilità multidominio. La tecnologia quantistica ed i sistemi avanzati sono capacità enormi ma di settore, con l'Intelligenza Artificiale diventano capacità in grado di produrre vantaggio strategico.

In tale prospettiva, la sicurezza viene intesa nella sua accezione più ampia: non solo come compito funzionale della Difesa ma come dovere di garantire il bene comune, le Istituzioni, tutti i cittadini ed il sistema Paese nel suo complesso.

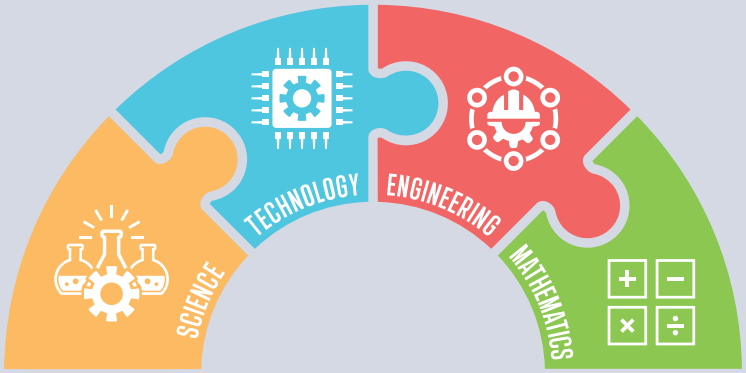
Gli Atti qui presentati restituiscono la ricchezza e l'articolazione dei contributi emersi nel corso dei lavori e documentano non solo lo stato dell'arte nelle riflessioni sulle discipline STEM nella Difesa ma anche la maturazione di una visione che riconosce nell'innovazione tecnologica una leva strategica da governare con consapevolezza e responsabilità.

Le nuove sfide richiedono competenze tecnologiche avanzate ed esigeranno crescenti capacità specialistiche ed una formazione in grado di interpretare le nuove minacce, i cambiamenti e gli scenari sempre più sofisticati. L'innovazione tecnologica non è neutrale, dipende dall'utilizzo consapevole; va governata,

orientata e messa al servizio dell'uomo e della Nazione.
L'Italia si è dotata di una strategia nazionale sulle tecnologie quantistiche con lead del Ministero dell'Università della Ricerca (MIUR), e con la partecipazione e la collaborazione di altri dicasteri come il Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI), la Difesa, il Ministero delle Imprese e del Made in Italy (MIMIT) e altre agenzie dello Stato. Un passaggio decisamente importante.
Parallelamente l'Italia ha adottato anche la prima legge nazionale sull'Intelligenza Artificiale (n.132 del 2025) che comprende molti elementi di prospettiva e di grande interesse. Ad esempio, evidenzia la potenzialità di alcuni rischi e la necessità di richiamare anche le Pubbliche Amministrazioni, non solo ogni singolo cittadino, ad un utilizzo consapevole e responsabile di questo strumento.
Più in generale, investire nella complessità della formazione STEM diventa una azione di "sistema Paese", capace di favorire l'accesso al mercato del lavoro in settori molto dinamici ad alto valore aggiunto, in cui si registra una notevole richiesta di professionalità con un gap tra "domanda e offerta" nonché un gender gap da colmare con la rimozione di stereotipi e pregiudizi.
Per utilizzare gli strumenti tecnologici secondo una responsabile visione etica è necessario intrecciare le discipline scientifiche e tecnologiche con i saperi umanistici e filosofici – le STEM con le STEAM - che hanno distinto la nostra millenaria civiltà. Solo coniugando le competenze tecniche e il pensiero critico è possibile governare e gestire l'innovazione, costruire il nuovo umanesimo tecnologico in cui l'IA, le tecnologie quantistiche e tutte quelle emergenti sono uno strumento imprescindibile al servizio dell'uomo; non lo sostituiscono, né debbono diminuire la sua capacità creativa.
Tale approccio antropocentrico ispira l'azione della Difesa, che mantiene al centro di ogni processo la risorsa umana, il soldato, la persona, l'operatore. Le discipline STEM sono centrali e cruciali per la Difesa, sono la leva strategica per la sicurezza nazionale, la chiave di accesso al mondo per comprenderlo nella sua complessità e per migliorarlo. Investire sulla formazione dei giovani in queste discipline significa rafforzare la sicurezza, tutelare il principio della libertà individuale e collettiva, favorire lo sviluppo tecnologico, economico ed occupazionale. Significa garantirsi un vantaggio competitivo nello scenario globale e difendere l'interesse nazionale, l'autonomia e la sovranità.

Scuola Navale Militare "Francesco Morosini"

Venezia



LE DISCIPLINE STEM NELLA DIFESA

LA SFIDA DELL'INTELLIGENZA ARTIFICIALE E LA SICUREZZA COMUNE

TERZA CONFERENZA NAZIONALE

VENEZIA - SCUOLA NAVALE MILITARE "FRANCESCO MOROSINI"
4 FEBBRAIO 2026 - ORE 9.30-16.30

PROGRAMMA

Evento promosso dal Sottosegretario di Stato alla Difesa, Sen. **Isabella RAUTI**,
con delega alla "Formazione del personale civile e militare della Difesa"

LE DISCIPLINE STEM NELLA DIFESA

LA SFIDA DELL'INTELLIGENZA ARTIFICIALE E LA SICUREZZA COMUNE

PRESENTA
Veronica MAYA
Conduttrice televisiva

Ore 09.30-10.00
Saluto di benvenuto
Amm. Sq. Stefano BARBIERI
Comandante delle Scuole della Marina Militare

INTERVENTI ISTITUZIONALI

On. Guido CROSETTO
Ministro della Difesa

Professor Giuseppe VALDITARA
Ministro dell'Istruzione e del Merito

Sen. Anna Maria BERNINI
Ministro dell'Università e della Ricerca

Sen. Isabella RAUTI
Sottosegretario di Stato alla Difesa

On. Marta SCHIFONE
Capogruppo Commissione Lavoro FDI
Prima firmataria della legge sull'istituzione della settimana nazionale delle discipline STEM

INTRODUCE E COORDINA
Alessio JACONA
Giornalista curatore dell'Osservatorio Intelligenza Artificiale di ANSA

Ore 10.00-10.35
Primo panel - *"STEM: risorsa per fronteggiare le sfide della sicurezza"*

- **Gen. Luciano PORTOLANO**
  Capo di Stato Maggiore della Difesa
- **Gen. C.A. Carmine MASIELLO**
  Capo di Stato Maggiore dell'Esercito Italiano
- **Amm. Sq. Giuseppe BERUTTI BERGOTTO**
  Capo di Stato Maggiore della Marina Militare
- **Gen. S.A. Antonio CONSERVA**
  Capo di Stato Maggiore dell'Aeronautica Militare
- **Gen. C.A. Salvatore LUONGO**
  Comandante Generale dell'Arma dei Carabinieri

Ore 10.35-10.55
Secondo panel - *"Luci e ombre dell'Intelligenza Artificiale"*

- **Prof.ssa Barbara CAPUTO**
  Ordinario al Politecnico di Torino
- **Padre Paolo BENANTI**
  Presidente della Commissione Intelligenza Artificiale per l'Informazione della Presidenza del Consiglio

Ore 10.55-11.15
COFFEE BREAK

Ore 11.15-13.00
Terzo panel 1ª parte - *"Applicazioni STEM a scenari di crisi simulati"*
Presentazione dei progetti degli Allievi di Scuole Militari, Scuole Sottufficiali e Accademie delle Forze Armate, dell'Arma dei Carabinieri e della Guardia di Finanza

- **Scuole Militari: "Visione artificiale per la sorveglianza di infrastrutture strategiche"**
  - **Scuola Militare "Nunziatella"**
    Allievi: Beatrice NIGRO, Biagio PELLECCHIA, Giacomo SCOVOTTO
    Tutor: Cap. Salvatore ADDESSO
  - **Scuola Militare "Teuliè"**
    Allievi: Gioele BARSOTTI, Maria Vittoria FLORESTA, Chiara INVERNIZZI
    Tutor: Ten. Col. Filippo BUQUICCHIO
  - **Scuola Militare Navale "Morosini"**
    Allievi: Francesco BALLETTA, Raffaele MIRAGLIA, Maristella Rosa Magdalena SALVO
    Tutor: C.C. Giuseppe MELLUSO
  - **Scuola Militare Aeronautica "Douhet"**
    Allievi: Gaia DE LUCA, Francesco DONVITO, Pierluigi Maria STORNELLI
    Tutor: Ten. Alessandro MASSA
- **Scuole Sottufficiali: "Oltre l'orizzonte del contagio"**
  - **Scuola Sottufficiali dell'Esercito Italiano**
    Allievi: Giuseppe CHIARA, Leandro LA BIANCA, Sara LUBRANO DI SCASSACANCIELLO
    Tutor: Cap. Simone DELLA CIANA

LE DISCIPLINE STEM NELLA DIFESA

LA SFIDA DELL'INTELLIGENZA ARTIFICIALE E LA SICUREZZA COMUNE

- **Scuola Sottufficiali della Marina Militare**
  Allievi: Lorenza CHILLEMI, Andrea RUGGIRELLO, Saverio SCIACOVELLI
  Tutor: C.C. Antonio MANZO
- **Scuola Marescialli dell'Aeronautica Militare**
  Allievi: Gabriele ARDIZZONE, Chiara CATAMO, Samuele MANFREDI, Matteo MATTA, Massimo MENEGHELLI
  Tutor: Ten. Col. Mario TANZI
- **Scuola Marescialli e Brigadieri dei Carabinieri**
  Allievi: Luca ESARTI, Martina DAFANO, Alessia MAROTTA, Iacopo VETRUCCIO
  Tutor: Ten. Col. Onofrio FLORE

- **Scuola Ispettori e Sovrintendenti della Guardia di Finanza:**
  "GdFCoach: tutor e simulatore per le attività ispettive della Guardia di Finanza";
  "A.R.C.A. (Analisi di rischio contabilità anomale): applicativo che supporta l'attività investigativa analizzando contabilità e documentazione fiscale"
  Allievi: Federico FREDDO, Salvatore MILIONE
  Tutor: Cap. Giulia ROMANAZZI

- **Accademie:**
  "IA, sistemi autonomi e space technologies per la sicurezza integrata dell'Artico"
  - **Accademia Militare di Modena**
    Allievi: Domenico PELLEGRINO, Sofia PERROTTA, Alessandro URBANO
    Tutor: Cap. Marco LEOPIZZI
  - **Accademia Navale della Marina Militare**
    Allievi: Emanuele BARSOTTI, Michele D'ANDREA, Antongiulio IZZO, Erika PACE
    Tutor: C.C. Giacomo MAIO
  - **Accademia dell'Aeronautica Militare**
    Allievi: Martina CENNAMO, Sara NOGAROTTO, Alessandro Gerlando RIZZO
    Tutor: Cap. Luca BARBATO

Ore 13.00-14.00
PAUSA PRANZO - Standing lunch

Ore 14.00-14.30
Terzo panel 2ª parte - *"Applicazioni STEM a scenari di crisi simulati"*
Presentazione del progetto del Centro Alti Studi Difesa/Scuola Superiore Universitaria (CASD/SSU) "AI LITERACY dall'esigenza all'offerta formativa"

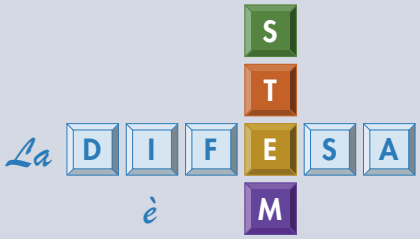
- **Col. Giacinto D'URSO**
  Capo Ufficio Formazione digitale e sviluppo tecnologico
- **C.F. Gilberto PETRINI**
  Capo Sezione Formazione Digitale

Ore 14.30-15.40
Quarto panel - *"Formazione militare, Discipline STEM e Intelligenza Artificiale: una sintesi compiuta?"*

- **Gen. C.A. Antonello VESPAZIANI**
  Comandante per la Formazione, Specializzazione e Dottrina dell'Esercito
- **Amm. Sq. Stefano BARBIERI**
  Comandante delle Scuole della Marina Militare
- **Gen. S.A. Francesco VESTITO**
  Comandante delle Scuole dell'Aeronautica Militare
- **Gen. C.A. Marco MINICUCCI**
  Comandante delle Scuole dell'Arma dei Carabinieri
- **Gen. C.A. Stefano MANNINO**
  Presidente del Centro Alti Studi Difesa - Scuola Superiore Universitaria
- **Gen. C.A. GdF Vito AUGELLI**
  Ispettore delle Scuole della Guardia di Finanza

Ore 15.45-16.30
CONCLUSIONI
Sen. Isabella RAUTI
Sottosegretario di Stato alla Difesa

Il convegno sarà trasmesso in streaming sui canali social della Difesa
www.facebook.com/ministerodifesa
www.youtube.com/@ministerodifesa
www.difesa.it


La DIFESA è
S
T
E
M


Scuola Navale Militare


"Francesco MOROSINI"
DISCIPLINE
TEM

Saluto di benvenuto del Comandante delle Scuole della Marina Militare Ammiraglio di Squadra Stefano BARBIERI

Ammiraglio di Squadra Stefano BARBIERI

Rivolgo a tutti il mio saluto di benvenuto, nella prestigiosa e storica sede della Scuola Navale Francesco MOROSINI. Ringrazio il Sottosegretario di Stato alla Difesa, Senatrice RAUTI per averci onorato della possibilità di ospitare l'evento odierno e saluto l'Onorevole Marta SCHIFONE (prima firmataria della legge sull'istituzione delle discipline STEM).

Rivolgo il mio saluto al Ministro della Difesa, Onorevole CROSETTO e al Ministro dell'Istruzione e del Merito, Onorevole VALDITARA che non hanno potuto prendere parte alla giornata.

Saluto i Capi di Stato Maggiore delle Forze Armate e i Comandanti Generali dell'Arma dei Carabinieri e della Guardia di Finanza intervenuti, in collegamento e i loro delegati.

Saluto i rappresentanti della politica, della magistratura e della cultura e del mondo accademico qui presenti. Ringrazio il presidente del C.A.S.D., il Generale MANNINO per la sua Alta Guida nel mare della Formazione. Ringrazio della partecipazione Padre BENANTI e la professoressa Barbara CAPUTO per la gradita disponibilità a fornire i loro autorevoli approfondimenti sul tema dell'Intelligenza Artificiale.

Un caloroso saluto ai colleghi, Comandanti della Formazione delle altre Forze Armate e, soprattutto, un saluto e ringraziamento a tutti i giovani allievi e frequentatori delle Accademie militari, delle Scuole Sottufficiali e delle Scuole Militari che hanno lavorato allo sviluppato dei progetti che verranno presentati oggi.

Non è casuale che la terza conferenza sulle discipline STEM nella Difesa approdi qui, a Venezia. La citta della laguna per secoli è stata la Silicon Valley del Mediterraneo: l'Arsenale di Venezia non era solo una fabbrica di navi, ma un centro di innovazione tecnologica, ingegneristica e matematica senza eguali nel suo tempo.

Oggi, raccogliamo quel testimone. Il nostro motto, "Patria e Onore", si declina in questo millennio attraverso una nuova consapevolezza: non c'è difesa efficace della Patria senza supremazia tecnologica, e non c'è supremazia tecnologica senza una solida cultura STEM.

La funzione educativa degli Istituti di Formazione militari deve a mio avviso superare la tradizionale dicotomia tra "sapere umanistico" e "sapere tecnico". La formazione militare moderna deve essere un ecosistema integrato. Il Comandante di domani non potrà limitarsi a gestire uomini e mezzi; dovrà possedere la capacità analitica

di comprendere sistemi complessi e interconnessi, per intuire le implicazioni operative di un'innovazione scientifica e per trasformare il dato grezzo in vantaggio decisionale. Le discipline STEM, in quest'ottica, non sono un bagaglio accessorio, ma l'ossatura stessa della leadership moderna.

Il contesto globale, quindi, ci pone di fronte a una sfida non solo geopolitica, ma anche e soprattutto profondamente ingegneristica e cognitiva. La supremazia non si misura più esclusivamente in tonnellaggio o numero di piattaforme, ma nella capacità di processare informazioni più velocemente dell'avversario. Siamo immersi in uno scenario caratterizzato da asimmetrie fulminee, dove un vantaggio tecnologico nel dominio cyber o nell'uso dell'Intelligenza Artificiale può rendere obsoleta una tecnologia convenzionale in pochi istanti. La difesa moderna richiede quindi una continua tensione verso l'innovazione: non basta più adattarsi al cambiamento, bisogna anticiparlo attraverso la ricerca e lo sviluppo ed è anche per questo che siamo qui oggi.

Ciò premesso, rivolgo un pensiero speciale e un ringraziamento a voi, giovani allievi e frequentatori, Voi non siete solo i destinatari di questa formazione, siete il motore di questa trasformazione. La Difesa guarda a voi non solo per la vostra "flessibilità mentale" ma per la vostra nativa capacità di abitare il mondo digitale.

Il mio augurio è che queste giornate di lavoro siano state per voi come un punto nave preciso: un momento per definire la rotta, consapevoli che il mare delle conoscenze scientifiche è vasto, ma è l'unico che vi permetterà di navigare sicuri nelle tempeste della complessità moderna.

Nel ringraziare anche tutti coloro che hanno lavorato dietro le quinte per la realizzazione di questo evento, do di nuovo il benvenuto a tutti alla Scuola Navale Militare "Francesco Morosini" e auguro a tutti voi il più marinaresco buon vento per i lavori di questa terza conferenza sulle discipline STEM nella Difesa.

Ministro della Difesa

On. Guido CROSETTO

Messaggio del Ministro della Difesa
On. Guido CROSETTO

Desidero ringraziare il Sottosegretario RAUTI per aver promosso la terza edizione della Conferenza sulle discipline STEM, un appuntamento che dimostra in modo concreto quanto la Difesa creda nei giovani e nella loro capacità di costruire un futuro più sicuro, innovativo e competitivo per il Paese.

Rivolgo un saluto particolarmente sentito agli Allievi delle Scuole Militari e degli istituti di formazione delle Forze Armate, dell'Arma dei Carabinieri e della Guardia di Finanza. Siete voi il cuore di questa iniziativa. Un ringraziamento va anche ai relatori, ai comandanti, ai docenti e ai professionisti, civili e militari, che accompagnano questo percorso di crescita e confronto.

Le discipline STEM non sono solo materie di studio: sono un modo di pensare, basato su metodo, curiosità, sperimentazione e capacità di lavorare insieme. È grazie a questo approccio che nascono le innovazioni che stanno cambiando la nostra vita quotidiana, dalla sanità all'energia, dall'industria alle tecnologie digitali. Innovazioni che si inseriscono in uno scenario di sicurezza profondamente mutato, in cui anche il dominio cibernetico è diventato uno spazio di confronto strategico, con effetti reali sulla vita delle persone, delle istituzioni e delle imprese.

Per questo oggi parlare di sicurezza significa guardare oltre i confini fisici: significa occuparsi di sicurezza tecnologica, economica, energetica e sociale. Viviamo una fase di trasformazioni rapidissime, forse la più intensa di sempre, in cui robotica e intelligenza artificiale incideranno profondamente sul lavoro, sulla produzione e sui servizi. Nei prossimi anni molte professioni cambieranno, alcune nasceranno, altre si trasformeranno: non è una minaccia, ma una grande responsabilità e un'enorme opportunità, soprattutto per la vostra generazione.

Alla CES 2026 di Las Vegas sono stati presentati robot umanoidi italiani come "Gene.01", sviluppato dall'Istituto Italiano di Tecnologia di Genova, e "RoBee", destinato ad applicazioni industriali e sanitarie. Sono esempi concreti che dimostrano come il talento, la ricerca e la passione possano permettere all'Italia di competere ai massimi livelli internazionali. Intelligenza Artificiale, High Performance Computing e Quantum Computing stanno aprendo una nuova era e stanno cambiando anche il modo di pensare la Difesa e la sicurezza.

L'obiettivo è mettere ricerca e innovazione al servizio del bene comune, rafforzando la sovranità tecnologica del Paese. In questo quadro si inserisce la strategia italiana sulle tecnologie quantistiche, che coinvolge università, centri di ricerca, industria e istituzioni. Investire sui giovani, sulle competenze e sulla conoscenza è essenziale per non lasciare indietro nessuno. Oggi l'Italia è tra i Paesi più avanzati in Europa e nel mondo in questo settore, grazie anche al lavoro di oltre 130 gruppi di ricerca attivi sul territorio.

Messaggio del Ministro della Difesa, On. Guido CROSETTO

Le tecnologie quantistiche avranno un impatto concreto su molti ambiti della nostra società: dalla sanità all'energia, dalla logistica alla difesa. Dai sensori capaci di funzionare anche senza GPS, alla crittografia post-quantum, fondamentale per proteggere i dati nel tempo, parliamo di strumenti che richiederanno competenze, responsabilità e senso etico.

Concludo rivolgendo un saluto particolare a Voi, che sarete chiamati ad affrontare nuove e sempre più complesse sfide tecnologiche in un mondo in rapido cambiamento ma anche ricco di possibilità. La vostra missione sarà essenziale: dovrete coniugare tradizione e innovazione, padroneggiare tecnologie complesse e metterle al servizio del Paese. La vostra preparazione sarà determinante per affrontare le sfide che ci attendono senza dimenticare che il vostro impegno, il vostro rigore e la vostra dedizione saranno i veri fattori di successo.

Con questa fiducia, vi auguro buon lavoro e buon cammino.

Messaggio del Ministro dell'Istruzione e del Merito Prof. Giuseppe VALDITARA

Ministro dell'Istruzione e del Merito
Prof. Giuseppe VALDITARA

Un caro saluto a tutti i partecipanti e un saluto particolare al Ministro Guido Crosetto, un ringraziamento anche per avermi coinvolto in questa splendida iniziativa, in questa terza edizione della Conferenza sulle discipline STEM nella Difesa. Un ringraziamento e un caro saluto anche all'Ammiraglio Stefano Barbieri, Comandante delle Scuole della Marina Militare. Un saluto molto molto affettuoso a tutti voi, allievi delle varie scuole militari e ai loro docenti.

Devo dire che il Ministero in questi tre anni ha operato una piccola rivoluzione nel mondo delle STEM. Innanzitutto, abbiamo riformato in profondità i programmi, la didattica, dunque, delle materie STEM a iniziare dalla scuola primaria per proseguire con la Scuola secondaria di I grado e stiamo per varare la riforma anche con riferimento alla Secondaria di II grado.

Le Linee guida, che abbiamo peraltro già approvato nel 2023, dettano una significativa innovazione: sostanzialmente la didattica è sempre più incentrata sui problemi reali. La didattica delle materie STEM parte dalla realtà per arrivare alla teoria, per far sì che anche coloro che non hanno il cosiddetto "bernoccolo" della matematica possano affascinarsi e appassionarsi alle materie STEM.

L'aula diventa dunque una sorta di laboratorio attivo dove si esplora, si formulano ipotesi, si costruiscono significati. Gli studenti da semplici fruitori diventano protagonisti, progettano loro stessi, discutono, interpretano dati, trasformando anche l'errore in una risorsa. E in questo contesto la matematica è certamente lo strumento per leggere la realtà, ma è anche cerniera culturale fra l'area scientifico-tecnologica e l'area umanistico-artistica. È importante infatti costruire connessioni fra queste aree e non è casuale che abbia voluto inserire proprio la matematica fra le materie orali della Maturità del Liceo classico.

L'innovazione si completa recuperando anche la dimensione storica e culturale delle scoperte per formare un vero e proprio pensiero STEM, un pensiero critico, un pensiero creativo, un pensiero collaborativo.

E prima di concludere questo mio rapido saluto voglio anche ricordare quello che abbiamo fatto non soltanto dal punto di vista dei programmi e della didattica della matematica. Sul digitale abbiamo investito 2 miliardi e 100 milioni di euro per la trasformazione delle aule in ambienti didattici fortemente innovativi. Ad oggi sono stati realizzati ben 115 mila ambienti digitali in soli tre anni. Abbiamo anche investito delle risorse particolarmente importanti per i laboratori innovativi nell'ambito della riforma del cosiddetto 4 + 2 dell'istruzione tecnico-professionale con un investimento di 210 milioni di euro. Abbiamo costruito 103 campus proprio per favorire all'interno della filiera del 4 + 2 una didattica sempre più incentrata, sempre più attenta a queste tematiche, che sappia utilizzare e valorizzare le tecnologie digitali. Abbiamo anche investito 450 milioni di euro nella formazione dei docenti e del personale scolastico finalizzato alla didattica digitale, allo sviluppo di tecniche innovative nella didattica e abbiamo investito 100 milioni di euro per la formazione specifica nella Intelligenza Artificiale, un'altra grande sfida.
Abbiamo inserito nei nuovi programmi scolastici e nelle nuove Linee guida sull'Educazione civica l'educazione all'utilizzo corretto dell'Intelligenza Artificiale e alla prevenzione dei rischi connessi all'Intelligenza Artificiale.
Un ulteriore investimento di 600 milioni di euro è stato specificamente destinato al potenziamento delle discipline STEM e, fra l'altro, anche per ridurre i divari di genere.
E infine, abbiamo avviato, fra i primi Paesi al mondo, una sperimentazione dell'utilizzo dell'Intelligenza Artificiale nelle classi ai fini della personalizzazione della didattica. Ecco, tutto questo significa la centralità delle nuove tecnologie, delle materie STEM, dell'Intelligenza Artificiale per la scuola italiana, significa una scuola italiana in forte movimento verso il futuro. Grazie e buon lavoro e un carissimo saluto ancora a tutti voi, in particolare agli allievi e ai vostri docenti.

Messaggio del Ministro dell'Università e della Ricerca Sen. Anna Maria BERNINI

Ministro dell'Università e della Ricerca
Sen. Anna Maria BERNINI

Carissimo Ministro Crosetto, carissima Sottosegretario Rauti e cari allievi tutti della Scuola Navale e Militare Francesco Morosini, questa è la settimana delle discipline STEM e vorrei iniziare con una parola semplice ma tanto sincera. Complimenti.
Complimenti per la scelta che avete fatto, che è un percorso impegnativo, rigoroso, che richiede studio, disciplina e carattere. Ma è un percorso che non solo prepara, ma forma.
La scuola navale militare è a tutti gli effetti una scuola STEM, quindi scienza, tecnologia, ingegneria, matematica, che non sono solo materie astratte, ma diventano strumenti concreti per affrontare la complessità del mondo reale. Nei laboratori, attraverso le simulazioni, voi state acquisendo le competenze fondamentali per una Difesa moderna, capace di operare in più domini, grazie alla spinta innovativa della Marina militare. Ma c'è qualcosa di ancora più importante. Oggi la vera innovazione è unire, integrare, non separare. E quindi accanto alle discipline scientifiche qui trovano spazio anche le materie umanistiche, l'arte, il pensiero critico.
È l'approccio STEAM. Alla forza della tecnologia si unisce la forza della creatività, della filosofia, delle nostre potenti radici culturali. Anche nel contesto militare più avanzato non si perde mai il contatto con la dimensione umana delle operazioni, tanto decisiva quanto un algoritmo. Voi vi state formando per essere professionisti competenti e donne e uomini consapevoli, capaci di servire il Paese con testa, cuore e responsabilità. Continuate su questa rotta con orgoglio e determinazione. Buon lavoro e buon vento a tutti.

Intervento del Capogruppo della Commissione Lavoro di Fdl On. Marta SCHIFONE

Capogruppo della Commissione
Lavoro di Fdl
On. Marta SCHIFONE

Buongiorno a tutti e grazie per l'invito a questo evento così partecipato in questa prestigiosa scuola militare. Ringrazio le autorità civili e militari. Ringrazio il Ministro Crosetto e il Sottosegretario Rauti per la sensibilità e per l'impegno continuo. Questo è il terzo anno, la terza edizione della settimana che partirà il 4 di febbraio e si concluderà l'11. Una settimana che è stata istituita da una legge votata all'unanimità della quale mi onoro di essere stata prima firmataria. Una legge che ha voluto prevedere per sempre nella nostra Repubblica un tempo dedicato alla scienza, per raccontarne semplicemente la bellezza e tutte le opportunità. Abbiamo voluto realizzare questo contenitore nel quale ci sono attività di sensibilizzazione, di comunicazione, di divulgazione, nel quale abbiamo voluto coinvolgere tutti gli attori della filiera, a partire dalla Difesa, passando per la Scuola e l'Università, per le associazioni, per i luoghi di cultura, per le aziende pubbliche e private, e naturalmente per le Istituzioni. Noi, insieme a tutti gli attori della filiera stiamo facendo la nostra parte, speriamo di farla bene. Riteniamo che debba passare un messaggio culturale importante che deve essere ed è trasversale e deve arrivare a tutta la società. Il sistema educativo, l'accademia, le aziende sono particolarmente coinvolti nella promozione e valorizzazione delle competenze STEM ma c'è un deficit comunicativo perché l'opinione pubblica, le famiglie, i docenti non lo sono particolarmente altrettanto. Noi stiamo facendo la nostra parte perché stiamo provando a porre queste materie - avete sentito i Ministri competenti e il Sottosegretario Rauti - in maniera centrale nell'agenda politica, ma c'è bisogno della collaborazione di tutti per far passare il messaggio dell'importanza della scienza e dell'urgenza di acquisire competenze STEM. Perché a breve nasceranno professioni e professionisti che oggi neanche immaginiamo. Di questo dobbiamo essere consapevoli quando facciamo promozione, comunicazione e divulgazione delle discipline STEM. È a tutti gli effetti una urgenza della nostra società. STEM è matematica, è chimica, è fisica. Ma è matematica, chimica e fisica applicata, mi piace dire aumentata, per usare un termine che si applica a settori innovativi nei quali siamo già immersi e che sottendono alle sfide transizionali che noi già stiamo vivendo, al salto tecnologico che noi abbiamo approcciato e quindi parlo di cybersicurezza, parlo di robotica, parlo di automazione, parlo di data science, parlo di nano e biotecnologie, di neuroscienze.

Tutte queste sono discipline STEM, sono competenze STEM. L'intelligenza artificiale ci ha permesso di aprire il dibattito su questo. E c'è una domanda che è, come dire, un pò abusata quando si parla di intelligenza artificiale, e cioè come governare questi processi. Ecco, le competenze STEM sono degli strumenti tecnici e cognitivi che permettono di governare l'innovazione contemporanea. E questo è il focus che vogliamo far passare. È anche un interesse nazionale - lo ha detto benissimo il Sottosegretario prima - in un contesto di competizione globale, contingenze geopolitiche che ben conosciamo, è fondamentale avere competenze e coltivare i talenti in Italia, nel nostro interesse, non esportandoli ma diventando particolarmente competitivi. STEM è a tutti gli effetti, mi sento di dire, un asset strategico e STEM è anche uno degli ambiti maggiormente attenzionati dalle aziende. Le aziende chiedono a gran voce profili STEM, chiedono a gran voce queste skills e non le trovano. STEM è il campo con il tasso occupazionale in termini assoluti più alto nel mercato del lavoro, ma è anche il campo che è meno scelto dai nostri giovani. C'è questo grande mismatch tra domanda e offerta Viviamo un cambio di paradigma e anche rispetto a questo ci dobbiamo interrogare, cioè noi nel mercato del lavoro abbiamo sempre lavorato con strategie di contrasto alla disoccupazione. Oggi ci troviamo invece, grazie anche ad un boom occupazionale molto importante a cui stiamo assistendo in questi tempi, anche da quando c'è il nostro governo, che ci porta a dire che c'è un mismatch tra domanda e offerta. Un recente report di Unione Camere lo dice benissimo: oltre il 40 per cento sarà la richiesta per la formazione terziaria e quindi ritorniamo alle competenze STEM, quelle accademiche avanzate, ma anche naturalmente gli ITS e i livelli diciamo mediani di formazione.
E quindi STEM è il campo con il maggiore tasso occupazionale, il campo che senza ipocrisia ci dà il massimo della retribuzione e della prospettiva di carriera e anche di soddisfazione professionale. Dobbiamo raccontarlo ai nostri giovani perché, per paradosso, i nostri giovani non scelgono questo campo. Quando poi, e faccio un breve flash e mi avvio alla conclusione, andiamo a parlare dei numeri delle donne che scelgono queste competenze, vediamo che questi numeri scendono vertiginosamente. In media uno su quattro sceglie queste competenze. Anche se le donne sono il maggior numero di laureati in Italia, solo 16 su 100 di loro scelgono questo ambito. Ci sono dei retaggi culturali, dei messaggi distorti che sono stati trasmessi a queste donne, fin da bambine, quando gli è stato passato il messaggio che la matematica è noiosa, che la chimica è complicata, che la fisica non è roba da donne. Noi vogliamo invece raccontare a queste ragazze, anche e soprattutto con la settimana STEM e con questi progetti, che ci sono state invece delle donne nella storia che hanno abbattuto e combattuto questi stereotipi e che hanno segnato la storia della scienza. Penso ad Ada Lovelace e Rosalind Franklin, alle nostre Rita Levi-Montalcini e Margherita Haack fino ad arrivare oggi a Samantha Cristoforetti. Penso alle molte altre donne che scrivono la storia della scienza in silenzio nei loro dipartimenti, nelle loro università, nei loro laboratori. A queste donne bisogna guardare e a loro bisogna fare ferimento. Concludo dicendo che se anche un solo ragazzo o una sola ragazza, grazie ad un evento che si svolge durante la settimana nazionale delle STEM, si orienterà e sceglierà la sua strada seguendo queste materie, noi avremo raggiunto l' obiettivo di contribuire al processo di formazione delle professioni e dei professionisti del futuro. Grazie.

Riflessioni a margine del dibattito a cura del moderatore Alessio Jacona

Moderatore Alessio Jacona

In un mondo che si trasforma con velocità senza precedenti seguendo traiettorie a volte imprevedibili, ogni settore e scenario sembra subire la forza, la pervasività e l'implacabile efficienza con cui ciò che chiamiamo l'intelligenza artificiale - nelle sue molte forme - sta riplasmando il mondo. Le forze armate non fanno eccezione.

Anzi: sono una delle frontiere più avanzate in cui questa tecnologia trova le condizioni favorevoli per evolversi; il contesto in cui la distanza tra R&D e applicazione pratica si riduce fino quasi ad azzerarsi, accelerando il progresso con i suoi pro e i suoi contro. Cambia il mondo e con esso il modo di fare la guerra assieme a quello di garantire la pace. E poi, ancora, cambia l'idea stessa di cosa sia un militare di professione, di quali siano i suoi compiti, di quali debbano essere le sue competenze e di come formarle. È un passaggio necessario affinché i professionisti della Difesa e della sicurezza possano affrontare le sfide che li aspettano, in un quadro globale di competizione aperta e senza quartiere, dove restare indietro semplicemente non è un'opzione. Perché la guerra ormai è ibrida, spesso nemmeno dichiarata; un conflitto non convenzionale dove strategie e tattiche militari si combinano e complicano con quelle cibernetiche, economiche, diplomatiche con un unico scopo: mettere in crisi un avversario, possibilmente senza sparare un colpo.

Nella pratica, il supporto dell'AI sul campo di battaglia si traduce innanzitutto in una capacità di analisi senza precedenti: sistemi avanzati, come quelli testati dagli Stati Uniti nelle operazioni in Medio Oriente, sono in grado di elaborare istantaneamente una mole immensa di dati che provengono dal territorio, dalle forze di cielo, terra e mare, dall'intelligence, dalla rete, per coordinare attacchi e strategie con un'efficienza che supera le capacità umane.

Un'evoluzione che oggi tocca il suo apice nello sviluppo di droni autonomi: macchine capaci di muoversi in sciami e di dirigersi verso l'obiettivo in quasi totale autonomia, trasformando il fronte in un laboratorio tecnologico dove la velocità d'esecuzione diventa prioritaria su tutto. E dove è proprio tale velocità a porre nuovi e complessi interrogativi di natura etica, per esempio quando strategie e tattiche vengono elaborate alla velocità sovrumana delle macchine: in quel caso, ci si chiede, l'essere umano che deve premere il grilletto ha ancora il tempo di comprendere cosa sta accadendo e prendere decisioni informate e consapevoli?

E poi, ancora, la guerra odierna si combatte anche sul piano dell'informazione, con l'AI generativa che è diventata uno strumento potentissimo per confondere l'opinione pubblica attraverso la creazione di deepfake e contenuti sintetici. L'obiettivo è duplice: destabilizzare gli avversari e galvanizzare i propri sostenitori che, a loro volta, utilizzano sempre di più sistemi di AI generativa per "fabbricare la realtà", per generare prove false a conferma della loro visione del mondo, da riversare in rete aumentando l'entropia e contribuendo al caos.
Infine, se c'è guerra prima poi dovrà seguire la pace: quando quel momento arriva, paradossalmente l'AI che prima è servita per distruggere poi servirà poi per ricostruire. E questo perché gli stessi dati raccolti per fini bellici possono diventare la base per addestrare sistemi intelligenti dedicati alla ricostruzione delle città e alla rinascita delle nazioni.
Intanto vecchie alleanze si spezzano e gli amici di ieri diventano i "competitor" di oggi. Intanto nuovi scenari geopolitici si ricompongono intorno alle potenze rese tali dal primato tecnologico, che si gioca sul controllo del software, della catena di produzione dell'hardware, e - sempre di più - sul controllo e la raccolta appunto dei dati, il nuovo petrolio nell'era dell'AI.
Alla luce di tutto questo, come deve essere il militare del futuro? Come si deve formarlo? Qual è il ruolo delle materie STEM nella costruzione delle sue competenze? E qual è l'impatto dell'AI su tutto questo?
Di tutto questo e di altro ancora abbiamo parlato il 4 febbraio, presso la Scuola Navale Militare "Francesco Morosini" di Venezia, durante la 3ª Conferenza sulle discipline STEM nella Difesa dedicata a "La sfida dell'Intelligenza Artificiale e la sicurezza comune", con il Sottosegretario di Stato alla Difesa Senatrice Isabella Rauti (che ha promosso e organizzato l'evento) con i capi di Stato Maggiore, i comandanti di tutte le scuole delle forze armate e i 12 gruppi di allievi che hanno sviluppato e presentato progetti ad hoc.

Primo Panel

"STEM: risorsa per fronteggiare le sfide della sicurezza"

STEM

Intervista al Capo di Stato Maggiore della Difesa Generale Luciano PORTOLANO

In un contesto nazionale segnato da competizione tecnologica, minacce ibride e crescente complessità operativa, quale ruolo svolgono oggi le discipline STEM – in particolare quelle afferenti all'intelligenza artificiale – nel rafforzare la sicurezza nazionale?

Mi consenta, innanzitutto, di rivolgere un cordiale saluto alle autorità politiche, civili e militari, agli allievi di tutti gli istituti di formazione militare in sala e in collegamento, e tutti gli ospiti presenti.
In particolare, vorrei ringraziare il Ministro della Difesa, Onorevole Crosetto, per il suo video-messaggio, e la Senatrice Isabella Rauti, per l'invito a questa Terza Conferenza nazionale sulle discipline STEM.
Tornando alla sua domanda, ritengo che le discipline STEM rappresentino, oggi, uno dei principali fattori abilitanti per il sistema Difesa e per la credibilità internazionale di un Paese.
I moderni conflitti ne sono un esempio emblematico, essendosi rapidamente trasformati, tra l'altro, in veri e propri laboratori di sperimentazione, grazie anche all'impiego di nuove tecnologie, compreso l'uso estensivo dell'Intelligenza Artificiale.
Stiamo assistendo oggi a un profondo cambiamento nel modo di combattere e di decidere.
Parliamo di operazioni multi-dominio, di tempi decisionali compressi e di una massa di dati disponibili che supera le capacità umane di analisi, di elaborazione e di diffusione delle informazioni, rendendo, quindi, l'Intelligenza Artificiale uno strumento prezioso per il conseguimento del cosiddetto vantaggio decisionale.
In questo senso, l'Intelligenza Artificiale integra dati provenienti dalle dimensioni fisica, virtuale e cognitiva, li analizza in tempo reale, individua schemi e anomalie, e supporta il comandante in contesti sempre più mutevoli e complessi.
E queste potenzialità stanno trovando applicazione concreta anche ai fini addestrativi.
Mi riferisco al wargaming, che può essere enormemente potenziato dall'Intelligenza Artificiale evolvendo in adaptive wargaming, ricreando scenari realistici, che includono anche la minaccia ibrida, così da individuare le vulnerabilità e migliorare il coordinamento e la capacità di risposta, non solo militare, ma anche civile, nel cosiddetto Whole Government Approach.
Accanto all'Intelligenza Artificiale, l'elevata potenza di calcolo, il super calcolo - o come viene tecnicamente identificato, l'high performance computing - rappresenta un ulteriore fattore abilitante per l'elaborazione avanzata dei dati e il supporto al processo decisionale.
In questo senso, vale la pena ricordare che l'Italia occupa una posizione di assoluto rilievo nel panorama europeo e globale, collocandosi tra i primi paesi al mondo e al secondo posto in Europa per capacità di calcolo.
Si tratta di un vantaggio strategico al quale anche la Difesa deve ambire, per garantirsi autonomia, sicurezza e continuità nei processi di comando e controllo, soprattutto in contesti caratterizzati da elevata e repentina evoluzione, e poter, quindi, aspirare ad

Generale Luciano PORTOLANO

accedere al mondo delle tecnologie quantistiche, come più volte evidenziato dal Ministro della Difesa, Onorevole Guido Crosetto.
Un ambito, quello delle tecnologie quantistiche, nel quale ogni ritardo rischia di tradursi in una vulnerabilità strategica dell'intero sistema Paese.
Dunque, è osservando questo quadro d'insieme che emerge, con maggior chiarezza, anche la dimensione geopolitica delle discipline STEM.
Numerosi Paesi investono in modo sistematico su formazione scientifica, ricerca e innovazione. La Cina, in particolare, ha integrato in modo coerente il sistema universitario, l'industria e il comparto della Difesa e, oggi, circa la metà dei ricercatori in questo campo, a livello globale, è di formazione cinese.
Ma ritengo che il dato più rilevante è che Pechino porta alla laurea, ogni anno, milioni di profili STEM in più rispetto agli Stati Uniti, tanto da poter disporre, nel breve periodo, di un bacino STEM paragonabile al resto del mondo.
In questo contesto, solo l'India è su analoga traiettoria.
In definitiva, e concludo, tutto questo ci consegna una realtà chiara, ossia che le competenze e il talento sono oggi due dei principali fattori di potenza a livello globale.
Evoluzione?

Generale, cosa sta facendo lo Stato Maggiore della Difesa per accompagnare questa evoluzione?

Considerato il contesto che ho appena descritto, l'azione della Difesa non si può limitare al presidio delle singole tecnologie.
Essa deve svilupparsi secondo una visione integrata e multilivello, in cui la valorizzazione delle discipline STEM – per loro natura trasversali – sia pienamente recepita nelle priorità strategiche che ho individuato per sviluppare il processo di adattamento dello strumento

militare interforze.
Mi riferisco, nello specifico, alla transizione della difesa dal paradigma "net centrico" a quello "data-centrico", così come all'implementazione delle emerging disruptive techologies, e, in particolare, dell'Intelligenza Artificiale.
Quindi, lo Stato Maggiore della Difesa è impegnato a costruire uno strumento militare, come è stato ricordato, interconnesso, interoperabile e intercambiabile, che dovrà poter contare, anche, su una cornice tecnologica e di cybersicurezza solida e resiliente.
In tale prospettiva, si collocano, in modo sinergico, la "strategia digitale della Difesa" - elaborata dallo Stato Maggiore della Difesa e recentemente presentata al Ministro Crosetto - e la "strategia della Difesa per l'Intelligenza Artificiale", che è già stata menzionata - documento complementare alla "strategia digitale" - che è stata stilata dal Gabinetto del Ministro con la guida della professoressa Barbara Caputo
Allo stesso tempo, siamo consapevoli del ruolo centrale della formazione militare, chiamata non solo a favorire l'impiego delle nuove tecnologie, ma anche a sviluppare una capacità critica, consapevole dei limiti dei sistemi intelligenti come, ad esempio, le cosiddette "allucinazioni algoritmiche", ossia quegli errori generati da modelli di Intelligenza Artificiale che producono risposte apparentemente plausibili, ma oggettivamente false, non supportate dai dati nè dalla conoscenza reale.
Da ciò scaturisce che l'Intelligenza Artificiale, dal mio punto di vista, non deve e non può sostituire il fattore umano, ma deve amplificarne le capacità.
Ritengo, quindi, che acquistino così grande significato i progetti sviluppati dagli allievi delle Scuole e delle Accademie Militari, che oggi verrano presentati.
Esperienze che traducono le STEM in soluzioni operative e innovative, espressioni di competenza, di spirito critico e di creatività, qualità fondanti per la leadership militare di domani.
In chiusura, vorrei richiamare un punto che ritengo particolarmente importante:
La trasformazione tecnologica è rapida, sì, ma la sicurezza non può essere garantita solo dalla tecnologia.
Infatti, affinché le innovazioni possano generare gli effetti desiderati, dovremo essere in grado di comprenderle, di governarle e, quando necessario, anche di limitarle.
In altre parole, la tecnologia non è fine a sé stessa ma in uno schema di ends, ways e means, essa ci mette a disposizione gli strumenti (i means) utili a perseguire i nostri scopi (gli ends), ma poi sta a noi individuare le modalità più efficaci di impiego delle risorse disponibili (ossia le ways) ed è qui che entra in gioco la leadership. Una leadership che, personalmente, intendo "team centrica" e non "leader centrica". Una leadership la cui qualità fa spesso la differenza fra successo e insuccesso, fra vittoria e sconfitta.
Con questo spirito, auguro a tutti una proficua giornata di lavori, ringraziandovi per l'attenzione.

Intervista al Capo di Stato Maggiore dell'Esercito Generale di Corpo d'Armata Carmine MASIELLO

Ai nostri microfoni abbiamo l'onore di avere il Capo di Stato Maggiore dell'Esercito, il Generale di Corpo d'Armata Carmine Masiello. Benvenuto Comandante e grazie per la disponibilità. Signor Generale, come evidenziato dagli interventi che si sono susseguiti nel corso della conferenza, lo stravolgimento del contesto strategico degli ultimi anni impone alla Difesa e quindi anche all'Esercito di cambiare passo e paradigma. Può spiegarci in cosa consisterà questo cambiamento per la nostra Forza Armata?

Grazie, e buongiorno a tutti. Viviamo in un'epoca ricca di sfide, caratterizzata da un contesto di sicurezza complesso, fortemente instabile e competitivo. A causa delle recenti crisi, la certezza della "pace permanente" consolidatasi negli anni successivi al crollo dell'Unione Sovietica si è improvvisamente sgretolata, rivelandosi una effimera illusione e facendoci riscoprire la parola "guerra".
Il contesto appena delineato ha imposto all'Esercito una profonda riflessione. Infatti, siamo passati da un periodo durato oltre 30 anni, in cui eravamo fortemente impegnati nelle operazioni di supporto alla pace, alla situazione attuale, in cui dobbiamo prepararci con serietà al peggio, pur sperando sempre che non accada mai. Noi siamo i primi a non volere la guerra perché abbiamo vissuto il dolore e lo sconforto di vedere i nostri fratelli in armi rientrare in Patria avvolti nel Tricolore. Tuttavia, se dovesse succedere, non possiamo permetterci di farci cogliere impreparati.

Generale di Corpo d'Armata Carmine MASIELLO

Ciò significa dedicarsi con molta più enfasi all'addestramento, immettere in servizio nuovi mezzi e sistemi d'arma e, soprattutto, realizzare una rivoluzione culturale nel modo di pensare e agire. Significa coinvolgere tutti, in particolare i più giovani, capaci come solo loro possono essere di intercettare i cambiamenti del mondo che ci circonda e di interagire in maniera naturale con le innovazioni tecnologiche.
Per quanto riguarda l'addestramento, il concetto è semplice: la vita del soldato è fatta di "pane e addestramento", perché esso è la garanzia di assolvere il compito ed è la migliore polizza assicurativa di un soldato, e per chi ha al proprio fianco. Sul fronte dei mezzi non mi dilungherò, ma stanno già entrando in servizio sistemi di nuova generazione nell'ambito dei principali settori di innovazione individuati, tra cui i primi veicoli cingolati "Lynx" per la componente pesante, i sistemi "Skynex", "SAMP-T" e "Grifo" per la capacità di difesa contraerea in ottica integrata e multilivello e il nuovo elicottero LUH per quanto attiene il potenziamento della componente elicotteristica. Questi rappresentano solo i primi risultati concreti del programma di ammodernamento e rinnovamento di mezzi e sistemi d'arma che l'Esercito ha avviato: come ho più volte affermato, "l'Esercito è tecnologico o non è".

In questo cambiamento riveste un ruolo particolare l'Intelligenza Artificiale (I.A.). In che modo l'Esercito italiano sta integrando questa modernissima tecnologia, soprattutto nello svolgimento delle sue attività?

In generale, la tecnologia e l'evoluzione dell'I.A. sono destinate a trasformare profondamente le società e i loro modelli organizzativi, incidendo anche sui sistemi di difesa e sicurezza e ridefinendo i paradigmi operativi e strategici delle Forze Armate: dai sistemi autonomi e semiautonomi (UAV, UGV) alla fusione automatizzata di dati multisensori per l'intelligence, fino ai sistemi di supporto decisionale per i Comandanti.
Di fronte alle minacce sempre più presenti nel dominio cibernetico, la formazione diventa un elemento fondamentale di prevenzione e difesa, poichè una popolazione alfabetizzata digitalmente riveste una rilevanza strategica. Per questo l'Esercito sta investendo nella promozione delle competenze cyber a 360°, dal reclutamento ai percorsi formativi dedicati, alla valorizzazione delle capacità dei giovani di gestire l'ondata incessante di innovazione tecnologica dei tempi in cui viviamo.
Abbiamo avviato una serie di iniziative presso la Scuola Ufficiali per sfruttare le potenzialità dell'I.A. all'interno dei corsi in atto sia per il supporto e il potenziamento della didattica sia nell'ambito delle piattaforme e-learning in utilizzo ai frequentatori. In particolare, l'I.A. viene già applicata in supporto alla docenza per la generazione automatica di contenuti didattici, per il supporto alle verifiche e, in generale, per fornire assistenza all'interno dei corsi. Inoltre, sono stati adottati applicativi per la sintesi automatica dei contenuti e per la semplificazione dell'apprendimento, insieme a un chatbot di supporto allo studio, che consentono ai nostri giovani di comprendere sin da subito le potenzialità dell'I.A., nonché di coltivare una mentalità critica, favorendo

una riflessione continua sulle sue implicazioni e sulle sue applicazioni future.
Dunque, alla luce delle straordinarie potenzialità offerte dall'Intelligenza Artificiale, il suo impiego in ambito Forza Armata non è solo auspicabile: è sempre più necessario. In tale prospettiva ho dato chiare indicazioni sulla necessità di procedere in questa direzione, orientando l'Esercito verso una struttura pronta a "ricevere", impiegare e addestrare efficacemente tali capacità. Le progettualità e le iniziative intraprese sono già molteplici; per esempio, è stata avviata una campagna di sperimentazione pluriennale sui Robotic Autonomous System (RAS), lanciata la prima challenge per valutare soluzioni di mercato off-the-shelf e sono stati definiti appositi percorsi formativi per elevare la preparazione tecnico-professionale del personale militare.
Si tratta solo dei primi passi di un percorso che dovrà essere progressivamente consolidato e sviluppato. Siamo consapevoli che l'ambito di applicazione deve avere una visione di lungo termine e non deve essere circoscritto ai processi decisionali o alla condotta delle operazioni. Al tempo stesso, è fondamentale non dimenticare che, in relazione agli aspetti etici e normativi di riferimento, nessuna innovazione può prescindere dalla centralità del rispetto dei principi di distinzione, proporzionalità e necessità militare. Pertanto, nelle decisioni che implicano l'uso della forza letale, la responsabilità ultima deve rimanere in capo all'essere umano (secondo il principio comunemente definito "human in the loop").

All'interno di questo grande cambiamento al quale è chiamata la Difesa ma anche l'Esercito ovviamente, quale ruolo giocano le discipline cosiddette STEM, quindi scienza, tecnologia, ingegneria e matematica?

Oggi il vantaggio competitivo risiede nella capacità di comprendere profondamente la tecnologia, nel saperla integrare e nel prevedere le implicazioni del suo impiego.
Quando parliamo di STEM non intendiamo solo un insieme di materie accademiche, bensì un approccio metodologico che integra rigore analitico, pensiero sistemico e capacità di operare con dati e modelli. Questo approccio promuove un metodo interdisciplinare per la risoluzione di problemi complessi, favorendo il confronto e il dialogo secondo una logica di complementarietà e interdipendenza. Per questo motivo, l'obiettivo è avere un Esercito costruito su solide competenze STEM, perché non solo sarà più efficace sul campo di battaglia – qualora dovesse essere necessario – ma, soprattutto, sarà una risorsa per la difesa del Paese nella sua interezza. Infatti, chi comprende profondamente gli algoritmi, la matematica delle reti sociali, i pattern statistici della manipolazione può contrastare efficacemente le minacce contemporanee alla Nazione e alla libertà stessa dei cittadini, ovvero le campagne di disinformazione, la manipolazione dell'opinione pubblica, i deepfake e le sofisticate forme di "ingegneria del consenso". A queste considerazioni, aggiungo un ulteriore elemento: noi italiani siamo i padri dell'Umanesimo e non possiamo dunque trascurare il valore di discipline come la letteratura, la filosofia e la storia.
Per questo, negli istituti di formazione, ho preteso di affiancare alle competenze STEM

lo studio delle discipline umanistiche e della filosofia, promuovendo un modello educativo che sviluppa la complementarità tra il sapere, il saper fare e il saper far fare, con l'obiettivo di sviluppare spirito critico e consapevolezza e formare menti libere e creative, in grado di porsi le domande giuste muovendosi sempre su due binari complementari: la reazione alle sfide e la proattività nel prevenirle. Grazie.

Intervista al Capo di Stato Maggiore della Marina Militare Ammiraglio di Squadra Giuseppe BERUTTI BERGOTTO

Ammiraglio, oggi proteggere l'Italia significa sia sorvegliare i nostri mari, sia proteggere le 'autostrade invisibilÌ che corrono sotto l'acqua, come i cavi internet e i gasdotti. Con l'avvento dell'Intelligenza Artificiale e delle minacce informatiche, come sta cambiando il vostro lavoro? In che modo l'AI vi aiuta a capire in anticipo cosa succede sopra e sotto il mare e come permette alla Marina di garantire la pace in un mondo dove gli attacchi possono essere digitali e silenziosi prima ancora che fisici?

La difesa del territorio non si esaurisce più nella protezione dei confini fisici, ma comprende la salvaguardia di infrastrutture critiche, reti digitali, dati, tutti elementi vulnerabili ad azioni ostili condotte nel dominio cyber e cognitivo. In questo conteso l'utilizzo dell'AI diventa centrale sia come moltiplicatore di capacità difensive — attraverso l'analisi predittiva delle minacce, il rilevamento di anomalie e il supporto decisionale in tempo reale — sia come nuovo fattore di rischio strategico.
Come potrà immaginare, la quantità enorme di dati da elaborare e la dinamica estremamente veloce di alcuni eventi richiedono dei sistemi di supporto alle decisioni che facciano largo uso di modelli basati sui dati raccolti in questi anni.
Un esempio pratico riguarda la nostra Maritime Situational Awareness: ogni giorno nel Mediterraneo ci sono oltre 10000 contatti in mare (se consideriamo il solo naviglio superiore alle 500 tonnellate).

Ammiraglio di Squadra Giuseppe BERUTTI BERGOTTO

A tal riguardo le tecnologie AI ci possono dare una rapida consapevolezza della presenza di anomalie garantendo così una situazione più chiara in un ambiente come il Mediterraneo estremamente denso di attività e di traffici marittimi.
Le tecnologie di AI permettono di costruire efficientemente questi modelli e renderli adattivi ai diversi contesti. Proprio nell'ambito della sicurezza cibernetica, l'analisi comportamentale basata sull'addestramento dei modelli di Intelligenza Artificiale consente di individuare l'uso di tecniche di attacco "non note".

Ammiraglio, per una Marina moderna essere pronti a intervenire significa avere navi che non si fermano mai. In questo senso, la logistica è il 'motore invisibile di ogni missione. Guardando alle nuove tecnologie, in che modo l'Intelligenza Artificiale sta cambiando il vostro modo di operare? Ad esempio, quanto siamo vicini a un sistema capace di prevedere un guasto a bordo prima ancora che avvenga, o di gestire in automatico i rifornimenti per una flotta impegnata lontano dall'Italia, assicurando che non manchi mai nulla proprio nel momento del bisogno?

La Strategia si inserisce in un percorso già avviato fornendo indirizzi per promuovere lo sviluppo di capacità tecnologiche autonome, rafforzare il capitale umano e la valorizzazione dei dati, innovare i processi e, in particolare, fornire supporto ai decisori multilivello.
Noi stiamo investendo da più di dieci anni in questo campo, in sistemi in grado di effettuare una valutazione della condizione di efficienza dei macchinari di bordo. Alcune di queste funzioni sono già una realtà consolidata.
Ad esempio per alcuni fenomeni legati alle vibrazioni dei macchinari, siamo in grado di intercettare un guasto prima che si verifichi e di diagnosticare anche il singolo sotto-componente che si romperà con un'elevata precisione. Purtroppo, la natura di alcuni fenomeni fisici legati al funzionamento dei macchinari limita questa capacità previsionale ad alcune specifiche dinamiche. Molto è stato fatto, ma ci sono ancora margini di miglioramento.
Anche se la chiamiamo Intelligenza Artificiale, dietro a queste tecnologie ci sono dei modelli statistici comunque fallibili, che commettono errori con una certa probabilità. Per questo la preparazione tecnica dei nostri uomini deve essere tale da poter trattare le indicazioni fornite da questi sistemi in modo critico.

Ammiraglio, l'Intelligenza Artificiale impara macinando enormi quantità di dati. Per questo è ancora più vero e diventa strategico quando si tratta di addestrare sistemi automatizzati che devono supportare il personale e le operazioni della Marina. In un mondo dove i dati sono preziosi quanto il petrolio, chi controlla i dati con cui 'istruiamo le nostre tecnologie, e come facciamo a garantire che rimangano sempre sotto una gestione nazionale sicura, evitando che finiscano nelle mani sbagliate o che vengano manipolati per trarci in inganno?

I dati rappresentano un fattore abilitante per implementare la strategia della Difesa in materia di Intelligenza artificiale unitamente alla capacità di calcolo proprietaria (High Performance Computing - supercalcolatori).
I dati non sono più una semplice risorsa tecnica, ma un vero e proprio asset di potere, in grado di determinare l'efficacia, l'affidabilità e la superiorità operativa dei sistemi di IA.
"Il dato, la sua disponibilità, integrità, accessibilità e la sua protezione diventano un tema centrale per il concetto di Sicurezza Nazionale nel suo senso più ampio" (Audizione MoD presso la IV Commissione Difesa della Camera dei Deputati, 23 gennaio 2025).
La gestione dei dati è pertanto un tema critico, visto che i dati sono il vero valore dietro ai sistemi basati sull'AI.
A livello strategico nel documento di policy - Strategia della Difesa in materia di Intelligenza Artificiale, recentemente firmato dal Sig. Ministro della Difesa (gennaio 2026), viene indicata chiaramente la necessità di mettere a sistema risorse umane e tecnologiche per implementare policy di data management e processi di data governance volte a valorizzare "il dato come asset strategico fondamentale [...]".
Stiamo riorganizzando la nostra struttura sia dal punto di vista organizzativo che da quello delle procedure di lavoro.
Le informazioni costituiscono il know-how organizzativo: è sui dati e sulle informazioni che essi rappresentano che prendiamo le decisioni. Perdere questi dati può significare perdere il vantaggio competitivo. Avere dati non affidabili ci impedirebbe di prendere decisioni adeguate. Se i dati sono manipolati, le decisioni saranno conseguentemente condizionate.
Per tale ragione cerchiamo di proteggere questo patrimonio informativo cercando di limitare al massimo ogni rischio di compromissione delle nostre banche dati. Per alcune applicazioni non possiamo accettare il rischio di utilizzare soluzioni Cloud non direttamente sotto il controllo della Difesa.

Intervento del Capo di Stato Maggiore dell'Aeronautica Militare Generale di Squadra Aerea Antonio CONSERVA

Evoluzione del Concetto di Sicurezza e Difesa

La sicurezza del nostro Paese oggi rappresenta una dimensione complessa e multi-dominio che attraversa lo spazio aereo, il cyberspazio, le infrastrutture critiche, le reti digitali, i sistemi logistici, sanitari ed energetici.

In questo nuovo scenario, l'Intelligenza Artificiale non è una tecnologia del futuro, ma una capacità strategica già oggi operativa.

Tuttavia occorre aver presente che l'IA non è una tecnologia neutra in quanto amplifica la capacità decisionale, accelera i processi critici e moltiplica l'impatto delle scelte umane. In ambiti strategici e di sicurezza, ogni algoritmo può tradursi in un'azione concreta, con conseguenze reali su persone, infrastrutture e sistemi complessi.

In un contesto in cui i volumi di dati crescono in modo esponenziale, l'IA consente di trasformare l'informazione grezza in conoscenza operativa. Permette di individuare pattern, correlazioni e segnali deboli che l'uomo, da solo, non potrebbe rilevare in tempi compatibili con le esigenze operative. Questo significa operare meglio, più velocemente e in maggiore sicurezza.

Dove cresce la potenza degli strumenti, deve però crescere allo stesso modo la responsabilità di chi li progetta, li controlla e li impiega. La sfida dell'Intelligenza Artificiale quindi è prima di tutto una sfida di responsabilità.

La questione dei Dati

L'IA non sostituisce l'uomo, ma lo potenzia. La centralità dell'essere umano resta infatti il principio cardine. L'elemento umano è e rimane insostituibile nella valutazione, nella responsabilità e nella decisione finale. L'Intelligenza Artificiale è uno strumento di supporto alla decisione, non un sistema che prende decisioni in autonomia. L'osservazione, l'orientamento, la decisione e l'azione restano saldamente nella responsabilità dell'uomo, secondo il principio circolare dell'Osservare, Orientare, Decidere e Agire (OODA Loop). Chi completa il ciclo più velocemente dell'avversario ottiene un vantaggio decisivo. L'obiettivo è "entrare dentro" l'OODA loop dell'avversario, agendo più rapidamente di quanto lui possa osservare e reagire. L'IA supporta e identifica, correla, analizza e traccia, ma l'azione resta sempre una scelta umana. Un algoritmo è affidabile solo quanto lo sono i dati con cui viene addestrato e questo dà adito ad una seconda grande sfida che dobbiamo affrontare come Forza Armata e come Paese: quella dell'intelligence e della qualità dei dati. La qualità dei risultati dell'Intelligenza Artificiale dipende direttamente dalla qualità dei dati, dalla loro rappresentatività e dalla loro validazione attraverso l'esperienza operativa. In questo quadro, il ruolo dell'intelligence è centrale. La raccolta delle informazioni, la loro selezione, la loro verifica e la costruzione di database strutturati e certificati rappresentano la base su cui poggia l'intera architettura dell'Intelligenza

Generale di Squadra Aerea Antonio CONSERVA

Artificiale. Senza dati affidabili non esiste previsione credibile, non esiste supporto decisionale efficace, non esiste automazione sicura. La costruzione dei database operativi è quindi una funzione strategica della sicurezza nazionale. L'IA non è un prodotto che si acquista, ma una capacità che si costruisce nel tempo, attraverso la conoscenza, l'esperienza operativa e l'intelligence.

Gap tecnologico e fabbisogni

L'Intelligenza Artificiale è oggi una realtà operativa nelle Forze Armate e in particolare nell'Aeronautica Militare. La Forza Armata ha compreso che l'IA non rappresenta una rivoluzione teorica, ma un moltiplicatore reale di sicurezza, efficienza e affidabilità. Una tecnologia che, se governata correttamente, rafforza la sovranità nazionale, tutela i cittadini e rende il Paese più resiliente.

È già allo studio avanzato nella manutenzione predittiva dei velivoli, nel monitoraggio dello stato di salute degli equipaggi, nell'analisi automatica dei flussi video e dei dati provenienti dai sensori, nel supporto alla sicurezza delle operazioni di volo. Non si tratta di sperimentazioni accademiche, ma di applicazioni concrete che migliorano ogni giorno l'efficienza e l'affidabilità delle capacità operative.

L'Intelligenza Artificiale moderna è una tecnologia ad altissima intensità di calcolo. Senza infrastrutture adeguate, l'IA resta una promessa incompiuta. In questo contesto, il sistema di High Performance Computing dell'Aeronautica Militare e il progetto di acquisizione del nuovo sistema HPC rappresentano un passaggio strategico fondamentale. L'HPC non è un semplice potenziamento informatico, ma l'infrastruttura abilitante dell'Intelligenza Artificiale. Grazie all'HPC è possibile addestrare modelli complessi su grandi volumi di dati, ridurre drasticamente i tempi di calcolo, simulare scenari operativi complessi, alimentare digital twin e ambienti

di sperimentazione, collegare i dati alle catene di progettazione e produzione. La velocità di calcolo diventa un moltiplicatore di capacità e consente di passare dal dato all'algoritmo, dall'algoritmo al prototipo e dal prototipo alla capacità operativa in tempi che oggi non sono ancora disponibili con le architetture tradizionali.
L'automazione è una leva straordinaria di efficienza, ma non può diventare delega della responsabilità. Gli automatismi devono essere governati, gli ingaggi devono restare sotto controllo umano, le decisioni critiche devono essere validate dall'uomo. L'IA deve essere una leva di affidabilità, non una scorciatoia tecnologica.

Ruolo STEM

Oggi l'Intelligenza Artificiale non è solo un elemento abilitante dell'operatività del Comparto Difesa, ma diventa un pilastro della sicurezza comune. Sicurezza comune significa protezione delle reti digitali, continuità dei servizi essenziali, resilienza delle infrastrutture, capacità di prevenire eventi critici, gestione delle emergenze, tutela delle catene logistiche e sanitarie. L'IA è uno strumento fondamentale per garantire questa nuova dimensione della sicurezza. In questo contesto si inserisce il Rapid Prototyping Warfare, che rappresenta il laboratorio operativo dell'innovazione in fase di realizzazione. Il RPW è il luogo in cui l'Intelligenza Artificiale diventa capacità applicata. È l'ambiente in cui la modellazione 3D, i digital twin e la simulazione avanzata si integrano con l'IA per progettare, sviluppare e sperimentare le tecnologie emergenti prima del loro impiego operativo. È il ponte tra ricerca e operatività, tra idea e capacità concreta, tra innovazione e sicurezza nazionale.
Il RPW consentirà di passare rapidamente dall'idea al prototipo, dal prototipo alla sperimentazione e dalla sperimentazione alla capacità operativa, accorciando drasticamente i tempi dell'innovazione. Sarà il luogo in cui verranno sviluppati e testati sistemi basati su IA per la cooperazione tra droni, il riconoscimento automatico dei bersagli, la protezione delle basi e dei velivoli, il supporto alle decisioni di volo.
Le tecnologie di Intelligenza Artificiale sviluppate in ambito militare generano ritorni diretti per il sistema Paese in termini di crescita industriale, sviluppo delle competenze, occupazione qualificata e innovazione tecnologica. Investire in Intelligenza Artificiale significa investire nella sicurezza nazionale, nella sovranità tecnologica e nella capacità dell'Italia di affrontare le sfide future con strumenti adeguati.
Per concludere, l'Intelligenza Artificiale e le sue applicazioni non sono più solo uno strumento operativo, ma una responsabilità verso i cittadini. Governare l'IA significa garantire un futuro più sicuro, più resiliente e più moderno per l'Italia. Significa dotare il Paese di strumenti in grado di proteggere le infrastrutture, le reti, i servizi essenziali e, soprattutto, le persone.
Perché la sicurezza comune non è un concetto astratto. È una missione quotidiana. È una responsabilità condivisa. È il fondamento della nostra sovranità e della nostra libertà. E l'Intelligenza Artificiale, se governata con competenza, visione e responsabilità, è uno degli strumenti più potenti che abbiamo per difenderle.

Intervento del Comandante Generale dell'Arma dei Carabinieri Generale di Corpo d'Armata Salvatore LUONGO

Generale di Corpo d'Armata
Salvatore LUONGO

La terza Conferenza Nazionale sulle discipline STEM rappresenta una straordinaria occasione per ribadire la fondamentale sinergia che unisce l'intero comparto Difesa. È anche la sede più appropriata per affermare con chiarezza che la sicurezza del futuro si costruisce oggi, nelle aule, nei laboratori, nelle scuole: è lì che si forgiano le menti che dovranno governare — e non subire — la rivoluzione tecnologica in atto.

Il sistema di Difesa e di Sicurezza nazionale affronta oggi molteplici e interconnessi fattori di rischio, e lo fa proprio attraverso i collaudati meccanismi di integrazione tra le Forze Armate e di coordinamento tra le Forze di Polizia, in un costante impegno sinergico di tutte le Istituzioni coinvolte. Questa condizione si raggiunge mediante un modello interforze integrato, che veda il pieno coinvolgimento non solo delle organizzazioni civili e del mondo accademico, ma anche del mondo dell'impresa, fattore trainante dello sviluppo tecnologico.

Non potendo essere fisicamente presente a Venezia, ho affidato il compito di illustrare nel dettaglio le applicazioni pratiche e formative dell'Arma al Vice Comandante Generale, il Gen. C.A. Marco Minicucci. Il suo intervento, che vi invito a leggere, testimonia concretamente il percorso di trasformazione della nostra Istituzione.

Desidero tuttavia cogliere l'occasione per condividere la visione strategica che guida l'Arma in questa transizione epocale.

Ci troviamo a operare in un'epoca di "policrisi", in cui non affrontiamo più fattori di instabilità isolati, ma un sistema complesso dove conflitti armati, tensioni economiche ed emergenze climatiche si intrecciano e si amplificano reciprocamente. A questo scenario si aggiungono le insidie poste dai nuovi domini: lo spazio, la dimensione cyber e cognitiva, l'ambiente underwater - frontiere largamente inesplorate, ricche di materie prime e cruciali per il controllo delle rotte commerciali e delle comunicazioni - nonché lo sviluppo di computer quantistici e dell'Intelligenza Artificiale, capaci di minare le basi stesse della sicurezza dei nostri sistemi e di ridisegnare in modo assoluto la sicurezza cibernetica, rendendo vulnerabili gli attuali modelli crittografici.

Di fronte a questa complessità, non è sufficiente reagire, ma occorre anticipare.

E per anticipare, occorre rinnovarsi. La strategia dell'Arma si fonda su un principio chiaro: l'innovazione non deve essere considerata un semplice aggiornamento tecnologico, ma un vero e proprio rinnovamento culturale. Dobbiamo spostare il nostro baricentro dalla semplice risposta all'anticipazione delle minacce. Per raggiungere il traguardo è indispensabile una rigorosa razionalizzazione delle risorse, da allocare non più per consuetudine ma secondo effettive necessità, sostenuta da una digitalizzazione spinta, essenziale per diminuire la burocrazia e trasformare il patrimonio informativo in decisioni operative immediate.
Per rispondere efficacemente a tali esigenze, stiamo investendo importanti risorse nella realizzazione di piattaforme avanzate di Comando e Controllo e nel potenziamento degli applicativi di analisi dei fenomeni criminali, implementando le capacità operative dei Reparti dedicati alla digital forensics e alla cyber investigation.
Ma per attuare questa visione, emerge un'esigenza vitale per le Forze Armate e per l'intero Sistema Paese: dobbiamo attrarre, formare e valorizzare i giovani talenti nelle discipline STEM. L'innovazione è un acceleratore decisivo del progresso sociale ed economico, ma per governarla servono investimenti mirati nelle competenze e la diffusione di una solida cultura digitale che sostenga l'adattamento continuo. Abbiamo bisogno di menti brillanti in grado di presidiare le nuove frontiere tecnologiche per garantire la sicurezza collettiva.
Sul fronte della trasformazione digitale dei processi operativi, un esempio concreto è il progetto che stiamo sviluppando con PagoPA SpA per la digitalizzazione delle denunce di smarrimento tramite App IO, con un sistema che libererà oltre un milione di ore-lavoro — risorse preziose che potranno essere restituite al territorio, alle indagini, alla prossimità con il cittadino.
L'Intelligenza Artificiale, in senso proprio, apre scenari ulteriori e più profondi. Stiamo già sviluppando soluzioni di IA per efficientare i processi interni, potenziare le capacità investigative dell'Arma e innovare i metodi di addestramento. Non si tratta di sperimentazioni isolate, ma di un approccio sistematico trasversale a tutte le funzioni istituzionali — dall'organizzazione territoriale alla tutela del patrimonio culturale e ambientale, dalla lotta alla criminalità informatica alla formazione del personale. L'obiettivo è costruire un'Istituzione che sappia usare l'intelligenza artificiale come moltiplicatore di capacità, senza mai delegare le decisioni che richiedono giudizio, responsabilità e coscienza.
In tutti questi ambiti, resta infatti centrale e insostituibile la componente umana. L'Intelligenza Artificiale sa cosa fa; il perché lo decide sempre e soltanto l'uomo. Nessun algoritmo potrà mai surrogare il contatto umano e il discernimento etico. È questa la lezione più importante che possiamo trarre dall'esperienza sul campo, e che deve orientare ogni scelta formativa: non formare esecutori di macchine, ma comandanti capaci di governarle.
Vi è infatti il rischio che i sistemi algoritmici incorporino bias latenti, generando trattamenti discriminatori; per questo diventa fondamentale progettare strumenti che favoriscano equità e inclusione. In un contesto così dinamico, i principi etici

e i valori fondanti della nostra Istituzione continueranno a essere il nostro scudo, mentre l'innovazione sarà il nostro motore, intesa non come un destino da subire ma come una sfida da governare.
Il filosofo Kant fece suo il celebre motto latino Sapere Aude: "Abbi il coraggio di servirti della tua propria intelligenza".
Allo stesso modo esorto i giovani talenti che oggi si avvicinano alle discipline scientifiche: siate audaci nello studio e rigorosi nel metodo, perché solo unendo il coraggio del cuore alla precisione della mente - la stessa sintesi che da sempre distingue il Carabiniere - potrete essere le sentinelle di una sicurezza che non dorme mai.


★ Scuola Navale Militare "Francesco MOROSINI" ★


★ Scuola Navale Militare "Francesco MOROSINI" ★


★ Scuola Navale Militare "Francesco MOROSINI" ★
LE DISCIPLINE
STEM
NELLA DIFESA
LA SFIDA DELL'INTELLIGENZA ARTIFICIALE E LA SICUREZZA COMUNE
4 FEBBRAIO 2026


LE DISCIPLINE
STEM
NELLA DIFESA
SFIDA DELL'
EZZA COMUNE

SECONDO PANEL

"Luci e ombre dell'Intelligenza Artificiale"

STEM

Intervento della Professoressa Barbara CAPUTO Ordinaria al Politecnico di Torino

Professoressa Barbara CAPUTO

Intelligenza Artificiale e Difesa: tra trasformazione tecnologica e sovranità

Parlare di Intelligenza Artificiale e difesa può sembrare, a prima vista, un esercizio che introduce una dimensione radicalmente nuova. In realtà, sotto molti aspetti, si tratta di una declinazione specifica di una trasformazione più ampia che riguarda tutte le grandi organizzazioni complesse contemporanee. L'intelligenza artificiale è infatti una tecnologia trasformativa — spesso definita dirompente — non tanto perché introduce qualcosa di completamente inedito, ma perché amplifica, accelera e rende scalabili dinamiche già presenti. Viviamo nel secolo del digitale. Che lo si consideri un progresso o una fonte di criticità, è un dato di fatto con cui ogni sistema organizzativo deve confrontarsi. I sensori sono ormai pervasivi e il loro costo è drasticamente diminuito. Rendere misurabili e quantificabili fenomeni che fino a pochi anni fa sfuggivano alla registrazione sistematica — dal battito cardiaco al respiro, fino alle nostre interazioni quotidiane — è diventato semplice, economico e diffuso.

Questo ha portato alla costruzione di un mondo fondato sui dati digitali. Ogni dato rappresenta un fatto, una traccia, un elemento osservabile della realtà. E, aspetto non secondario, una parte significativa di questi dati viene condivisa volontariamente, spesso senza una piena consapevolezza del loro valore e delle loro implicazioni. Si crea così una massa informativa di dimensioni senza precedenti.

Di fronte a questa disponibilità di dati, si apre una scelta fondamentale. Possiamo limitarci a raccoglierli senza utilizzarli, lasciandoli come residuo informativo — con il rischio che altri soggetti, pubblici o privati, li analizzino e ne traggano valore — oppure possiamo interrogarli, attribuire loro un significato, trasformarli in conoscenza e in capacità decisionale. È in questo passaggio che si colloca il ruolo dell'Intelligenza Artificiale.

Le quantità di dati oggi disponibili eccedono la capacità cognitiva umana di analizzarli in modo sistematico e scalabile. Questo non implica un limite qualitativo dell'intelligenza umana, ma evidenzia una complementarità: il cervello umano è straordinariamente efficace nell'interpretazione, nella creatività, nel giudizio contestuale; le macchine eccellono nella capacità di calcolo, nella ripetizione e nella

gestione di grandi volumi di informazione. L'Intelligenza Artificiale si inserisce esattamente in questo spazio di complementarità, come insieme di tecniche che consentono di estrarre struttura, pattern e significato da masse di dati altrimenti inaccessibili.

In questo senso, l'Intelligenza Artificiale non è soltanto uno strumento tecnologico, ma una componente sempre più centrale dei processi decisionali. Essa modifica il modo in cui le organizzazioni osservano la realtà, costruiscono conoscenza e prendono decisioni. Non sostituisce la responsabilità umana, ma ne cambia profondamente il contesto: introduce nuove possibilità di previsione, di simulazione, di anticipazione, ma anche nuove forme di rischio legate alla qualità dei dati, alla robustezza dei modelli e alla comprensibilità degli esiti.

Per una organizzazione come la difesa, questo si traduce nella necessità di interrogarsi in modo molto concreto su alcune dimensioni fondamentali: quali infrastrutture di calcolo adottare, come gestire e proteggere i dati, dove collocarli, come integrarli nei processi operativi, e soprattutto come trasformarli in vantaggio informativo e decisionale. La questione non è più se adottare o meno queste tecnologie — perché non è più una scelta — ma come governarne l'integrazione in modo coerente con gli obiettivi strategici, mantenendo al contempo la capacità di valutazione critica.

Questa trasformazione ha un impatto diretto anche sul concetto di sovranità. In un mondo che è simultaneamente fisico e digitale, il perimetro della Difesa si è ampliato in maniera significativa. Le infrastrutture critiche non sono più soltanto quelle visibili e tradizionali, ma includono anche reti invisibili e distribuite: cavi sottomarini, dorsali in fibra ottica, sistemi di comunicazione che sostengono il funzionamento quotidiano delle nostre società.

Si tratta di infrastrutture che attraversano spazi complessi e spesso difficilmente accessibili, come il dominio subacqueo, e che costituiscono una componente essenziale della sicurezza nazionale. La loro protezione non è un tema astratto, ma incide direttamente sulla vita dei cittadini, sulla continuità dei servizi, sulla stabilità economica. Difendere oggi significa, in larga misura, difendere il nostro quotidiano: il modo in cui comunichiamo, lavoriamo, accediamo all'energia, utilizziamo servizi digitali.

In questo contesto, il concetto di sovranità territoriale si estende oltre i confini geografici tradizionali e si proietta nello spazio digitale. Tuttavia, la sovranità digitale non può essere ridotta alla sola dimensione fisica della localizzazione dei dati o delle infrastrutture di calcolo. Questa è certamente una componente rilevante, ma non sufficiente.

La questione centrale riguarda la capacità di comprensione e di controllo. Possiamo dirci realmente sovrani se utilizziamo sistemi di cui non conosciamo il funzionamento? Se non siamo in grado di comprendere la logica che governa gli algoritmi su cui si basano decisioni critiche? Se il software che utilizziamo — spesso composto da milioni o miliardi di righe di codice — resta, di fatto, una "scatola nera"? La sovranità tecnologica richiede quindi un livello di competenza che va oltre il

semplice utilizzo. Non implica necessariamente la produzione autonoma di ogni tecnologia, ma richiede la capacità di comprenderla, di valutarla criticamente, di intervenire su di essa quando necessario. In altre parole, non si tratta di autarchia tecnologica, ma di indipendenza funzionale.

Un'analogia utile è quella con i mezzi militari tradizionali. Non ci si è mai aspettati che le Forze Armate producessero integralmente ogni piattaforma o sistema, ma è sempre stata considerata essenziale la capacità di manutenerli, comprenderli e gestirli in autonomia. Nel dominio digitale, questa esigenza si ripropone con ancora maggiore urgenza, perché la complessità e l'opacità dei sistemi possono generare forme di dipendenza meno visibili ma altrettanto rilevanti.

L'adozione dell'Intelligenza Artificiale nella Difesa deve quindi essere accompagnata da un investimento significativo nelle competenze: competenze tecniche, certamente, ma anche capacità di integrazione tra dimensione tecnologica e strategica. È necessario sviluppare una cultura che consenta di utilizzare queste tecnologie in modo consapevole, mantenendo il controllo sui processi e sulle decisioni, e preservando la responsabilità ultima dell'azione.

In ultima analisi, l'Intelligenza Artificiale non è semplicemente una tecnologia da adottare, ma un fattore che ridefinisce il rapporto tra conoscenza, potere e decisione. Per la Difesa, questo significa ripensare non solo gli strumenti, ma anche i modelli organizzativi, i processi e le competenze. Significa riconoscere che la superiorità non si gioca più soltanto sulla dimensione fisica, ma sempre più sulla capacità di interpretare, governare e, quando necessario, mettere in discussione l'informazione su cui si fondano le decisioni.

Intervento di Padre Paolo BENANTI
Presidente della Commissione Intelligenza Artificiale per l'Informazione della Presidenza del Consiglio

Padre Paolo BENANTI

Intervengo volentieri su questo tema partendo da una prospettiva che mi è propria, a metà tra la riflessione filosofica e una formazione di tipo ingegneristico. Quando parliamo di Intelligenza Artificiale, infatti, non stiamo semplicemente parlando di uno strumento: stiamo parlando di qualcosa che incide profondamente sul modo in cui l'essere umano esercita le proprie capacità cognitive. Non esiste tecnologia che sia davvero comprensibile se non a partire dall'uomo che la utilizza.

Per questo motivo, ogni discorso sull'Intelligenza Artificiale è inevitabilmente anche un discorso sull'umano. E, in particolare, su come cambiano i nostri processi cognitivi nell'interazione con questi sistemi. Mi piace usare una metafora semplice: quando il nostro stile di vita è diventato più sedentario, abbiamo sentito il bisogno di introdurre le palestre per mantenere la forma fisica. Oggi, in modo analogo, abbiamo bisogno di una sorta di "palestra mentale", perché l'uso continuo di sistemi intelligenti rischia di modificare — e talvolta indebolire — alcune nostre capacità cognitive.

Non è un fenomeno del tutto nuovo. Già in passato abbiamo delegato alcune funzioni alla tecnologia: penso, ad esempio, alla memoria dei numeri di telefono, che molti di noi hanno smesso di esercitare con l'introduzione delle rubriche digitali. Tuttavia, oggi il livello della delega è molto più profondo: non riguarda più soltanto abilità marginali, ma investe direttamente i processi decisionali.

Ed è qui che emerge un primo punto fondamentale: l'essere umano deve rimanere titolare della decisione, soprattutto in ambiti strategici e delicati come quello della difesa. Ma questo non si realizza semplicemente limitando l'automazione. Richiede, piuttosto, un lavoro su due piani. Da un lato, dobbiamo preservare e rafforzare la nostra capacità decisionale; dall'altro, dobbiamo comprendere come questa capacità possa essere influenzata — o anche alterata — dall'interazione con sistemi di Intelligenza Artificiale.

Allo stesso tempo, non possiamo ignorare il fatto che queste tecnologie rappresentano anche una straordinaria opportunità. In molti contesti, l'Intelligenza Artificiale può offrire una vera e propria "risoluzione cognitiva" a problemi concreti, come la carenza di competenze altamente specializzate. Pensiamo, ad esempio, alla possibilità di

supportare personale non esperto, in contesti remoti, attraverso sistemi digitali avanzati capaci di guidare interventi complessi. In questo senso, l'AI non sostituisce l'uomo, ma ne estende le capacità operative.
Tuttavia, proprio per questo, non è sufficiente introdurre nuove tecnologie: è necessario ripensare i processi e, in molti casi, anche le strutture organizzative. Il modo in cui umano e macchina collaborano non è dato automaticamente, ma dipende da come questa collaborazione viene progettata.
A questo proposito, trovo utile richiamare la distinzione tra diversi livelli del nostro funzionamento cognitivo. Sappiamo che esistono modalità rapide e intuitive di risposta e modalità più lente e riflessive. Una buona formazione dovrebbe rendere ciascuno capace di passare consapevolmente dall'una all'altra, a seconda del contesto.
L'Intelligenza Artificiale introduce però un ulteriore elemento, che potremmo definire come una sorta di "livello zero": un sistema che, se non progettato con attenzione, tende a orientare automaticamente il comportamento dell'utente verso determinate scelte.
Questo ci porta a riconoscere che la progettazione delle interfacce e delle modalità di interazione non è un fatto neutro. Al contrario, è uno degli atti più rilevanti — e, direi, più politici — del nostro tempo. Le interfacce guidano l'attenzione, suggeriscono percorsi decisionali, influenzano il comportamento. E se questi sistemi sono progettati con obiettivi che non coincidono con il pieno sviluppo delle capacità umane, si genera una tensione che diventa particolarmente critica in ambiti sensibili.
Infine, vorrei richiamare un rischio molto concreto: quello della non compatibilità tra i tempi della macchina e i tempi dell'essere umano. Esistono già oggi sistemi che, da un lato, incentivano una delega ampia — ad esempio permettendo all'utente di distrarsi — e, dall'altro, richiedono un intervento umano in tempi estremamente ridotti. Questa dinamica non è compatibile con i limiti cognitivi reali delle persone e mette in evidenza quanto sia necessario progettare tecnologie che tengano conto, in modo serio, della natura umana.
In definitiva, la sfida che abbiamo davanti non è soltanto tecnologica. È una sfida antropologica e culturale: si tratta di comprendere come integrare queste nuove capacità senza perdere ciò che rende propriamente umano il nostro modo di conoscere, decidere e agire.*

**trascrizione dell'intervento non revisionata dal relatore*


LE DISCIPLINE
STEM

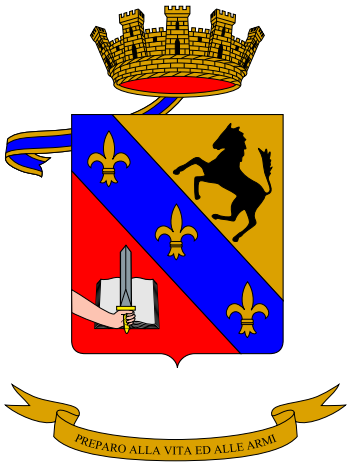
TERZO PANEL

"Applicazioni STEM a scenari di crisi simulati"

PARTE PRIMA

Presentazione dei progetti degli Allievi di Scuole Militari, Scuole Sottufficiali e Accademie delle Forze Armate, dell'Arma dei Carabinieri e della Guardia di Finanza

STEM



Progetti **STEM**
Scuole militari

Visione artificiale per la sorveglianza di infrastrutture strategiche

ENTE

Scuola Militare Nunziatella

Scenario di simulazione cyber e supporto AI
Simulazione operativa di risposta a minaccia cyber su infrastruttura mission-critical con supporto IA

L'esercizio svolto dalla Scuola Militare Nunziatella illustrerà una simulazione operativa di difesa cyber sviluppata nell'ambito della Terza Conferenza sulle Discipline STEM nella Difesa, dedicata al tema "La sfida dell'Intelligenza Artificiale e la sicurezza comune".

Lo scenario di riferimento è un contesto di confronto ad alta intensità, coerente con le missioni di difesa del territorio nazionale, nel quale viene ipotizzata una minaccia cyber coordinata, deliberatamente progettata per operare sotto la soglia di attribuzione certa, sfruttando ambiguità tecniche e temporali.
L'esercitazione si svolge su un'infrastruttura mission-critical simulata, rappresentata da una centrale elettrica, protetta da difese informatiche standard e da sensori eBPF (extended Berkeley Packet Filter) dedicati al monitoraggio comportamentale dei sistemi. La finalità è valutare la capacità di rilevamento precoce, analisi e decisione in presenza di minacce avanzate, senza impatti sulla continuità dei servizi essenziali (come strutture sanitarie o altre infrastrutture critiche ecc).

Durante la simulazione, i sensori eBPF rilevano un'anomalia significativa riconducibile a una reverse shell, ovvero una minaccia non identificata, tramite un processo, sta tentando di stabilire una connessione verso un sistema esterno. L'evento viene identificato in modo puntuale attraverso parametri tecnici (Process ID, comando eseguito, indirizzo IP e porta di destinazione), consentendo una rapida qualificazione della minaccia.
Sulla base di tale evidenza, viene attivato un ciclo immaginato dagli allievi, di analisi e decisione, che integra:

- dati forniti dai sensori,
- supporto dell'Intelligenza Artificiale,
- valutazione e responsabilità decisionale umana.

All'interno di tale ciclo è impiegato il Nunziatella AI Assistant, un assistente di Intelligenza Artificiale progettato ad hoc per l'esercizio, basato su modelli linguistici della famiglia Gemini e distillato dagli allievi specificamente per il contesto operativo simulato. L'assistente svolge un ruolo di supporto analitico e, interrogato tramite un prompt strutturato, fornisce:

- una valutazione del rischio,
- un supporto al decision making,

- un piano di mitigazione operativo, comprensivo di azioni tecniche per il contenimento dell'evento (terminazione del processo malevolo, isolamento della sorgente esterna, verifica di eventuali meccanismi di persistenza).

Contestualmente, l'IA esegue un'analisi avanzata dei flussi comportamentali, individuando un Pattern of Life anomalo e ipotizzando una possibile compromissione indiretta di un operatore interno.

La decisione finale resta in capo all'elemento umano, che dispone l'immediata interruzione dell'azione ostile. Viene esplicitamente verificato che la soluzione AI non interferisce con i processi operativi della centrale elettrica e non compromette la continuità della fornitura energetica verso infrastrutture critiche, quali strutture sanitarie e servizi essenziali. L'evento viene quindi classificato come tentativo di esfiltrazione dati, non come sabotaggio operativo.
Su indicazione dell'IA, viene avviata un'indagine interna di sicurezza, che conduce all'individuazione della causa primaria della compromissione: la creazione di un hotspot Wi-Fi fraudolento, esterno ai sistemi della centrale ma utilizzato per compromettere un dispositivo personale di un operatore, consentendo la fuga di informazioni.

Le conclusioni sottolineano un principio fondamentale: l'Intelligenza Artificiale non sostituisce il comando umano, ma ne potenzia l'efficacia. L'IA agisce come moltiplicatore di capacità – rileva, correla e accelera – mentre l'uomo mantiene il controllo decisionale, l'interpretazione del contesto e la responsabilità dell'azione.
La simulazione dimostra la validità di un modello integrato uomo–AI nella protezione delle infrastrutture critiche, evidenziando come l'uso corretto dell'Intelligenza Artificiale possa diventare un moltiplicatore cognitivo, in grado di accelerare il processo decisionale mantenendo il controllo umano quale elemento centrale del sistema di difesa.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=8936 (2:29:00 – 2:38:15)

SCUOLA MILITARE NUNZIATELLA

ESERCITO

TERZA CONFERENZA
LE DISCIPLINE STEM NELLA DIFESA

«La sfida dell'Intelligenza Artificiale e la sicurezza comune»

Venezia, 04/02/2026

AGENDA

ESERCITO

- SCENARIO ED ESERCIZIO ASSEGNATO
- NUNZIATELLA BLUE TEAM & AI
- COMPETENZE E CONOSCENZE
- PROCESSO DI ANALISI E DECISIONE
- SIMULAZIONE ATTACCO E ATTIVAZIONE CICLO
- RISPOSTA AI VS VALUTAZIONE UMANA
- CONCLUSIONI

SCENARIO ED ESERCIZIO ASSEGNATO

Scenario di confronto ad alta intensità per difesa del territorio nazionale
1^ missione: difesa dello Stato
Minaccia cyber

Una minaccia non identificata ha avviato un'operazione cyber coordinata, progettata per rimanere parzialmente sotto la soglia di attribuzione certa, sfruttando ambiguità tecniche e temporali.

L'esercizio si svolgerà su un'infrastruttura *mission-critical* simulata, ovvero una **CENTRALE ELETTRICA**, protetta da difese standard e da sensori ***extended Berkeley Packet Filter (EBPF)*** per il monitoraggio comportamentale.

NUNZIATELLA BLUE TEAM & AI


COMPETENZE E CONOSCENZE
ESERCITO
Spicy
LEONARDO
Telsy
A TIM ENTERPRISE BRAND
Napul.ETH
YouTube
coursera
Hugging Face
reddit
OPEN SOURCE
• Laboratori coding e IA
• Hackaton
• Laboratori di realtà aumentata
• Cyber Sec
• Laboratorio di penetration test
• Blockchain
• Web 3
• Quantum Computing
CAMPO DIGITALE 2025
PASSIONE


PROCESSO DI ANALISI E DECISIONE
ESERCITO
Difese Standard
Antivirus
IDS
Infrastruttura Mission-Critical Simulata
CENTRALE ELETTRICA
ATTIVAZIONE CICLO
Sensori eBPF
HUM
SENSORE
Valutazione e Decisione
FASE 5
Analisi e correlazione
FASE 1
Rilevamento azione anomala
(notifica variazione insolita)
FASE 2
Prompt nell'IA
FASE 3
Opzioni di risposta dell'IA
FASE 4
AI
SENSORE
HUM

SIMULAZIONE ATTACCO
FASE 1 E FASE 2

ATTACCO

Analisi e correlazione
FASE 1

Rilevamento azione anomala
FASE 2

Notifica variazione insolita

REVERSE SHELL DETECTED! PID: 1920 | CMD: shell.elf | REMOTE: 192.168.122.88:6166

SPIEGAZIONE REVERSE SHELL

ESERCITO

REVERSE SHELL DETECTED! PID: 1920 | CMD: shell.elf | REMOTE: 192.168.122.88:6166

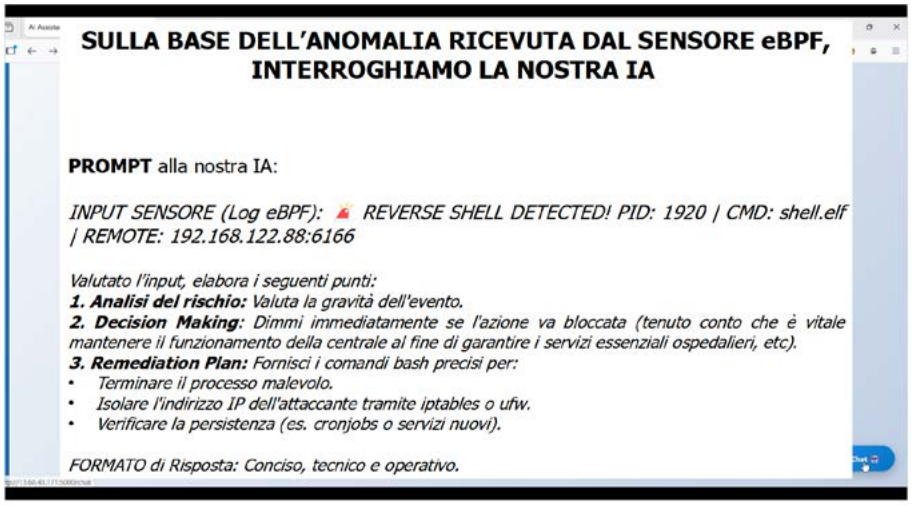
REVERSE SHELL DETECTED: un processo **sta tentando** di aprire una connessione verso l'esterno.

PID: 1920 Process ID è il numero identificativo del «processo» che sta cercando di aprire una connessione verso l'esterno.

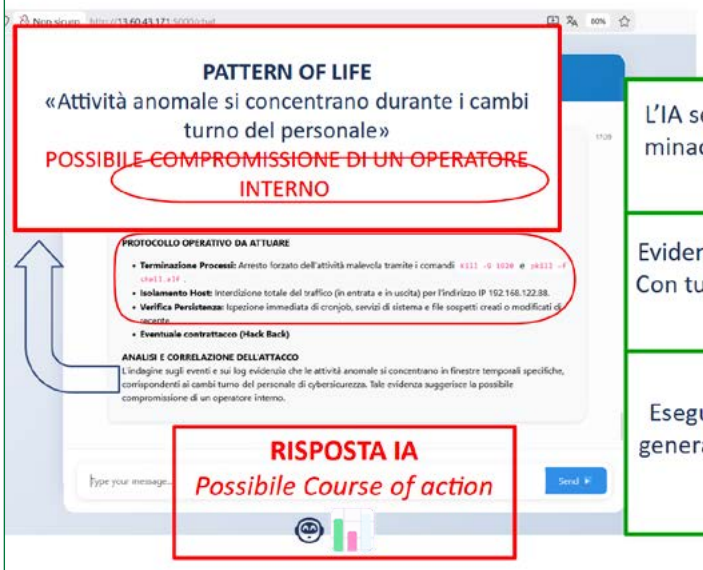
CMD: shell.elf indica il comando eseguito dal «processo» 1920

REMOTE: 192.168.122.88:6166
Il «processo» 1920 ha aperto una connessione verso l'esterno, precisamente verso l'IP 192.168.122.88 sulla porta 6166. Questo è l'indirizzo del presunto attaccante.

FASE 3 - PROMPT NELLA NOSTRA IA



FASE 4 :RISPOSTA IA

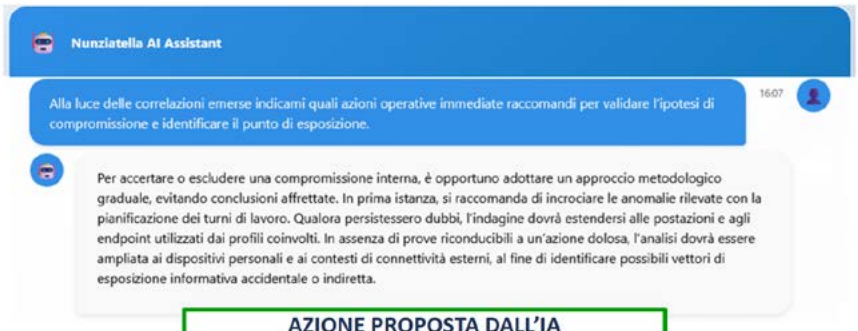


L'IA segnala l'anomalia come una probabile minaccia e suggerisce un'azione immediata per neutralizzarla

Evidenzia un protocollo operativo da attuare Con tutti i comandi per bloccare l'operazione ostile

Esegue un'analisi avanzata sui flussi di dati generati dai sensori per la modellazione del **Pattern of Life**

FASE 4 ULTERIORE PROMPT ALL'IA



AZIONE PROPOSTA DALL'IA
AVVIO INVESTIGAZIONE INTERNA CON ANALISI DI TUTTI I DISPOSITIVI DI LAVORO E PRIVATI DEL PERSONALE DELLA CENTRALE ELETTRICA

FASE 5 VALUTAZIONE E DECISIONE UMANA

PROPOSTA DELL'AI *Possibile Course of action*		DECISIONE UMANA
L'azione è probabilmente ostile e l'obiettivo è, verosimilmente, il furto di dati.	**È possibile che un ostile attacchi la centrale? SI.**	Procedere come indicato dall'AI.
Interrompere immediatamente la probabile azione malevola.	**La soluzione AI interferisce con i processi operativi della centrale elettrica e ha impatti sulla disponibilità energetica dei servizi critici connessi, come strutture sanitarie o altre infrastrutture essenziali? No.**	Eseguire i comandi suggeriti dall'AI.
Avviare un'indagine interna al fine di individuare la fonte di informazioni dell'ostile.	**È possibile che un operatore sia stato compromesso? SI.**	Mettere in atto il consiglio dell'AI

RISULTATO INVESTIGAZIONE

EXERCISE

WIFI

GRATIS

SCAN CODE WITH YOUR PHONE'S CAMERA

NETWORK

TERZA_CONFERENZA_STEM

PASSWORD

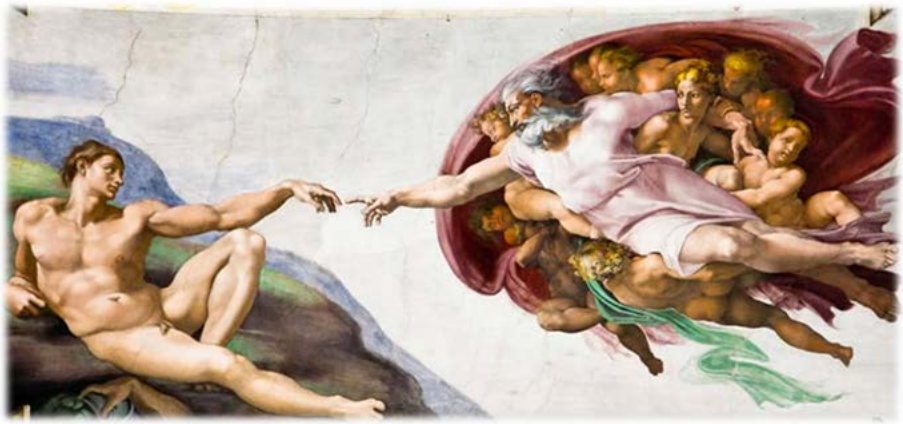
123456

EXERCISE

COMPROMESSO **IL WIFI** DEL BAR DELLA CENTRALE ELETTRICA

Creato un finto hotspot con lo stesso nome di quello legittimo e hackerato il telefono del personale di vigilanza con conseguente fuga di dati

CONCLUSIONI



INTELLIGENZA ARTIFICIALE E GIUDIZIO UMANO

L'IA non è Dio.

E non è nemmeno Adamo.

CONCLUSIONI

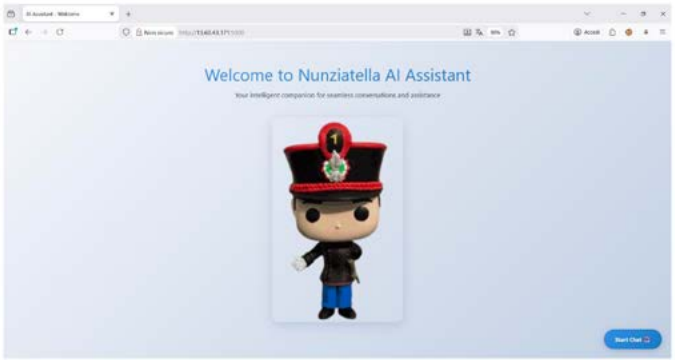
ESERCITO

Solo la mente umana «che per sua natura si diletta delle cose divine, infinite ed eterne, non può non aspirare alle sublimi, tentare le grandi, compiere le straordinarie»

Cit. G. Vico, De mente heroica, 1732

CONCLUSIONI

EMAIL: ctecp2@scuolana.esercito.difesa.it



Allievi Scuola Militare Nunziatella

ENTE

Scuola Militare Teulié

Visione artificiale per la sorveglianza di infrastrutture strategiche

Contesto

Una caserma di artiglieria terrestre appartenente all'Esercito Italiano è stata oggetto di un improvviso attacco nemico condotto mediante l'utilizzo di razzi a medio raggio. L'azione ostile ha provocato ingenti danni a veicoli tattici, munizioni e armamenti, depositi logistici e infrastrutture interne alla base, compromettendo temporaneamente la piena operatività dell'unità di artiglieria.
A seguito dell'attacco, il comando della caserma si trova nella necessità immediata di acquisire in tempi rapidi informazioni accurate sull'accaduto al fine di rafforzare le misure di sicurezza, prevenire e contrastare eventuali ulteriori azioni offensive. È indispensabile disporre di dati aggiornati e affidabili per identificare la provenienza dei razzi, valutare l'entità dei danni e pianificare le azioni di contenimento e difesa più efficaci, in attesa di supporto delle unità alleate.

Obiettivo

Per rispondere a tali esigenze, l'obiettivo prioritario è lo sviluppo di un sistema automatizzato di sorveglianza e raccolta dati basato sull'impiego di una rete di droni e sensori distribuiti all'interno ed esterno della caserma. Questi droni, equipaggiati con telecamere multispettrali e sensori di ultima generazione, permettono un monitoraggio continuo del perimetro e la raccolta in tempo reale di immagini e termogrammi.
L'integrazione dell'intelligenza artificiale con la rete senziente costituirà il cuore del sistema consentendo l'elaborazione automatica delle informazioni acquisite per l'analisi dei danni, e la rilevazione e la previsione di minacce. Tale architettura può garantire una costante sorveglianza del perimetro, assicurando al comando della caserma l'aggiornamento della situational awareness fino all'arrivo dei rinforzi alleati e al pieno ripristino delle condizioni operative.

IL MODELLO DI VISIONE ARTIFICIALE

Lo sviluppo di un modello di visione artificiale per il rilevamento automatico di minacce terrestri deve essere inteso come un sistema di analisi predittiva, capace di trasformare immagini e flussi video provenienti dai droni in informazioni strutturate e immediatamente utilizzabili dal comando per semplificare il processo decisionale.
Il modello non si limita a "riconoscere" ciò che è presente in una scena, ma deve anche localizzarlo nello spazio attraverso bounding box, cioè riquadri che identificano con

precisione la posizione degli oggetti rilevati all'interno dell'immagine o del frame video.
L'input è costituito da immagini statiche o da stream video acquisiti dai sensori di bordo dei droni. Queste immagini provengono da telecamere infrarosse e multispettrali (sensori che catturano immagini in specifiche bande dello spettro elettromagnetico, inclusi l'infrarosso e l'ultravioletto) per analizzare proprietà chimico-fisiche degli oggetti invisibili all'occhio umano, così da aumentare la capacità di individuazione anche in condizioni difficili, come scarsa illuminazione, fumo, polvere o mimetizzazione. Il dato grezzo, tuttavia, non è direttamente interpretabile da un sistema intelligente: è necessario un modello che estragga automaticamente le informazioni visive rilevanti.

Il primo stadio fondamentale del modello è la convoluzione. Con questo termine si indica un'operazione matematica mediante la quale dei filtri, detti kernel convoluzionali, vengono confrontati sull'immagine. Ogni kernel è specializzato nell'individuare determinati pattern locali, ovvero strutture visive elementari.
Nei livelli iniziali della rete, la convoluzione permette di riconoscere elementi molto semplici come bordi, contorni, variazioni di intensità luminosa o differenze cromatiche. Queste informazioni di base sono essenziali perché costituiscono i "mattoni" con cui, negli strati successivi, il modello può riconoscere forme sempre più complesse. Ad esempio, combinando bordi e angoli, la rete può iniziare a individuare sagome compatibili con un veicolo militare o con una figura umana armata. In questo senso, la convoluzione rappresenta il meccanismo attraverso cui il modello impara a "vedere" in modo progressivamente più astratto e significativo.

Successivamente, nella fase di pooling, si sintetizzano le informazioni estratte mantenendo solo quelle importanti e scartando i dettagli meno rilevanti e ridondanti. Il pooling riduce il rumore e rende il modello più robusto a piccole variazioni dell'immagine, come spostamenti, rotazioni leggere o parziali occlusioni degli oggetti. Questo aspetto è cruciale in uno scenario warfare, dove truppe e mezzi possono essere parzialmente nascosti da edifici, vegetazione o macerie. Grazie al pooling, il modello non dipende da una rappresentazione perfettamente nitida dell'oggetto ma riesce a riconoscerlo anche quando solo alcune parti sono visibili, ovvero rende trascurabili elementi "di disturbo" come il fumo prodotto da un'esplosione.
Una volta completate le fasi di convoluzione e pooling, le informazioni visive sono ancora organizzate sotto forma di matrici bidimensionali, che rappresentano la distribuzione spaziale delle feature nell'immagine. Per poterle utilizzare nelle fasi successive è necessario il flattening.

Il flattening consiste nella trasformazione di queste matrici 2D in un vettore monodimensionale (cioè una forma semplificata e compatta delle informazioni estratte da un'immagine). Non si tratta di un'operazione di interpretazione, ma di una

riorganizzazione dei dati che consente di passare da una rappresentazione spaziale a una forma adatta agli strati successivi del modello. In pratica, il flattening prepara le informazioni estratte affinché possano essere elaborate da un classificatore.
La fase di classificazione rappresenta il momento in cui il modello attribuisce un significato semantico alle informazioni visive. Attraverso strati neurali completamente connessi, il sistema combina le feature apprese per stimare la probabilità che una determinata regione dell'immagine contenga una specifica categoria di oggetto.
In un contesto di rilevamento, la classificazione non produce solo un'etichetta globale per l'intera immagine, ma opera su porzioni localizzate, associando a ciascun bounding box una classe, come "militare", "carro armato", "veicolo tattico" o "altra minaccia terrestre", insieme a un valore di confidenza che indica quanto il modello è sicuro della propria previsione. Questo approccio consente al comando di avere non solo l'informazione sulla presenza di una minaccia, ma anche la sua posizione precisa nello spazio osservato.
Nel caso di stream video, il modello può sfruttare anche la continuità temporale, confrontando frame successivi per migliorare l'affidabilità del rilevamento. Se un oggetto viene parzialmente nascosto o temporaneamente occluso, la sua presenza può essere comunque osservata grazie alla predizione del movimento nel tempo. In questo modo, la visione artificiale diventa dinamica e adattiva, capace di mantenere il tracciamento delle minacce anche in scenari complessi e in rapido mutamento.
Applicato a compiti come il rilevamento di nemici da immagini aeree, il monitoraggio continuo di aree critiche, l'analisi dei danni alle infrastrutture o il riconoscimento di attività sospette, un modello di visione artificiale strutturato secondo questo schema consente di trasformare l'enorme quantità di dati visivi raccolti dai droni in una consapevolezza situazionale aggiornata e affidabile. In questo senso, ogni passaggio del processo, dalla convoluzione alla classificazione, contribuisce a costruire una rappresentazione sempre più ricca e significativa del campo operativo, supportando le decisioni del comando.

SVILUPPO DEL MODELLO DI VISIONE ARTIFICIALE

Il processo di sviluppo del modello di visione artificiale si articola in quattro fasi principali:

1. Raccolta dati e database

La prima fase del piano è la raccolta dei dati e la costruzione del dataset. Si realizza un dataset che rappresenti fedelmente la complessità dello scenario reale della caserma e delle aree circostanti colpite dall'attacco. Le immagini e i video vengono acquisiti da diverse fonti, tra cui droni impiegati sia a diverse altezze di quota per osservare il perimetro e le aree interne della base, camere fisse installate nei punti sensibili, immagini satellitari utili a fornire una visione d'insieme. Il dataset

include sia situazioni semplici, in cui veicoli tattici, depositi logistici e infrastrutture strategiche risultano chiaramente visibili, sia casi più complessi caratterizzati da occlusioni dovute a edifici danneggiati, vegetazione, fumo, polvere o detriti.
L'etichettatura avviene mediante annotazione manuale delle bounding box sugli elementi di interesse secondo linee guida uniformi, includendo esempi in cui gli oggetti sono solo parzialmente visibili e, ove possibile, registrando un valore che indichi il grado di occlusione. Il dataset viene infine suddiviso in insiemi di addestramento, validazione e test, con la creazione di un sottoinsieme di test dedicato ai casi di occlusione leggera, media e forte, così da consentire analisi mirate delle prestazioni del modello.

2. Addestramento supervisionato con data augmentation

La seconda fase riguarda l'addestramento supervisionato del modello con l'ausilio di tecniche di data augmentation, fondamentali per aumentare la robustezza del sistema in condizioni operative reali. A partire dalle immagini etichettate grazie alla prima fase, il modello apprende le caratteristiche visive degli asset e dei danni, mentre le operazioni di incremento dei dati permettono di simulare situazioni che possono verificarsi nello scenario post-attacco ma che non sono sempre presenti in numero sufficiente nel dataset originale. Vengono applicate tecniche di mascheramento casuale di porzioni dell'immagine per riprodurre l'effetto di fumo, polvere, vegetazione o ostacoli strutturali, così da abituare il modello a riconoscere gli oggetti anche in presenza di occlusioni parziali.
L'uso di mosaic e MixUp consente di aumentare la varietà dei contesti e di migliorare il rilevamento di target di piccole dimensioni, mentre variazioni realistiche di blur, rumore, compressione e luminosità simulano il degrado della qualità visiva dovuto alle condizioni ambientali.
Le operazioni di resize e variazione di scala riproducono diverse distanze e altitudini di acquisizione, mentre rotazioni e cambi di prospettiva moderati favoriscono la generalizzazione del modello a punti di vista differenti da quelli osservati in fase di addestramento.

3. Scelta del modello e pipeline di training

La terza fase del piano è la scelta del modello di object detection e la definizione della pipeline di training. Si adotta un approccio basato su reti neurali convoluzionali, selezionando un detector moderno in funzione dei vincoli di tempo di risposta e delle esigenze di accuratezza. Una configurazione di base viene utilizzata come punto di partenza e sottoposta a più cicli di addestramento e ottimizzazione, durante i quali vengono regolati parametri quali la soglia di confidenza, il bilanciamento tra precisione e recall (accuratezza e completezza), la dimensione dell'input e la strategia di aggiornamento dei pesi.
La pipeline prevede una valutazione continua delle prestazioni, con particolare attenzione ai risultati ottenuti sui dati che presentano occlusioni, al fine di individuare

tempestivamente eventuali criticità. L'uso di meccanismi di early stopping (uno dei metodi di regolarizzazione per reti neurali più comuni ed efficaci) e il monitoraggio costante delle metriche consentono di prevenire fenomeni di overfitting, garantendo che il modello mantenga una buona capacità di generalizzazione su scenari e condizioni differenti da quelli osservati durante il training.

4. Valutazione e criteri di accettazione

L'ultima fase riguarda la valutazione del modello e la definizione dei criteri di accettazione. Le prestazioni vengono misurate su dati nuovi, mai associati al modello, attraverso metriche standard come mAP (mean Average Precision), precision e recall, analizzando separatamente i risultati ottenuti sul dataset complessivo e sul sottoinsieme (subset) dedicato alle occlusioni.
Un'analisi dettagliata degli errori consente di individuare le principali cause di falsi positivi, ad esempio dovuti alla presenza di veicoli o strutture visivamente simili, e di falsi negativi legati a fumo, ombre, camouflage o dimensioni ridotte dei target. Sulla base di queste analisi vengono definite soglie minime di accettazione, come valori di recall e mAP ritenuti sufficienti a garantire un supporto informativo affidabile.
Il modello viene considerato idoneo solo se dimostra stabilità delle prestazioni su scenari diversi e un degrado controllato nei casi di occlusione più severa, assicurando così un contributo concreto alla comprensione della situazione operativa senza sostituirsi al giudizio umano.

COME L'AI PUÒ AIUTARE RISPETTO AL PIANO ELABORATO

L'intelligenza artificiale può offrire un contributo significativo al supporto delle attività di analisi e alla costruzione della situational awareness.
L'AI consente di automatizzare l'analisi di grandi quantità di immagini e flussi video, attività che risulterebbe onerosa e lenta se svolta esclusivamente da operatori umani, soprattutto in uno scenario caratterizzato da molteplici fonti di acquisizione.
In particolare, il sistema è in grado di evidenziare rapidamente la possibile presenza di asset di interesse, riducendo il carico di lavoro degli operatori e permettendo loro di concentrarsi sulle verifiche e sulle valutazioni più complesse.
Grazie alla sua capacità di operare in modo continuo, l'AI rende possibile un monitoraggio persistente ventiquattr'ore su ventiquattro, applicando criteri di analisi coerenti e ripetibili nel tempo. Questo contribuisce a ridurre la variabilità soggettiva e ad aumentare la stabilità delle osservazioni.
Inoltre, in base alle modalità di deploy (le strategie tecniche e le procedure utilizzate per rilasciare, installare e rendere operativo un sistema software o un'applicazione negli ambienti di produzione), il sistema può segnalare eventi sospetti o variazioni significative in tempi molto ridotti, accelerando i tempi di reazione informativa.
L'AI è anche in grado di produrre report strutturati e statistiche aggregate, come la distribuzione spaziale degli asset rilevati o la loro frequenza di comparsa, informazioni

utili per attività di pianificazione e valutazione complessiva della situazione (esempio output: Stato Munizioni: 45% delle scorte danneggiate/inutilizzabili; Veicoli Operativi: 6/12 veicoli d'artiglieria ancora pienamente operativi; Tempo di Ripristino Stimato: Stima automatica basata sui danni rilevati).
Infine, il sistema consente un miglioramento progressivo nel tempo, poiché i casi validati o corretti dagli operatori possono essere reinseriti nel ciclo di addestramento, contribuendo ad aumentare la robustezza e l'affidabilità del modello nelle successive iterazioni.

DOVE L'AI NON RISULTA APPLICABILE

L'intelligenza artificiale, pur rappresentando un valido supporto tecnologico, non sostituisce in alcun modo la responsabilità decisionale umana e presenta limiti strutturali che devono essere esplicitamente considerati nel piano elaborato.
In particolare, l'AI può fallire quando opera in condizioni che si collocano al di fuori del dominio dei dati utilizzati durante l'addestramento. Questo accade, ad esempio, in presenza di contesti non rappresentati nel dataset, come l'introduzione di nuovi mezzi mai osservati prima, l'utilizzo di sensori con caratteristiche differenti rispetto a quelli di training o condizioni ambientali estreme che alterano in modo significativo l'aspetto visivo della scena. In tali situazioni il modello può produrre errori difficilmente prevedibili, poiché le sue inferenze si basano su correlazioni apprese e non su una reale comprensione del contesto.
Inoltre, nelle decisioni critiche l'AI deve rimanere necessariamente uno strumento di supporto e non un decisore autonomo: il principio del man in the loop garantisce che l'output del sistema venga sempre interpretato, validato e contestualizzato da un operatore umano. Esistono poi casi di forte ambiguità visiva, come ombre, rottami, strutture danneggiate o veicoli visivamente simili, in cui anche un modello ben addestrato può confondere classi diverse o fornire risultati incerti, rendendo indispensabile una verifica umana.
Infine, la qualità insufficiente dei dati di input, dovuta a bassa risoluzione, forte compressione, frame degradati o acquisizioni instabili, limita direttamente l'affidabilità delle predizioni, riducendo il valore informativo del sistema e imponendo cautela nell'interpretazione dei risultati.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=9521 (2:39:00 – 2:44:08)


AI
MODELLO DI VISIONE ARTIFICIALE PER LA SORVEGLIANZA DI UN'INFRASTRUTTURA STRATEGICA
INTEGRAZIONE DELL'IA CON UNA RETE SENZIENTE DI DRONI E TELECAMERE

CONTESTO

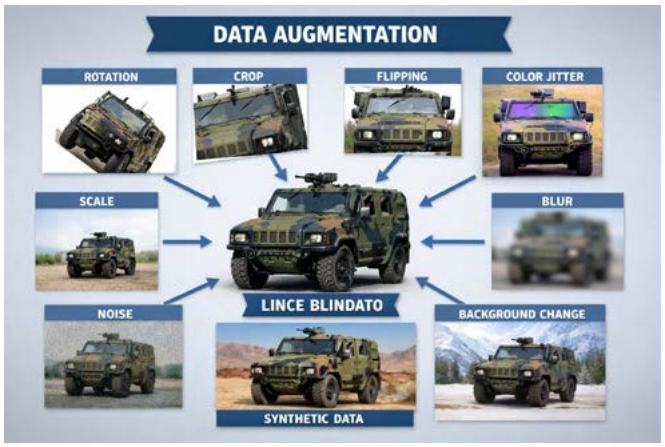
MODELLO DI VISIONE ARTIFICIALE

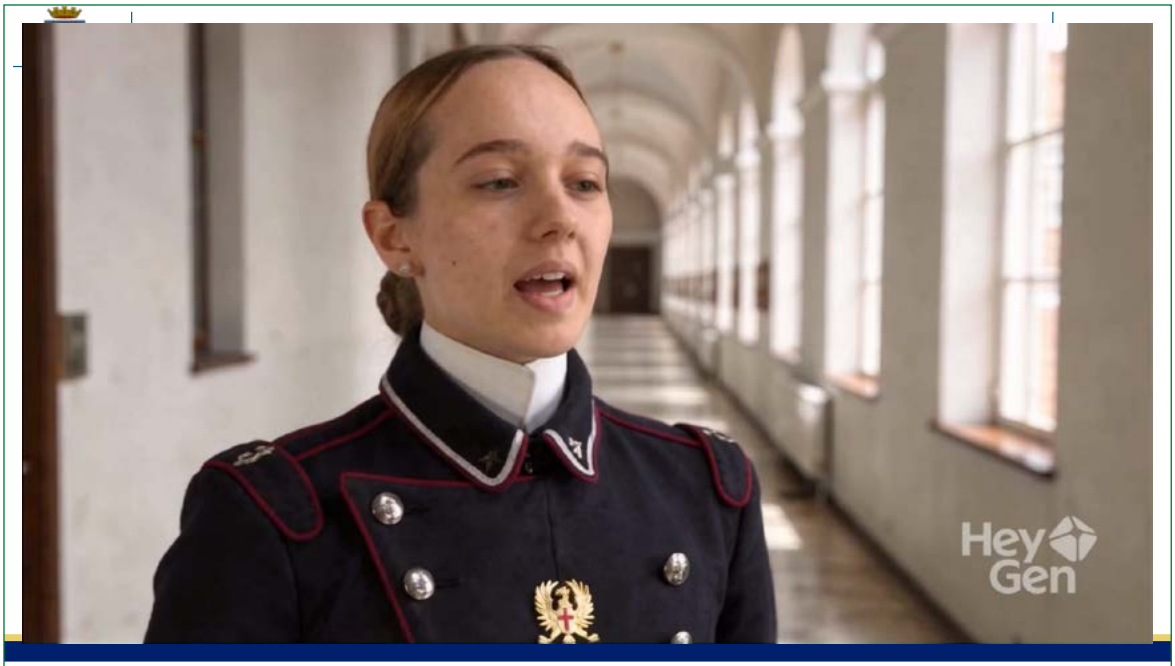
4 FASI

- CONVOLUZIONE
- *POOLING*
- *FLATTERING*
- CLASSIFICAZIONE

SVILUPPO DEL MODELLO

- RACCOLTA DATI E DATASET
- ADDESTRAMENTO SUPERVISION CON DATA *AUGMENTATION*
- SCELTA DEL MODELLO E *PIPELINE* DI *TRAINING*
- VALUTAZIONE E CRITERI DI ACCETTAZIONE





Allievi Scuola Militare Teuliè

ENTE

Scuola Navale Morosini

L'intelligenza Artificiale a supporto delle infrastrutture critiche sottomarine

Introduzione (slide 1)

I rischi connessi a sabotaggi e ad attacchi ai danni alle infrastrutture critiche sottomarine (CUI – Critical Underwater Infrastructure) rappresentano oggi una crescente preoccupazione tanto per i governi nazionali quanto per le organizzazioni internazionali. Appare quindi impellente la necessità di sviluppare e implementare sistemi tecnologicamente avanzati che aumentino ed ottimizzino la sorveglianza e la protezione delle reti di approvvigionamento energetico e delle dorsali digitali che si snodano per migliaia di chilometri nelle profondità marine, aumentando la capacità di raccogliere ed elaborare nel più breve tempo possibile informazioni accurate relative alla dimensione subacquea (UWSA – UnderWater Situational Awareness). L'impiego di soluzioni ed assetti tecnici e cibernetici avanzati, con particolare riferimento a sistemi sottomarini a pilotaggio remoto e all'Intelligenza Artificiale, risulta imprescindibile alla luce dell'estesa superficie da proteggere (impossibile da presidiare con personale umano) e delle complesse condizioni chimico-fisiche dell'ambiente sottomarino.
Nell'esercizio da noi sviluppato abbiamo dapprima delineato gli obiettivi strategici difensivi che si intendono perseguire nel dominio marittimo e successivamente abbiamo ipotizzato un piano d'azione basato sul supporto dell'Intelligenza Artificiale, individuando vantaggi e potenziali limiti dell'impiego di tale strumento.

Obiettivi (slide 2)

La difesa delle pipeline di diversa natura risulta un obiettivo prioritario per un Paese ad alto sviluppo tecnologico e digitale come il nostro. Nello specifico, le principali CUI a rischio nel contesto geopolitico del nostro Paese sono:

- i gasdotti provenienti dall'Africa e dall'Asia che passano sui fondali del Canale di Sicilia e del mar Adriatico;
- gli elettrodotti che collegano la penisola alle due isole maggiori e ai Balcani;
- i cavi di comunicazione sottomarini in fibra ottica che collegano il Paese agli Stati rivieraschi.

Per garantire il continuo stato di efficienza di questa fitta rete di infrastrutture poste nelle profondità degli abissi e la prevenzione da danneggiamenti non intenzionali (quali, per esempio, l'ancoraggio di navi) ma, soprattutto, per scongiurare atti mirati di sabotaggio da parte di attori ostili, è necessario da un lato incrementare le capacità di prevenzione tramite un monitoraggio costante di quanto avviene sotto la superficie e, dall'altro, mettere a punto celeri protocolli di risposta per neutralizzare possibili minacce ed, eventualmente, mitigarne i danni.

Piano d'azione (slide 3)

Il piano d'azione da noi ipotizzato si articola sull'impiego combinato di assetti statici e dinamici:

- per quanto riguarda gli assetti statici, essi sono costituiti da un'ampia gamma di sensori subacquei, quali sonar e idrofoni, collocati in prossimità delle condotte con compiti di allerta precoce (early warning) e di superficie, nello specifico boe con sensori acustici e boe che fungono da relay nella trasmissione dei dati raccolti. Tali barriere difensive hanno la funzione di rilevare l'avvicinamento di una possibile minaccia e di inviare i dati analizzati ai centri di Comando e Controllo (C2);
- gli assetti dinamici invece si distinguono tra assetti manned, ossia con personale umano a bordo (es. sommergibili) e unmanned, ossia a pilotaggio remoto. La first response alla minaccia è delegata a droni subacquei appartenenti sia alla categoria dei mezzi subacquei a pilotaggio remoto (UUV – Underwater Unmanned Vehicle) sia alla categoria dei mezzi sottomarini autonomi (AUV – Autonomous Underwater Vehicle), con i secondi che differiscono dai primi per una marcata capacità di azione indipendente e di autonomia di analisi proprio grazie all'integrazione dell'Intelligenza Artificiale. Quest'ultimo assetto in particolare quindi, impiegando sistemi di Visione Artificiale, è incaricato dell'identificazione e della classificazione di oggetti e attività potenzialmente ostili.

Piano d'azione (slide 4)

AUV e UUV potrebbero agire con continuità sui fondali mediante il posizionamento di alcune stazioni di ricarica (docking station), le quali svolgerebbero anche la funzione di nodo collettore per la trasmissione dei dati raccolti durante l'attività di pattugliamento. La neutralizzazione della minaccia avverrebbe secondo un protocollo articolato su più fasi, con le prime che vedrebbero l'impiego di sistemi soft kill quali falsi bersagli e disturbatori, per poi procedere a forme di ingaggio cinetico qualora le prime contromisure dovessero rivelarsi inefficaci. In ultima battuta è previsto infine l'impiego di Unità Navali con personale a bordo specializzate nel contrasto a minacce specifiche (es. Unità ASW, cacciamine).

IA - Vantaggi (slide 5)

Passiamo ora a sintetizzare i vantaggi di questo tipo di impiego dell'Intelligenza Artificiale. In primo luogo, come già detto, simili assetti permetterebbero il monitoraggio continuativo di decine di migliaia di km di condotte e tubature, riducendo drasticamente il personale richiesto per una simile funzione. In secondo luogo, le capacità computazionali dell'IA permetterebbero di raccogliere, analizzare, integrare e trasmettere una grossa mole di dati in tempi brevissimi, permettendo quindi la definizione di un quadro di situazione comune (COP - Common Operational

Picture) costantemente aggiornato e dettagliato. La stessa Intelligenza Artificiale, in base ai dati raccolti, sarebbe in grado di supportare il processo decisionale indicando le migliori opzioni di reazione alla minaccia.

Conclusioni: i limiti dell' IA (slide 6)

Permangono tuttavia delle criticità nell'impiego di un simile strumento. Innanzitutto l'ambiente underwater appare soggetto ad una quantità di variabili climatiche, oceanografiche e metereologiche che rappresentato una sfida sia alla navigazione che alle comunicazioni tra gli assetti remotizzati e i centri di C2 sulla terraferma. Inoltre fattori di carattere etico e giuridico, specie per quanto riguarda le azioni di ingaggio, richiedono che il decisore umano sia coinvolto quantomeno nelle vesti di supervisore, secondo il principio human-in-the-loop, con la conseguente dilatazione dei tempi di reazione. Sussiste inoltre il rischio di Data Poisoning: nel dettaglio, l'Intelligenza Artificiale potrebbe essere ingannata tramite l'uso di una strategia elusiva di lungo periodo che prevede la somministrazione calibrata di dati da parte del soggetto ostile, al fine, di fatto, di rendere la minaccia "familiare" all'IA fino a non farla più identificare come minaccia in quanto tale. Infine, la possibile adozione di regole di ingaggio eccessivamente permissive rischierebbe di scatenare escalation indesiderate, qualora gli AUV neutralizzino autonomamente eventuali bersagli valutati ostili.

Slide 7

Animazione da noi realizzata con un programma di rendering che illustra il nostro piano difensivo.

Slide 8

Video da noi realizzato con l'ausilio dell'IA che illustra il nostro piano difensivo.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=9853 (2:44:20 – 2:52:30)

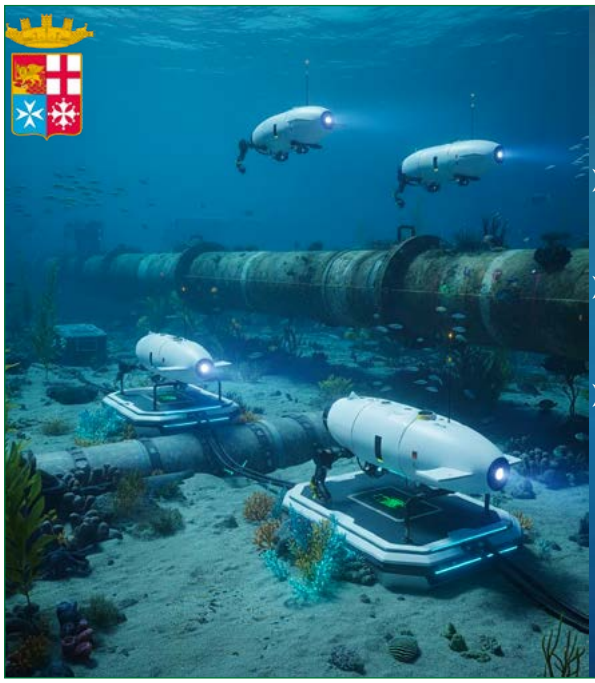

L'IA A SUPPORTO DELLE INFRASTRUTTURE CRITICHE SOTTOMARINE


AI
OBIETTIVI
Garantire flusso di materie prime e servizi essenziali
Sorvegliare e proteggere le CUI (Critical Underwater Infrastructure) da atti di sabotaggio
Aumentare la UWSA (UnderWater Situational Awareness)
Fornire reazioni tempestive ed efficaci contro potenziali minacce

AI

PIANO D'AZIONE

- Sensori statici distribuiti (sonar, idrofoni, boe) con funzione di *Early Warning*
- Impiego di AUV e UUV (*Autonomous/ Unmanned Underwater Vehicle*) con capacità di *manned-unmanned teaming*
- Identificazione e classificazione di oggetti, attività e anomalie tramite modelli di Visione Artificiale (raccolta e analisi dei dati gestiti da IA)



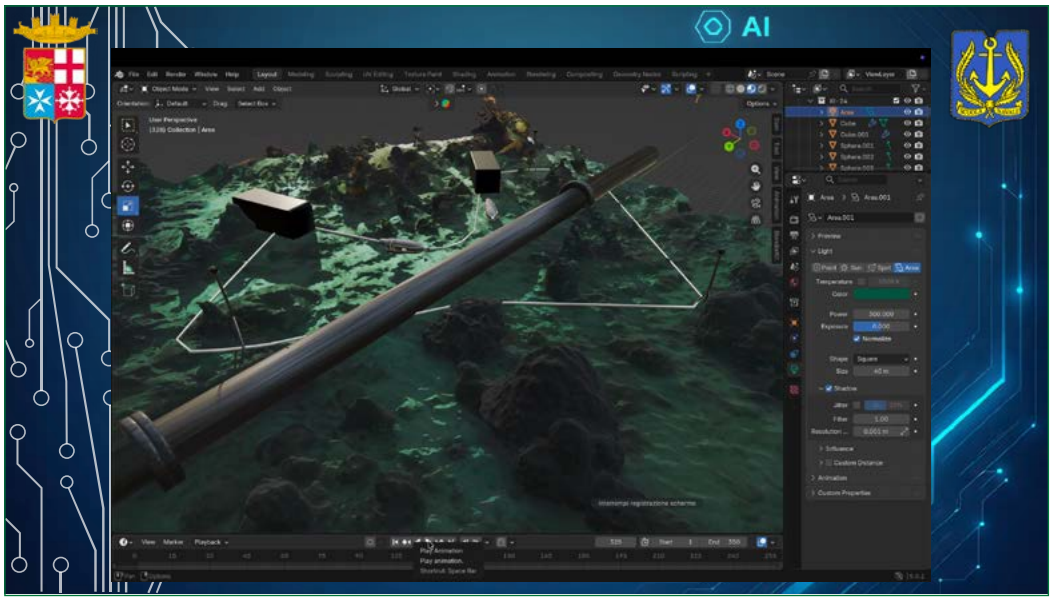
AI

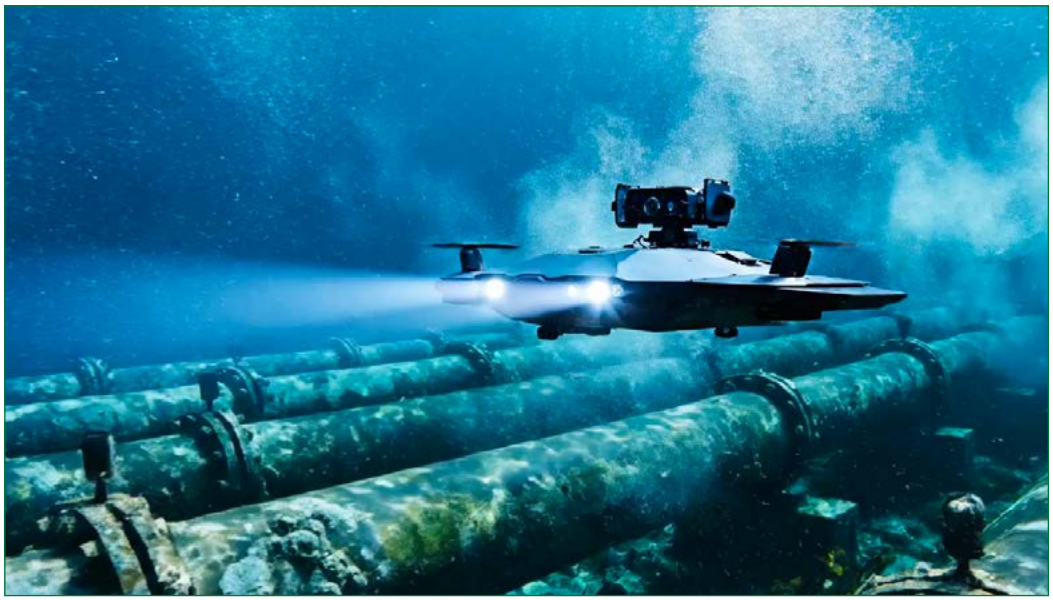
PIANO D'AZIONE

- *Docking station* posizionate sui fondali per le operazioni di ricarica e invio veloce dei dati
- *Decoy* acustici e disturbatori per inibire la minaccia
- Sistemi di ingaggio cinetico (*hard kill*) e dispiegamento delle Unità Navali


AI
IA - VANTAGGI
➢ Monitoraggio continuativo di aree estese
➢ Analisi automatizzata e trasmissione dei dati *real time* o *near real time* ai centri di Comando e Controllo
➢ Analisi dei danni e valutazione della *best response*
➢ Supportare e accelerare il processo decisionale


CONLUSIONI: LIMITI DELL'IA
➢ Possibili errori di identificazione (ambiente complesso)
➢ Decisioni critiche di ingaggio basate sul principio *human-in-the-loop*
➢ *Data poisoning*
➢ Escalation involontaria


AI




L'IA A SUPPORTO DELLE
INFRASTRUTTURE
CRITICHE SOTTOMARINE

Allievi Scuola Navale Morosini

ENTE

Scuola Militare Aeronautica Douhet

WARGAME – Scenario per le Scuole Militari

Confronto ad alta intensità per difesa del territorio nazionale - (1^Missione: Difesa dello Stato): Una potenza regionale ostile ha lanciato un'operazione su larga scala contro la Nazione. Si dispone di difese fisse, supporto aereo limitato oltre a un supporto da parte di Paesi alleati.

1. Scenario proposto dalla Scuola Militare Aeronautica "G. Douhet"

Una potenza regionale ostile ha avviato un conflitto aperto contro l'Italia con un obiettivo chiaro: ottenere un vantaggio rapido degradando il nostro sistema difensivo, prima dell'arrivo dei rinforzi alleati.
In particolare, il nemico non mira a occupare stabilmente il territorio bensì a negare l'uso diinfrastrutture critiche in primis i grandi aeroporti strategici colpendo:

- piste;
- carburanti;
- centri C2;
- flussi logistici.

Un aeroporto strategico non è solo una pista, è un sistema complesso con molte vulnerabilità: anche se parzialmente danneggiato, deve rimanere funzionalmente utilizzabile.
Le modalità di attacco del nemico includono.

- attacchi aeromissilistici e con UAS;
- saturazione delle difese;
- guerra elettronica e cyber;

Passando al sistema difensivo nazionale, l'Italia dispone di

- difese fisse sul territorio, ma con risorse limitate;
- supporto aereo nazionale ridotto da impiegare in maniera selettiva;
- supporto alleato garantito, ma non immediato.

2. Strategia difensiva nazionale

L'obiettivo dell'esercizio è pianificare e valutare una strategia difensiva volta a:

- mantenere il controllo di infrastrutture critiche;
- garantire la continuità operativa degli assetti essenziali;
- consentire l'arrivo e l'integrazione dei rinforzi alleati.

Il successo non è definito dalla sconfitta immediata dell'avversario, ma dalla tenuta del sistemadifensivo nazionale fino all'arrivo dei rinforzi alleati.
In questo contesto, la strategia difensiva sarà impostata sull'utilizzo di strumenti di AI intesi non come sistema autonomo di comando, ma come strumento di supporto al processo decisionale volto a:

- Supportare analisi importanza obiettivi in termini di weakness/strength;
- Dislocamento difese fisse a copertura obiettivi maggiormente sensibili;
- Supporto decisionale tattico per impiego assetti aerei e alleati in fase difensiva.

3. Sviluppo esercizio

Il nostro lavoro è stato incentrato sullo sviluppo di un modello progettato in Python al fine di creare un tool AI avanzato di simulazione decisionale per la difesa integrata di una base aerea militare in uno scenario di guerra ad alta intensità.

Come case study, abbiamo preso la base aerea di Gioia del Colle, sede del 36° Stormo dell'Aeronautica Militare Italiana, che dispone di due piste parallele (14L/32R e 14R/32L), taxiway centrale, apron, hangar rinforzati, shelter per velivoli, centro di comando, radar e batterie missilistiche.

In caso di attacco su larga scala da parte di una potenza regionale ostile (missili balistici, cruise, sciami di droni, incursioni aeree), la difesa si articola secondo il concetto di layered defense, integrando intelligenza artificiale per il supporto decisionale in tempo reale.

Il modello da noi teorizzato prevede un sistema difensivo basato sull'utilizzo dell'intelligenza artificiale al fine di gestire:

- Il Rilevamento e l'allarme precoce dai radar a lungo raggio (RAT-31DL, Kronos), link con AWACS alleati e dati ISR, fusi dall'AI per classificare le minacce e fornire early warning. Il ruolo dell'AI è di identificare vettori d'attacco e attiva immediatamente la dispersione dei velivoli e l'allerta delle difese.
- L'intercettazione a lungo raggio: le batterie SAMP/T ingaggiano per prime i missili balistici e cruise ad alta quota. L'AI ottimizza il weapon-target pairing, assegnando i bersagli in base a probabilità di abbattimento e priorità (protezione di piste e taxiway). I missili intercettori vengono lanciati in sequenza coordinata.
- Il Combat Air Patrol (CAP): gli Eurofighter Typhoon decollano rapidamente, armati con missili Meteor e AMRAAM, per intercettare minacce aeree e droni residui. L'AI supporta la gestione della CAP, indicando vettori ottimali e priorità di ingaggio.
- La Difesa Ravvicinata e Guerra Elettronica: Sistemi CAMM-ER, SHORAD e C-RAM contrastano le minacce a bassa quota. Unità di guerra elettronica attivano jamming RF/IR, spoofing GPS/INS e decoy gonfiabili per deviare o ingannare i seeker nemici.
- La Protezione Passiva e Ripristino: Velivoli sono posizionati in shelter rinforzati; carburante e munizioni distribuiti in siti ridondanti. In caso di impatto, team di ingegneri specializzati eseguono riparazioni rapide (crater repair su piste, ripristino infrastrutture critiche). L'AI ricalcola l'operatività residua e indica le priorità di intervento e i tempi previsti.

La difesa è progettata per mantenere un livello operativo sufficiente a generare sortite aeree continue, assorbire ondate multiple di attacco e guadagnare tempo fino all'arrivo

dei rinforzi alleati. L'impiego sistematico dell'AI per fusion di dati, ottimizzazione degli ingaggi e analisi di resilienza riduce significativamente il rischio di mission kill, trasformando risorse limitate in una capacità difensiva coerente e sostenibile.
In caso di danneggiamenti parziali causati da attacchi (es. crateri su piste, danni a taxiway, hangar o radar), la strategia si concentra su un ripristino rapido e prioritizzato per ripristinare un livello operativo minimo (almeno 50-70% per generare sortite aeree) entro 12-48 ore, evitando una completa interruzione delle operazioni.
L'approccio sopra descritto, basato sulla dottrina NATO per la resilienza, impiega l'intelligenza artificiale al fine di ottimizzare le risorse attraverso:

1. La valutazione immediata dei danni: Utilizzare droni di ricognizione e sensori ISR per mappare i danni. L'AI (tramite criticality analysis e simulazioni Monte Carlo) calcola l'operatività residua globale, identifica i nodi critici colpiti (es. taxiway principale come single point of failure) e genera priorità di intervento.
2. L'Isolamento e Sicurezza dell'Area: Evacuare personale non essenziale dalle zone danneggiate. Attivare protocolli di decontaminazione se sospetti agenti CBRN. Mantenere una CAP ridotta con gli assetti disponibili per prevenire attacchi secondari durante il ripristino.
3. Il calcolo dei tempi di ripristino delle infrastrutture critiche:
   - Piste e Taxiway: Team ingegneristici specializzati (NATO Rapid Runway Repair) riempiono crateri con materiali rapidi (es. cemento fibroso o mattonelle prefabbricate). Tempo stimato: 6-24 ore per pista parzialmente operativa. Priorità assoluta per almeno una pista e taxiway alternativo.
   - Centro di Comando e Radar: Ripristino ridondante con unità mobili (es. radar trasportabili). L'AI ricalcola flussi operativi per bypassare nodi danneggiati.
   - Hangar, Shelter e Depositi: Dispersione residua dei velivoli e carburante in siti alternativi. Riparazioni strutturali con kit prefabbricati; tempo: 12-36 ore.
   - Batterie SAM: Sostituzione moduli danneggiati con scorte pre-posizionate; integrazione con sistemi alleati per copertura temporanea.
4. La gestione logistica e delle risorse: Convogliare rifornimenti via elicotteri o convogli terrestri da basi alleate. L'AI ottimizza l'allocazione di manodopera e materiali.
5. Il Mantenimento Operativo Transitorio: Ridurre sortite a missioni essenziali (ISR, CAP limitata). Utilizzare piste parziali o atterraggi alternativi. L'AI supporta la pianificazione COA per massimizzare il tempo guadagnato fino ai rinforzi alleati.
6. Il Post-Ripristino: una volta stabilizzata (operatività >70%), condurre debrief con AI per analizzare vulnerabilità e aggiornare modelli difensivi. Integrare feedback per future simulazioni. Questa strategia di lesson-learned minimizza il downtime, sfrutta ridondanze e AI per decisioni datadriven, garantendo la continuità della difesa territoriale fino all'arrivo dei rinforzi.

4. Conclusioni

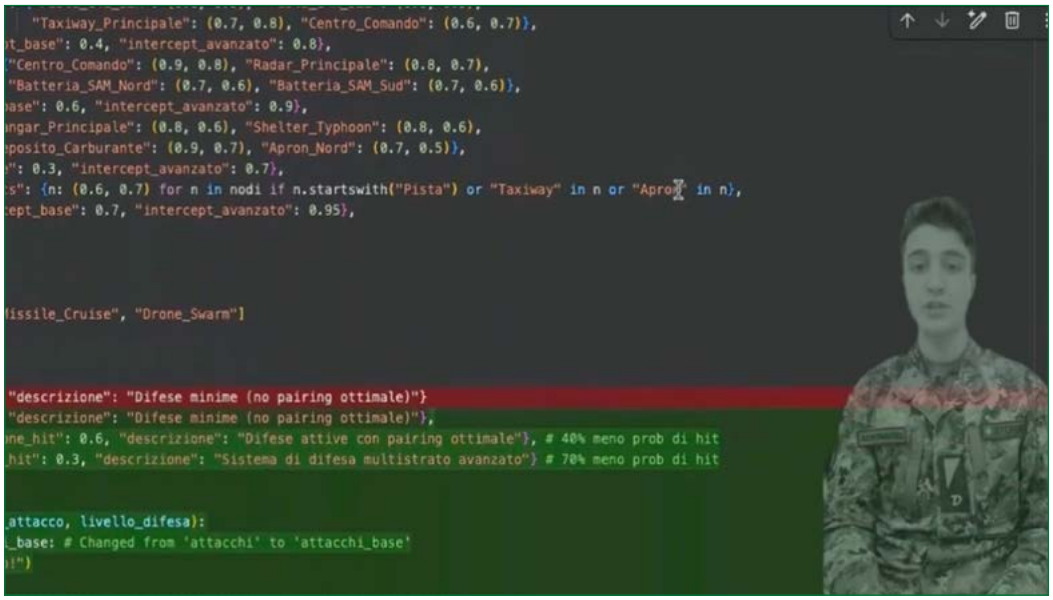
In conclusione, il modello di simulazione progettato in Python delinea un nuovo paradigma per la difesa aerea integrata, trasformando la risposta militare da puramente reattiva a strategicamente resiliente. L'intelligenza artificiale agisce come il nucleo di un ecosistema multi-layered, capace di orchestrare in tempo reale la fusione di dati ISR e civili, ottimizzando il weapon-target pairing e riducendo l'asimmetria dei costi rispetto alle minacce di saturazione.

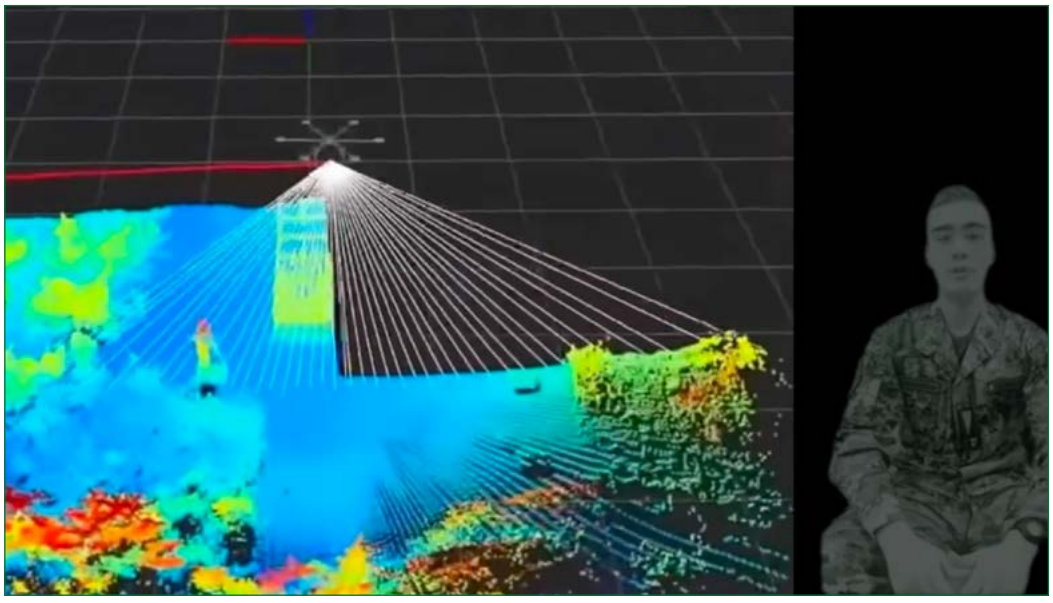
Il valore distintivo di questo algoritmo risiede nella sua natura omnicomprensiva: esso non si limita alla sola gestione tattica della difesa, ma integra un modulo analitico avanzato per calcolare la percentuale di danno sulle zone critiche e stimare con precisione i tempi di ripristino delle aree colpite.

Grazie a simulazioni Monte Carlo e analisi di criticità, lo strumento è in grado di mappare la vulnerabilità di qualsiasi infrastruttura aeroportuale, garantendo la continuità delle sortite aeree.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=10368 (2:53:00 – 2:58:05)


BYTE BACK:AI DEFENSE
In caso di attacco su larga scala da parte di una potenza regionale ostile, la difesa italiana si articola secondo il concetto di multi-layered defense, integrando intelligenza artificiale per il supporto decisionale in tempo reale.


"Taxiway_Principale": (0.7, 0.8), "Centro_Comando": (0.6, 0.7)},
t_base": 0.4, "intercept_avanzato": 0.8},
"Centro_Comando": (0.9, 0.8), "Radar_Principale": (0.8, 0.7),
"Batteria_SAM_Nord": (0.7, 0.6), "Batteria_SAM_Sud": (0.7, 0.6)},
ase": 0.6, "intercept_avanzato": 0.9},
ngar_Principale": (0.8, 0.6), "Shelter_Typhoon": (0.8, 0.6),
posito_Carburante": (0.9, 0.7), "Apron_Nord": (0.7, 0.5)},
": 0.3, "intercept_avanzato": 0.7},
s": {n: (0.6, 0.7) for n in nodi if n.startswith("Pista") or "Taxiway" in n or "Apron" in n},
ept_base": 0.7, "intercept_avanzato": 0.95},
issile_Cruise", "Drone_Swarm"]
"descrizione": "Difese minime (no pairing ottimale)"}
"descrizione": "Difese minime (no pairing ottimale)"},
ne_hit": 0.6, "descrizione": "Difese attive con pairing ottimale"}, # 40% meno prob di hit
_hit": 0.3, "descrizione": "Sistema di difesa multistrato avanzato"} # 70% meno prob di hit
attacco, livello_difesa):
_base: # Changed from 'attacchi' to 'attacchi_base'
!")



Allievi Scuola Militare Areonautica Douhet

STEM

Progetti **STEM**
Scuole Sottufficiali

Oltre l'orizzonte del contagio

ENTE

Scuole Sottufficiali EI, MM, AM, Arma CC

Scenario di emergenza epidemiologica (3^ Missione: Supporto in emergenza nazionale)

Un'epidemia di una malattia infettiva si è diffusa rapidamente nel territorio Nazionale, causando il collasso parziale dei servizi sanitari civili. Il governo ha attivato il piano di emergenza nazionale e ha richiesto il supporto delle forze armate per:

- supportare ospedali sovraccarichi;
- garantire continuità di servizi essenziali;
- gestire l'ordine pubblico;
- coordinare evacuazione e quarantena.

Si dispone di strutture logistiche, capacità di trasporto e personale medico.
Obiettivo dell'esercizio: pianificare un'operazione di supporto al dispositivo sanitario nazionale, in coordinamento con autorità civili, servizi sanitari e comunità locali.

Introduzione

Intervento dell'Arma dei Carabinieri

Il progetto sviluppato dagli allievi della Scuola Marescialli e Brigadieri dei Carabinieri, denominato GEN-LAMBDA26 propone un sistema di supporto alle decisioni basato su Intelligenza Artificiale, sviluppato nell'ambito dello scenario di emergenza epidemiologica nazionale, in coerenza con la Terza Missione delle Forze Armate: supporto alla popolazione e alle istituzioni in situazioni di crisi.
La soluzione si fonda su un'architettura modulare e multilivello, composta da un chatbot centrale di coordinamento e da sotto-bot specializzati per dominio funzionale, progettati per fornire informazioni affidabili, orientare il processo decisionale e ridurre l'incertezza informativa in contesti ad alta complessità. Il sistema integra dati provenienti da fonti aperte (OSINT) e, in ambienti autorizzati, da fonti chiuse (CLOSINT), adattando contenuti e funzionalità in base al profilo dell'utente e al livello di autorizzazione.

Attraverso una dimostrazione operativa, il progetto evidenzia la capacità del sistema di analizzare l'intento dell'utente, indirizzare automaticamente le richieste verso i moduli competenti e garantire coerenza informativa tra livelli istituzionali e cittadini. A supporto delle attività sul campo, il progetto prevede l'integrazione di dispositivi di realtà aumentata dotati di Intelligenza Artificiale (AI-GLASS ARMA), in grado di acquisire e trasmettere in tempo reale parametri ambientali e individuali rilevanti ai fini del controllo epidemiologico e delle attività di polizia. Tali dispositivi consentono, in scenari simulati, il supporto alle funzioni di controllo del territorio, la riduzione del contatto diretto tra operatori e soggetti controllati e un primo livello di valutazione situazionale, attraverso l'interazione con banche dati e sistemi informativi istituzionali. Il progetto affronta inoltre in modo critico i principali limiti e rischi, in particolare quelli legati alla tutela della privacy, alla governance dei dati e alla dipendenza dalle infrastrutture di rete, ribadendo il principio del "human-in-the-loop". GEN-LAMBDA26 si configura quindi non come sostituto del decisore umano, ma come abilitatore cognitivo, capace di migliorare la qualità, la tempestività e la responsabilità delle decisioni in contesti emergenziali complessi.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=10760 (2:59:40 – 3:09:25)

Intervento dell' Esercito Italiano

Il progetto da noi ideato prevede l'uso di una IA avanzata capace di coadiuvare l'Esercito Italiano.
Il nostro obiettivo è garantire la tutela del Paese, integrando le procedute tecnico tattiche attuali con capacità di calcolo avanzato basate sull'Intelligenza Artificiale.
Esponiamo dunque due possibili casi in cui vediamo l'Esercito servirsi dell'IA.

Caso 1
In uno scenario di emergenza epidemiologica, il nostro nemico più grande non è solo il virus, è il tempo. Nelle crisi passate, abbiamo imparato una dura lezione, quando un ospedale civile richiede l'intervento dell'Esercito perché è saturo, siamo già in ritardo. La reazione, per quanto veloce, rincorre sempre l'emergenza.

Il nostro progetto mira a prevederla, ad anticiparla, attraverso l'integrazione dell'Intelligenza Artificiale in un'operazione inter-agency tra l'Esercito Italiano e la Protezione Civile.
Non va immaginato un computer complesso o macchinoso. L'IA integrata nei sistemi adoperati dalla Protezione Civile, raccoglie informazioni e analizza dati semplici in tempo reale, come l'aumento delle chiamate al 118 per problemi respiratori, l'improvviso esaurimento di farmaci specifici nelle farmacie locali o i flussi di mobilità verso certe province.

Ed è qui che il sistema calcola cosa accadrà tra 72 ore.

L'IA proietta questi dati su una mappa e ci mostra le probabili zone prossime alla saturazione.

Grazie a queste informazioni saremo in grado di muoverci con largo anticipo, attivando ospedali da campo nei luoghi indicati dall'algoritmo.

In sintesi: passiamo da una Forza Armata che reagisce a un'emergenza, a una che si posiziona preventivamente per prevenirne gli effetti peggiori. Questa è la "logistica predittiva", questo è il futuro del nostro intervento.

Caso 2

Passiamo ora al secondo pilastro della nostra strategia: il controllo del territorio

Sappiamo che presidiare fisicamente ogni strada, ogni piazza e ogni varco di una zona di quarantena richiederebbe un numero di uomini di cui non disponiamo.

La soluzione è la tecnologia, l'impiego di diversi droni dotati di sensori avanzati e intelligenza artificiale. Non si tratta di semplice videoripresa, ma di monitoraggio analitico attivo.

L'IA adoperata sfrutta algoritmi capaci di machine-learning che analizzano i dati raccolti, imparano ad ogni nuova immissione, fornendo output sempre più efficienti. Riuscendo a discriminare situazioni concesse dagli standard di sicurezza, da un assembramento causato da azioni negligenti.
Questi droni sono equipaggiati con ottiche termiche e algoritmi di riconoscimento comportamentale. La loro missione è sorvolare le zone urbane per individuare particolari devianze dal comportamento consentito dalle norme in vigore.
Cosa intendiamo? L'algoritmo ignora il normale flusso della vita cittadina. Ma si attiva immediatamente se rileva anomalie.
Questo sistema funge da moltiplicatore di forze. Ci permette di controllare un'intera città con poche pattuglie a terra, che interverranno ove il sistema ha confermato una criticità. Massimo controllo del rispetto delle regole sanitarie, minimo impiego di risorse umane e massima tutela per la salute dei nostri operatori. Questa è la sorveglianza moderna.

Limitazioni IA.
L'IA non comanda, calcola le probabilità ma non ha etica, il soldato non deve mai spegnere il proprio intuito per seguire ciecamente l'algoritmo.

L'IA ci informa sul dove e quando agire, ma spetta all'uomo decidere se e come farlo. La priorità assoluta è quella di preservare la discrezionalità del Comandante. La decisione finale di intervenire, specialmente in contesti civili delicati, deve restare umana.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=11376 (3:09:40 – 3:16:00)

Intervento della Marina Militare

Nello scenario di un'emergenza epidemiologica nazionale, la Marina Militare si configura parte della capacità di risposta dello Stato. L'analisi odierna si focalizza su come l'integrazione dell'Intelligenza Artificiale possa trasformare le nostre unità navali da assetti logistici a veri e propri centri nodali di intelligenza sanitaria.

- Proiettata slide in cui scorre il video dell'area sanitaria di Nave Vulcano

La Marina dispone di assetti con capacità chirurgiche e di rianimazione d'avanguardia:

Nave Cavour (Portaerei/Nave ospedale):
- Capacità ROLE 2 che può essere implementata a ROLE 3
- 2 sale operatorie, terapia intensiva, tac, laboratorio analisi

Nave Trieste (LHD landing helicopter dock):
- Ospedale di 700m2
- Capacità anfibie per raggiungere aree isolate via mare

Nave Vulcano (LSS)
- Supporto logistico e mantenimento della catena del freddo (farmaci/vaccini).

Usufruendo di questi assetti l'IA può essere implementata articolandosi su tre direttrici fondamentali:
Attraverso algoritmi di Deep Learning, i dati di consumo di ossigeno, DPI e farmaci vengono incrociati con i tassi di ammissione, fornendo proiezioni logistiche con 48 ore di anticipo. Parallelamente, l'uso di un Gemello Digitale della costa permette di simulare lo sbarco di Posti Medici Avanzati, individuando i punti di approdo ottimali per non saturare ulteriormente le strutture civili.

Modelli come YOLO o Faster R-CNN su telecamere termiche e ottiche consentono un triage intelligente e simultaneo. Durante le fasi di imbarco/sbarco, possiamo rilevare anomalie biometriche in tempo reale, garantendo al contempo l'integrità

delle “aree rosse” a bordo, monitorando costantemente l’uso corretto dei dispositivi di protezione individuale per prevenire focolai in ambienti confinati.

Tuttavia, un’analisi STEM rigorosa impone di riconoscere dove l’IA deve fermarsi in quanto esistono casistiche in cui l’algoritmo non può e non deve sostituire l’uomo:

1. **Il Dilemma Etico e Il Triage Morale**: L’IA basandosi su algoritmi matematici, può classificare i pazienti in base ai parametri vitali ma non possiede l’empatia e la sensibilità umana.

2. **“Black Swan”:** L’IA si basa su dati storici (Covid 19), di conseguenza è in grado di produrre protocolli efficienti per contrastare minacce già note; mentre non è in grado di creare protocolli idonei per minacce non note.

3. **Responsabilità Giuridica e “Scatola Nera” (Black Box)**: Molti modelli di Deep Learning sono “scatole nere”: non spiegano perché hanno preso una decisione, quindi nel caso in cui dovesse causare u. decesso o un incidente logistico grave chi ne risponderebbe considerando che la tracciabilità della responsabilità è legale e gerarchica. L’IA non può essere imputata in un tribunale militare o civile.

4. **Architettura Tecnica: Sicurezza e Autonomia**: Per questo motivo, la nostra architettura si basa sull’adozione dell’Edge Computing. I modelli IA devono risiedere su server di bordo, garantendo operatività totale anche in assenza di connettività satellitare e proteggendo i dati sensibili dei cittadini. Deve essere un sisitema stand alone. Ogni output algoritmico segue rigorosamente il paradigma Human-on-the-loop: l’IA suggerisce, ma l’Ufficiale Medico e il Comandante decidono.

Conclusioni

In conclusione, l'integrazione delle discipline STEM e dell'IA nella Marina Militare non è una prospettiva futura, ma una necessità attuale. Trasformare i nostri assetti in Hub Sanitari Intelligenti significa garantire al Paese una difesa flessibile, tecnologica e, sopra ogni cosa, umana, pronta a rispondere con precisione millimetrica alle sfide di ogni nuova emergenza.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=11760 (3:16:00 – 3:20:40)

Intervento dell'Aeronautica Militare

Il nostro contributo completa idealmente il quadro esposto precedentemente dai colleghi dei Carabinieri, dell'Esercito e della Marina, portando l'attenzione su una dimensione diversa ma altrettanto cruciale:

La Terza Dimensione

- ***Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=12071 (3:21:25 – 3:29:00)***

La Terza Dimensione è quell'aerea dove velocità, flessibilità, e capacità di proiezione diventano fattori decisivi nella gestione delle emergenze sanitarie.
Nella risposta che abbiamo ipotizzato allo scenario assegnatoci il nostro intervento si focalizzerà su tre aspetti principali:

1. **Medevac (Medical Evacuation)**

L'Aeronautica Militare italiana è dotata di capacità di trasporto in biocontenimento estremo, garantendo la continuità delle cure senza compromettere la sicurezza degli equipaggi e delle infrastrutture.
Velivoli specializzati, rapidamente configurabili, impiegano il sistema ATI (Aircraft Transit Isolator), una barella isolata che opera come una vera e propria camera di biocontenimento mobile, consentendo il trasferimento sicuro di pazienti critici e dell'intero equipaggio da zone sature e ad alto rischio, in poche ore, verso tutto il

territorio nazionale.
In tale contesto, l'Intelligenza Artificiale agisce come sistema di supporto decisionale avanzato, analizzando in tempo reale parametri vitali, dati ospedalieri, condizioni meteo-operative e informazioni storiche per anticipare il deterioramento clinico, ottimizzare rotte e tempi di risposta (fino a –35%)[1], selezionare la struttura sanitaria più idonea e ridurre il rischio di errore medico.

2. Il supporto logistico

Nel contesto delle emergenze sanitarie, la logistica rappresenta un moltiplicatore di efficacia tanto quanto il trasporto dei pazienti.
L'Aeronautica Militare opera come infrastruttura logistica nazionale, capace di riconfigurare in tempi ridotti le proprie basi in hub sanitari aeroportuali.
Questi hub diventano centri di ricezione, stoccaggio e smistamento di materiali critici: DPI, vaccini, farmaci, respiratori e attrezzature biomedicali, riducendo i tempi di distribuzione, superando vincoli geografici e infrastrutturali, e garantendo una risposta uniforme anche verso le aree più periferiche o colpite.
In questo ambito, le discipline STEM e l'Intelligenza Artificiale trovano una delle loro applicazioni più concrete.
Una delle principali sfide della logistica sanitaria è prevedere con precisione fabbisogni, quantità e tempistiche: i modelli previsionali basati su IA, fino al 31% più accurati[2] di quelli tradizionali, integrano dati storici e predicono i trend in aumento dei ricoveri fino a 2 settimane. Inoltre, tramite simulazioni di Digital Twin, l'IA riproduce scenari di volo virtuali, prevedendo consumo di carburante e comportamento del carico.

[1] "Smart Route Optimization for Emergency, Vehicles: Enhancing Ambulance Efficiency through Advanced Algorithms" - Vishal Parmar, Vishal Kushwaha, M. Gangwar, CSIT Department, SIRT, Bhopal – July, 24, 2024.
[2] Ahtasham Mushtaq, M., Anis Noor, M., Santillo, L.C., Verde, R. (2025). Implementing AI for Dynamic Demand Forecasting in Lean Healthcare Logistics: A Case Study Approach. In: Gallo, M. (eds) Proceedings of LLEAHMM 2024. LLEAHMM 2024. Lecture Notes in Bioengineering. Springer, Cham. https://doi.org/10.1007/978-3-031-82923-9_26.

3. Point Of Entry (POE) di Villafranca

Un esempio emblematico della flessibilità di mezzi aeronautici è il POE di Villafranca, un point of entry proiettabile unico nel suo genere.
Si tratta di un Treatment Center campale-modulare progettato per accogliere fino a 92 pazienti, articolato in aree dedicate al triage, alla terapia intensiva, alla degenza e all'isolamento. Equipaggiato con sistemi avanzati di ventilazione e filtrazione, aree di biocontenimento e capacità di decontaminazione CBRN, opera secondo standard OMS assicurando continuità sanitaria in ambienti privi di supporto logistico. Si tratta, in buona sostanza, di un assetto plug and play rapidamente rischierabile presso hub aeroportuali nazionali.
È dotato di una marcata integrazione tecnologica: sensori di monitoraggio di parametri vitali, geolocalizzazione del personale e sistemi informativi per raccolta e strutturazione di dati clinici in tempo reale. Sono inoltre impiegati droni a guida autonoma, terrestri e aerei, per gli spostamenti controllati dei degenti all'interno dello stesso e per il trasporto rapido e sicuro di campioni verso strutture ospedaliere, digitalizzando l'intero processo operativo.
I dati confluiscono in sistemi di supporto informativo che assistono il personale medico nella gestione complessiva.

Conclusioni
Il limite principale dell'IA riguarda la qualità e il controllo dei dati: la cosiddetta sovranità del dato.
Se questi sono incompleti, imprecisi o soggetti a pregiudizi, le decisioni generate dall'IA possono riprodurre e amplificare tali distorsioni.
Nonostante i suoi progressi, l'Intelligenza Artificiale non può sostituire sensibilità, empatia e giudizio etico, qualità intrinsecamente umane. Affidarsi ciecamente all'IA rischia di svuotare la responsabilità decisionale.
Decisioni percepite come "imposte da un algoritmo" e veicolate dalle forze armate possono alimentare diffidenza, paura o conflitto sociale: il cosiddetto "black box effect".
Riflettendo sulla nostra esperienza, emerge come sia necessario migliorare

l'accessibilità alle risorse open sources e alle applicazioni attualmente disponibili nel mondo civile o, in alternativa, di un'IA nativa della Difesa, costruita sulle esigenze del personale e accompagnata da un percorso formativo e di certificazione sull'uso responsabile.

Intervento Conclusivo dell' Arma dei Carabinieri

Metodo

Il metodo di lavoro utilizzato si è basato su:

- L'impostazione di un'area di lavoro strutturata, sia fisica (aula riservata) che cibernetica (area dati condivisa su google workspace Arma al link https://drive.google.com/drive/folders/1sW8m8aUiWwL2B2cyrZfs7nah96vG0uDy?usp=drive_link);
- Una ricerca esperienziale dei militari, unita al confronto con il personale che ha prestato servizio durante la reale pandemia di COVID-19, tra cui video reali forniti dal Comandante della Scuola, al tempo Comandante della Legione Abruzzo e Molise.
- L'uso di appunti di Stato Maggiore per tracciare e indicare il progressivo avanzamento dei lavori.
- L'impiego dell'Intelligenza Artificiale per creare simulazioni separate, infografica e mappe mentali.

Idee presentate

Sono state presentate due idee che si inseriscono in uno scenario di emergenza sanitaria senza precedenti, in cui l'utilizzo dell'Intelligenza Artificiale avviene sotto la supervisione umana "human in the loop".

GEN-LAMBDA 26

La prima è un insieme di chatbot interoperabili (sperimentalmente ne sono stati utilizzati due), dove ciascun attore coinvolto ha una sovranità del dato di competenza, nonché la supervisione sulle fonti esterne utilizzate per alimentare il proprio bot.
Tali bot sono coordinati dal bot orchestratore denominato "GEN-LAMBDA 26". Esso è uno strumento intelligente di supporto alle decisioni, in grado di analizzare l'intento dell'utente, riconoscerne l'esigenza informativa e reindirizzare la domanda ai bot specializzati in ambiti specifici.
PREDICT-IA è uno dei due sotto-bot presentati, progettato per elaborare previsioni sull'andamento della pandemia e suggerire strategie di contrasto riducendo i tempi di reazione. Il sistema elabora informazioni provenienti sia da fonti aperte (OSINT) che chiuse (CLOSINT) e gestisce l'accesso tramite un sistema ad autorizzazioni differenziate. La piattaforma si alimenta autonomamente raccogliendo informazioni sia da fonti aperte (OSINT) che da fonti chiuse (CLOSINT). Integra inoltre i dati provenienti da Ministeri, Istituzioni e Forze Armate.
L'altro sotto-bot è Chattadino, istruito per fornire assistenza ai cittadini nella

comprensione delle misure di prevenzione del contagio nonché delle prescrizioni legislative volte a contenere la pandemia. Può spiegare cosa è permesso o vietato e come affrontare gli spostamenti.

AI-GLASS ARMA

La seconda idea presentata "AI-GLASS ARMA", sono degli occhiali con realtà aumentata integrati con sistemi di valutazione basati su Intelligenza Artificiale, sviluppati per l'Arma dei Carabinieri, che consentono di rilevare i parametri vitali delle persone nei dintorni.

Presentazione

La presentazione per la Scuola Marescialli dei Carabinieri si è svolta nelle seguenti fasi:

- Introduzione video: L'intervento si è aperto con la proiezione di un video, realizzato dall'Aeronautica Militare, che ha calato il pubblico in uno scenario di grave emergenza pandemica.
- Coinvolgimento del pubblico: Gli allievi hanno invitato i presenti a scansionare un QR Code che ha permesso al pubblico di accedere al Gen-Lambda 26.
- Dimostrazione dal vivo (Live Demo): È stata effettuata una simulazione ove è stata inserita in "GEN-LAMBDA 26" una domanda volta a stimare di durata della pandemia e suggerire una strategia di contrasto. II bot orchestratore ha reindirizzato la domanda al sotto-bot specializzato PREDICT-IA che ha fornito le risposte richieste, successivamente analizzate dalla relatrice. II bot è rimasto attivo e testabile dal pubblico per i giorni successivi.
- Esposizione delle tecnologie hardware: La presentazione è poi tornata sulle slide per introdurre il progetto AI-GLASS ARMA (gli occhiali in realtà auméntata). Ne sono stati illustrati i vantaggi operativi.

Conclusioni

La conclusione della presentazione si è fondata su una riflessione operativa ed etica, tanto profonda quanto concisa, sul ruolo dell'Intelligenza Artificiale, riassumibile in un principio fondamentale: "In un contesto sempre più complesso, la vera innovazione non consiste nel fare di più, ma nel farlo meglio, in sinergia con l'essere umano".
Questo concetto finale racchiude il senso dell'intero progetto e può essere approfondito sotto tre aspetti chiave:

- L'IA come supporto, non come sostituto: L'intero impianto tecnologico presentato non mira a rimpiazzare l'uomo, ma ad affiancarlo. II chatbot GEN-LAMBDA 26, ad esempio, non è un'entità che decide autonomamente, ma è concepito come un vero e proprio strumento di supporto alle decisioni. L'idea è che la tecnologia debba processare i dati (provenienti da Ministeri, Forze Armate e Istituzioni) per metterli immediatamente a disposizione dell'intelligenza umana.

- Il superamento dei limiti umani (il fattore tempo): In uno scenario pandemico in cui i contagi aumentano rapidamente e gli ospedali sono sotto pressione, il tempo diventa la risorsa più preziosa. L'innovazione ("farlo meglio") si concretizza nella capacità della macchina di intervenire "quando l'uomo non può arrivare in tempo". L'IA serve a elaborare velocemente informazioni e previsioni che possono fare la differenza per salvare vite umane, arrivando lì dove le tempistiche umane non sarebbero sufficienti.
- L'equilibrio tra efficacia e limiti etico-tecnologici: Un'innovazione in vera "sinergia con l'essere umano" richiede anche la consapevolezza dei rischi. Le conclusioni invitano a valutare attentamente il bilanciamento tra i grandi vantaggi operativi (come la maggiore sicurezza per gli operatori che utilizzano gli occhiali AI-GLASS ARMA riducendo il contatto diretto) e le criticità intrinseche del sistema. Tra queste, i relatori evidenziano in particolare il possibile impatto sul diritto alla privacy e la forte dipendenza dalla connessione di rete, limiti che l'uomo deve gestire per un uso corretto della tecnologia.


ITALIA
3ª CONFERENZA
LE DISCIPLINE STEM
NELLA DIFESA

INTELLIGENZA ARTIFICIALE: L'ARMA DEI CARABINIERI

GEN-LAMBDA26

Funzionalità/Scopo

Struttura

Autorizzazioni diversificate

DEMO

AI-GLASS ARMA

Funzionalità e Vantaggi Operativi

Rilevazione Parametri

Sicurezza Operatore

Efficienza e Continuità Operativa

Scuola Sottufficiali Esercito Italiano

Scuola Sottufficiali Marina Militare

Scuola Marescialli Aeronautica Militare

Scuola Marescialli e Brigadieri Arma dei Carabinieri

Scuola Ispettori e Sovrintendenti Guardia di Finanza

"GdF Coach"

ENTE

Scuola Ispettori e Sovrintendenti Guardia di Finanza

GdfCoach

Sono il Maresciallo Freddo Federico, attuale frequentatore del 95° Corso Argentera III, terzo anno di studi presso la Scuola Ispettori e Sovrintendenti della Guardia di Finanza L'Aquila. Oggi, insieme al mio collega, vi presenterò i risultati di due progettualità nate all'interno del nostro laboratorio di Intelligenza Artificiale. In questo contesto, abbiamo avuto l'opportunità di tradurre le competenze teoriche acquisite in soluzioni pratiche e innovative, particolarmente efficaci nell'ambito della didattica.
Nello specifico, oggi vi presento GdFCoach.
Si tratta di un tutor testuale e simulatore di scenari realistici, progettato per supportare l'allievo nella comprensione della materia e, soprattutto, nella memorizzazione dei passaggi fondamentali e delle procedure da attuare durante le attività ispettive della Guardia di Finanza, in particolare durante l'accesso e le successive fasi della verifica o del controllo fiscale.
Guardiamo assieme i punti chiave di questo applicativo:
il primo punto L'Intelligenza Artificiale impiegata: Abbiamo scelto di utilizzare una Gem di Gemini per tre ragioni fondamentali: la sua elevata potenza di calcolo, la gratuità del servizio e, soprattutto, l'estrema portabilità. Le Gem sono infatti fruibili da qualsiasi dispositivo — Android, iPhone o PC — tramite interfaccia web dedicata.
Importante è anche la capacità di simulazione operativa: GdFCoach, grazie alla capacità di generare casistiche realistiche di verifiche fiscali presso il contribuente, permette all'allievo di affinare le proprie conoscenze e di testare con mano le procedure che si troverà ad affrontare.
Vediamo il video!

GdfCoach: quali ulteriori potenzialità addestrative offre?
La vera forza di GdFCoach risiede nella sua utilità trasversale. Come abbiamo visto, la flessibilità della "Gem" permette di modificare istantaneamente le istruzioni impartite e la base di conoscenza (Knowledge Base) da cui l'IA attinge.
Caricando la normativa di riferimento e i manuali operativi specifici, GdFCoach smette di essere solo un simulatore per verifiche fiscali e si trasforma in un tutor virtuale adattabile a tutti i segmenti della missione istituzionale della Guardia di Finanza, che supporta l'allievo in ogni materia.
In sintesi, GdFCoach offre un'utilità trasversale perché è uno strumento sempre aggiornato alla fonte più recente. Indipendentemente dalla materia d'esame o dal futuro reparto d'impiego, l'allievo ha a disposizione un assistente specializzato in grado di calarlo in scenari operativi realistici per ogni segmento della nostra missione.

Analisi di Rischio Contabilità Anomale (A.R.C.A.)

Sono il Maresciallo Allievo Milione Salvatore, frequentatore del 3° anno di corso presso la scuola ispettori della Guardia di Finanza. Il progetto che vi presenterò si chiama A.R.C.A., che sta per Analisi di Rischio Contabilità Anomale.
A.R.C.A. è un software sperimentale nato nell'ambito del laboratorio di informatica operativa, che mette alla prova le nostre capacità di programmazione e la potenza dell'Intelligenza Artificiale.
In sintesi, si tratta di un simulatore avanzato che gira interamente in locale, progettato per analizzare flussi contabili e individuare e spiegare potenziali anomalie in totale sicurezza.
L'applicativo contiene al suo interno (nel codice sorgente) tutte le istruzioni utili per il suo funzionamento e sfrutta la potenza di calcolo Intelligenza Artificiale per analizzare grandi quantità di dati e, successivamente, elaborare gli alert di anomalia.
Vediamo come funziona!

In che modo contribuisce al percorso formativo degli allievi questa innovativa app?
Durante i tre anni di corso, sosteniamo esami nelle materie universitarie e di tecnica professionale che servono a formarci quali operatori di polizia economico-finanziaria. Al termine del percorso formativo, progetti come A.R.C.A., elaborati nell'ambito del laboratorio di informatica, servono per fornire un supporto pratico all'attività addestrativa. In sostanza, questa sperimentazione ha l'obiettivo di dare concretezza e di mettere in pratica le nozioni apprese sul piano teorico.
L'applicativo, come abbiamo visto, analizza i dati basandosi rigorosamente sul quadro normativo vigente e sugli indicatori di rischio elaborati partendo dalle migliori pratiche operative dei Reparti della Guardia di Finanza. Il risultato è la generazione di alert mirati, che non solo segnalano l'anomalia, ma illustrano nel dettaglio le motivazioni del rischio e forniscono tutti i riferimenti normativi necessari.
Per garantire un addestramento davvero efficace e fedele alla realtà, utilizziamo dataset fittizi costruiti su casistiche già esistenti e note. Questo ci permette di operare in un ambiente simulato ma estremamente verosimile, imparando esattamente quali elementi cercare e, soprattutto, quali percorsi logici seguire per individuare con precisione le frodi fiscali.
Grazie ad A.R.C.A., ci prepariamo a entrare nel mondo operativo con con una marcia in più, trasformando l'esperienza simulata in competenza reale.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=12537 (3:29:10 – 3:40:25)

Scuola Ispettori e Sovrintendenti
Guardia di Finanza

Applicativi di I.A. per le attività didattiche dei Reparti di Istruzione

Venezia, 4 febbraio 2026

Tutor virtuale esperto in ogni materia

I.A. Generativa verticale

Utilizzo delle GEMs di Gemini per creare scenari simulati di accessi e verifiche fiscali.

Retenzione Efficace

Metodologia innovativa che migliora la memorizzazione delle informazioni apprese.

Interazione Massima

Si può interagire con la GEM sia testualmente che vocalmente, aumentando il livello di realismo dello scenario e migliorando l'efficacia della simulazione.

Knowledge base controllata

La GEMs si basa solo sulla base di conoscenza caricata, eliminando il rischio di allucinazioni.

Adattabile

La GEM si può adattare a qualsiasi materia, rimanendo sempre aggiornata.

3 di 10

GdfCoach

Tutor e simulatore per l'attività di accesso e verifica fiscale.

A.R.C.A

Analisi di Rischio
Contabilità Anomale

Software di analisi di rischio e individuazione delle frodi

Supporto didattico I.A.

Sistema innovativo che utilizza l'I.A. per supportare l'attività didattica per l'applicazione pratica nelle materie tecnico-professionali.

Dati fittizi

L'applicativo, che si esegue in locale, analizza dati fittizi creati sulla base di casistiche già note.

Report

Generazione di *alert* specifici con motivazioni dettagliate del rischio e riferimenti normativi su 4 assi (Fiscale, Finanziario, Contabile, Frodi), per allenare l'allievo a riconoscere il più ampio numero di frodi economico-finanziarie conoscuto.

7 di 10

Scuola Ispettori e Sovrintendenti
Guardia di Finanza

Grazie per l'attenzione

Presentazione della Scuola Ispettori e Sovrintendenti Guardia di Finanza

STEM

Accademie

"IA, sistemi autonomi e space technologies per la sicurezza integrata dell'Artico"

"IA, sistemi autonomi e space technologies per la sicurezza integrata dell'Artico"

Nel quadro di uno scenario prospettico collocato in un futuro prossimo, gli Allievi delle Accademie hanno operato all'interno di un contesto strategico caratterizzato dalla crescente centralità della Groenlandia e dello spazio artico quale nodo cruciale per la sicurezza euro-atlantica. La riduzione della calotta polare e la conseguente navigabilità permanente delle acque hanno trasformato le rotte artiche in linee di comunicazione marittime di primaria importanza, accrescendo la competizione tra le principali potenze. Parallelamente, lo sfruttamento di risorse strategiche, in particolare terre rare e altre materie prime essenziali per le filiere tecnologiche e industriali avanzate, ha ulteriormente incrementato la rilevanza geopolitica dell'area. In tale contesto, caratterizzato da minacce ibride e attività ostili multi-dominio, gli Allievi hanno sviluppato un'attività di analisi congiunta finalizzata all'individuazione delle principali criticità operative e alla proposta di soluzioni tecnologiche avanzate, fortemente integrate con l'Intelligenza Artificiale, fattore abilitante per la fusione informativa, la riduzione dei tempi decisionali e il supporto al processo decisionale human-in-the-loop.

Un ruolo centrale nello scenario è attribuito alla dimensione marittima e subacquea, quale colonna portante della sicurezza complessiva nell'area artica. L'adozione di dispositivi integrati per la protezione dei fondali, supportati da sistemi di Intelligenza Artificiale, consente di assicurare la sorveglianza continua delle infrastrutture sottomarine e delle principali linee di comunicazione, riducendo l'ambiguità operativa e aumentando la capacità di individuazione tempestiva di anomalie e attività ostili. L'impiego coordinato di piattaforme di superficie, sistemi automatizzati e capacità subacquee avanzate abilita una situational awareness persistente, rafforzando in modo concreto deterrenza e capacità di risposta.

In integrazione con la dimensione marittima, i domini aereo e spaziale contribuiscono alla sorveglianza del teatro artico, alla resilienza dei servizi di navigazione e temporizzazione e alla correlazione multi-sensore. L'Intelligenza Artificiale supporta l'interazione dei dati multi-sensore e il riconoscimento di pattern anomali, migliorando la qualità del quadro operativo e rafforzando la capacità di operare in ambienti degradati o caratterizzati da interferenze intenzionali. Parallelamente, la dimensione terrestre e la sicurezza delle aree critiche contribuiscono alla protezione dei confini, delle landing station e delle infrastrutture strategiche attraverso sistemi avanzati di sorveglianza perimetrale, contrasto ai droni e analisi predittiva. L'impiego dell'Intelligenza Artificiale consente di filtrare il rumore ambientale, individuare precocemente anomalie e rafforzare la prevenzione delle minacce ibride.

Accanto ai domini fisici, il lavoro integra la dimensione cyber e cognitiva, includendo il contrasto alle campagne di disinformazione, la rilevazione dei deepfake e l'analisi dei flussi informativi e finanziari, al fine di ridurre l'ambiguità, rafforzare l'attribuzione tecnica e contrastare le attività ibride sottosoglia.

Nel complesso, il lavoro degli Allievi mette in evidenza il valore dell'approccio prospettico adottato e della sperimentazione concettuale di soluzioni tecnologiche avanzate, evidenziando come l'Intelligenza

Artificiale rappresenti un elemento chiave per incrementare l'efficienza, la tempestività e l'affidabilità delle capacità operative future. Le proposte sviluppate, accompagnate da una roadmap concettuale e da raccomandazioni strategiche, costituiscono una base di riflessione concreta per l'evoluzione degli strumenti di sorveglianza, prevenzione e supporto decisionale, in coerenza con le esigenze di un contesto operativo in rapida trasformazione.

Introduzione

Il presente elaborato rappresenta l'esito di un'attività congiunta di analisi e approfondimento concettuale condotta dagli Allievi dell'Accademia Militare, dell'Accademia Navale e dell'Accademia Aeronautica, nell'ambito di un contesto prospettico volto a esplorare le principali evoluzioni dell'assetto strategico e le relative implicazioni per lo strumento militare nazionale nel futuro prossimo. Lo stesso concetto di "evoluzione" si è ulteriormente ampliato negli ultimi decenni, riflettendo le dinamiche del nuovo disordine globale e le interconnessioni strategiche con aree più remote. Il lavoro si inserisce in una fase di profonda trasformazione degli equilibri geopolitici, tecnologici ed ambientali, con specifico riferimento alla crescente centralità della regione artica e della Groenlandia quali aree di primariaimportanza per la sicurezza e la stabilità dello spazio euro-atlantico.Il progetto si sviluppa all'interno di un impianto operativo unitario che ha orientato lo studio e l'ideazione concettuale del gruppo. Lo scenario di riferimento descrive una situazione caratterizzata da continue incursioni nello spazio euro-atlantico, realizzate mediante sconfinamenti di milizie, impiego di droni, assetti aerei e navali, nonché attraverso attacchi cibernetici con responsabilità non immediatamenteidentificabile. I settori interessati ricadono sotto la competenza delle Forze Armate italiane,impegnate nel garantirne la difesa. L'obiettivo del programma consiste nella pianificazione di attività volte ad assicurare l'integrità delle aree assegnate e nell'attuazione di misure di deterrenza idonee a scoraggiare future azioni ostili.

In questo quadro, gli effetti del cambiamento climatico, la riduzione della calotta polare e l'estensione dei periodi di navigabilità hanno determinato una riconfigurazione strutturale dell'ambiente polare,trasformando le rotte settentrionali in linee di comunicazione marittime di crescente valore strategico.

Parallelamente, lo sviluppo infrastrutturale e lo sfruttamento di risorse, nello specifico terre rare e altre materie prime essenziali per le filiere tecnologiche avanzate, hanno contribuito ad accrescere la centralità dell'area e l'articolazione delle dinamiche operative, accentuando la pressione sui sistemi infrastrutturali strategici e la loro esposizione a fattori di vulnerabilità.

La seconda missione dello strumento militare, ovvero la difesa degli spazi euro-atlantici ed euromediterranei, si concretizza nel contributo alla difesa collettiva e nel mantenimento della stabilità nelle aree incidenti, al fine di tutelare gli interessi vitali e strategici del Paese. Il teatro artico e il Mediterraneo Allargato, infatti, non possono essere considerati come ambiti separati, ma come componenti interconnesse di un unico spazio strategico. Le dinamiche di competizione, instabilità o coercizione che si sviluppano nell'area artica possono produrre ricadute sistemiche sul bacino euro-mediterraneo, incidendo sulla sicurezza delle Sea Lines of Communication (SLOC), sui flussi energetici

e sulle posture militari alleate, nell'ambito del quadro generale di tutela delle infrastrutture strategiche.

Ne consegue che la presenza e il contributo italiano nel teatro artico assumono una valenza che travalica il perimetro regionale, configurandosi come parte integrante della difesa avanzata degli interessi nazionali e della stabilità degli alleati. In questo quadro, l'impegno nel Nord contribuisce direttamente alla sicurezza del Mediterraneo Allargato, rafforzando la coerenza strategica tra dimensione euro-atlantica ed euro-mediterranea. Lo stesso concetto di "Mediterraneo Allargato" si sta espandendo strategicamente fino a includere la Groenlandia e l'Artico, trasformando l'area settentrionale in una "terza dimensione" geopolitica fondamentale per l'Europa e l'Italia. Questa estensione non sostituisce la definizione tradizionale (dall'Atlantico al Mar Rosso/Caucaso), ma integra l'Artico come zona cruciale per energia, materie prime critiche (terre rare) e sicurezza marittima. In sintesi, il "Mediterraneo allargato alla Groenlandia" rappresenta la continuità strategica tra la sicurezza del Mare Nostrum e le nuove sfide del Mar Glaciale Artico.

Il contributo degli Allievi si configura come esercizio di analisi integrata e di sperimentazione concettuale, volto a individuare le principali criticità e a ipotizzare soluzioni tecnologiche innovative capaci di consolidare le funzioni di sorveglianza, prevenzione e tutela dei domini di interesse. L'elaborato intende offrire una riflessione strutturata, coerente con l'evoluzione delle modalità di impiego dello strumento militare in contesti caratterizzati da minacce ibride, azioni sottosoglia e crescente saturazione informativa.

Un elemento strutturale del lavoro è rappresentato dall'impiego sistemico dell'Intelligenza Artificiale, quale fattore abilitante della fusione informativa, del supporto al processo decisionale e della gestione di architetture multi-dominio ad elevata complessità. L'IA non è considerata un fine, ma un moltiplicatore di efficacia, in grado di trasformare grandi volumi di dati eterogenei in quadri situazionali coerenti, tempestivi e utilizzabili a livello operativo e strategico. Nel seguito del documento, l'IA viene pertanto declinata in modo funzionale nei singoli domini, senza ripeterne il ruolo abilitante generale, che viene qui definito come riferimento architetturale unitario.

L'approccio inter-accademico ha consentito di integrare prospettive, competenze e sensibilità differenti, favorendo una visione complessiva delle principali criticità e delle potenzialità offerte dalle tecnologie emergenti. Particolare attenzione è stata dedicata al monitoraggio continuo degli ambiti di rilevanza e alla resilienza dei sistemi fisici e informativi, con specifico riferimento alla dimensione marittima e subacquea, quale componente di importanza strutturale per la sicurezza complessiva dell'ambiente artico. Nello specifico, la protezione delle infrastrutture critiche costituisce una priorità trasversale dell'intero impianto operativo. In tale ambito rientrano cavi sottomarini, landing station, pipeline, impianti energetici, nodi di telecomunicazione e data center ad alta latitudine, la cui compromissione può generare effetti strategici sistemici. Nel prosieguo, vengono illustrate le specifiche modalità di impiego operativo, con riferimento all'integrazione tra sensoristica di fondale, architetture C2 (Command and Control) interforze, assetti unmanned e task

group dedicati alla protezione attiva dei predetti sistemi.
Il presente contributo si configura quale riferimento formativo e concettuale, utile a stimolare una riflessione qualificata sui futuri sviluppi delle funzionalità operative e sull'impatto delle tecnologie emergenti, offrendo al contempo spunti di analisi coerenti con le esigenze di adattamento dello strumento militare a uno scenario in continua evoluzione.

1. Quadro strategico e mutamento del teatro artico

Lo scenario artico rappresenta, in un orizzonte temporale di medio-lungo periodo (circa un decennio), uno dei principali epicentri della competizione strategica globale. Lo scioglimento progressivo della calotta polare ha trasformato l'Artico da spazio periferico a nodo centrale delle SLOC, abilitando rotte marittime stabilmente navigabili (Northern Sea Route) e accelerando lo sfruttamento di risorse critiche, in particolare terre rare, idrocarburi residuali, infrastrutture energetiche e Data Center ad alta latitudine. Questa trasformazione ha prodotto una crescente densità di Critical Undersea Infrastructure (CUI), comprendente cavi sottomarini, landing station, pipeline, sistemi di generazione e distribuzione energetica, assetti dual-use civili/militari. La tutela di tali impianti costituisce un fattore determinante di stabilità strategica, poiché la loro compromissione produce impatti strategici rilevanti.
Il quadro strategico è caratterizzato dalla prevalenza di dinamiche di competizione sottosoglia (belowthe-threshold competition), tipiche della grey-zone warfare. In tale contesto, l'azione ostile si manifesta attraverso:• operazioni ibride che combinano strumenti militari, economici, informativi e cyber;• attività di plausible deniability, tramite assetti formalmente civili, quali navi scientifiche, mercantili,contractor, Unmanned Surface Vehicle (USV) e Unmanned Underwater Vehicle (UUV) civili;• campagne di disinformazione e information manipulation;• interferenze cyber-fisiche su sistemi Operational Technology (OT) e Industrial Control Systems (ICS).
Per il sistema difesa nazionale, ciò implica un mutamento concettuale: la deterrenza non è più basata esclusivamente sulla presenza militare visibile, ma sulla capacità di detection anticipata multi-layer e di attribution tecnica e politico-strategica, tali da ridurre l'ambiguità e aumentare il costo politico e operativo delle azioni ostili. In questo quadro, l'atteggiamento italiano, in sinergia con gli alleati euroatlantici, deve orientarsi verso un modello data-centric, multi-domain e AI-enabled.La Marina Militare assume un ruolo centrale nella protezione delle SLOC e delle infrastrutture di fondale, garantendo presenza costante, underwater domain awareness e capacità di risposta modulare.
L'Aeronautica Militare fornisce sorveglianza a lungo raggio, early warning, capacità ISR (Intelligence, Surveillance and Reconnaissance) e contributo alla resilienza del dominio spaziale e PNT (Positioning, Navigation and Timing). L'Esercito Italiano assicura la protezione dei nodi terrestri critici, delle landing station e delle infrastrutture logistiche, mentre l'Arma dei Carabinieri, nel ruolodi Stability Police, concorre alla sicurezza interna, alla protezione dell'integrità informativa ed

economica e alla dimensione di law enforcement in contesti ibridi.
L'evoluzione dell'area artica impone l'adozione di un approccio integrato che superi la logica dei domini separati, inquadrando un unico sistema operativo interconnesso, nel quale ogni evento fisico, cyber o informativo viene inserito in una catena di correlazione multi-dominio. In tale prospettiva, l'architettura descritta consente la fusione, la correlazione e l'interpretazione di grandi volumi di dati eterogenei in tempi compatibili con i cicli decisionali operativi.

2. Sicurezza multi-dominio e architetture interforze

La sicurezza del teatro artico deve essere concepita come intrinsecamente Multi-Domain Operations (MDO), dove l'efficacia deriva dall'architettura C2 e dal data fabric interforze, più che dalla singola piattaforma. L'obiettivo è la generazione di una Common Operational Picture (COP) persistente, coerente e a bassa latenza, governata a livello operativo interforze, con responsabilità chiaramente attribuite in ambito C2 e meccanismi di prioritizzazione dinamica delle informazioni, quale output primario dell'architettura JADC2 (Joint All-Domain Command and Control), basata su sensor-toshooter loop digitalizzati, reti resilienti (mesh e multi-bearer), data lake federati e motori IA per multi-source data fusion e decision support.
La Marina Militare contribuisce con nodi C2 marittimi e subacquei, reti acustiche e cueing verso assetti mobili; l'Aeronautica Militare con radar, assetti ISR e integrazione Space Situational Awareness (SSA)/space data; l'Esercito Italiano con protezione fisica dei nodi critici, sensoristica terrestre e integrazione C2 tattica; l'Arma dei Carabinieri con continuità tra sicurezza militare e law enforcement, a supporto della dimensione ibrida.
L'IA abilita fusione multilivello (data/feature/track), association management, riduzione dei falsi allarmi e correlazione temporale dei weak signals, trasformando eventi frammentati in indicatori di manovra ostile. La transizione da platform-centric a data-centric, con governance del dato e cyberresilience, costituisce il principale moltiplicatore di efficacia interforze.

3. Dominio subacqueo e Underwater Domain Awareness

Il dominio subacqueo rappresenta uno dei principali centri di gravità strategici nel teatro artico. La crescente dipendenza da asset di fondale, in particolare cavi sottomarini per telecomunicazioni e dati, rende il seabed un elemento critico del sistema globale di connettività e interdipendenza strategica.
La capacità di garantire Underwater Domain Awareness (UDA) persistente è pertanto un requisito essenziale per la protezione degli interessi nazionali e alleati, in quanto consente la costruzione di pattern-of-life del traffico subacqueo e l'individuazione precoce di anomalie compatibili con attività ostili o preparatorie.
In coerenza con il ruolo già delineato nel quadro generale, nel dominio subacqueo la Marina Militare opera quale riferimento funzionale per lo sviluppo e l'impiego delle capacità di Underwater Domain Awareness, attraverso architetture multi-layer

orientate a detection precoce, tracking persistente e attribuzione tecnico-forense (intesa come correlazione strutturata di evidenze multi-dominio a fini probatori e di sostegno alle decisioni politico-strategiche), a supporto della gestione integrata del seabed e dei processi decisionali politico-strategici.

Il primo livello è costituito da reti acustiche distribuite sul fondale, comprendenti cortine idrofoniche, nodi passivi e, ove applicabile, configurazioni multi-statiche a bassa potenza. Questi sistemi consentono una capacità di monitoraggio continuo di choke points, corridoi di transito e tratti infrastrutturali critici. È importante sottolineare, però, che gli impianti di fondale non possono essere installati ovunque, ma solo in assenza di sedimenti rocciosi e montagne sottomarine, preferendo fondali sabbiosi e relativamente bassi. L'elaborazione dei segnali richiede beamforming digitale avanzato, analisi spettrale adattiva e classificazione automatica delle firme acustiche tramite tecniche di Machine Learning(ML).

Il secondo livello è rappresentato dal Distributed Acoustic Sensing (DAS), che abilita l'impiego dei cavi in fibra ottica come sensori lineari vibrazionali distribuiti. Il DAS consente di monitorare attività prossime ai cavi, quali ancoraggi, drag, scavi o manomissioni, fornendo un moltiplicatore di copertura con un numero limitato di nodi attivi. L'integrazione del DAS con sistemi sonar tradizionali e
con l'IA riduce i falsi positivi e correla eventi vibrazionali con attività in superficie o anomalie cyberfisiche.

Il terzo livello è costituito da AUV (Autonomous Underwater Vehicle) under-ice, impiegati come sensori mobili ISR per verifica, target confirmation e ispezione infrastrutturale. Tali piattaforme operano mediante sistemi di navigazione inerziale (INS – Inertial Navigation System) accoppiati a DVL (Doppler Velocity Log), sonar di navigazione e tecniche di ice-relative navigation. L'assenza di GPS richiede un uso estensivo di sensor fusion e algoritmi di SLAM (Simultaneous Localization and Mapping) adattati al contesto subacqueo. Il quarto livello è rappresentato dalla fusione multi-sensore avanzata, che integra dati acustici, DAS, AIS (Automatic Identification System), osservazioni satellitari, dati GNSS (Global Navigation Satellite System) e modelli oceanografici predittivi. Architetture di data association e filtri bayesiani consentono di generare una COP subacquea persistente, abilitando l'identificazione di campagne multifase e la riduzione sistemica dei falsi allarmi.

L'IA ha un ruolo centrale, costruendo modelli dinamici del background acustico, apprendendo i pattern nominali del traffico e identificando deviazioni statisticamente significative compatibili con UUV, piattaforme a bassa segnatura o attività di interferenza subacquea. Questa capacità abilita cueing automatizzato verso assetti mobili e l'attivazione selettiva di sensori ad alta risoluzione.

Sul piano operativo, la risposta nel dominio subacqueo è strutturata tramite un Subsea Security Group, modulabile in base al livello di rischio, al grado di confidenza informativa e alla postura autorizzata.

La configurazione Sentry fornisce sorveglianza persistente e riduzione dell'incertezza, includendo unità C2/OPV (Offshore Patrol Vessel), USV e AUV/ROV

(Remotely Operated Vehicle) per ispezione selettiva. La configurazione Guardian introduce una nave madre, team subacquei specializzati e una cyber/OT cell integrata per intelligence tecnica e protezione delle infrastrutture. La configurazione Bastion rappresenta il livello massimo di assetto operativo, con capacità ASW (Anti-Submarine Warfare) passive rinforzate, boe gateway temporanee, AUV multipli e piani di repair con nave posacavi.

Nel dominio del fondale, la deterrenza non deriva dall'invulnerabilità fisica, ma dalla capacità di garantire detection precoce, attribuzione tecnico-forense, ripristino rapido e riduzione strutturale del rapporto costo-beneficio per l'attore ostile. L'integrazione tra architettura di sensor fusion adattiva e capacità operative modulari costituisce il fondamento di un assetto credibile di protezione e sicurezza marittima nel teatro artico.

4. Dominio aereo e sistemi cooperativi

Il dominio aereo costituisce il layer primario per la superiorità informativa, l'early warning e la gestione delle minacce sottosoglia, con impatto diretto sui tempi di ciclo decisionale OODA (Observe, Orient, Decide, Act) e sulla capacità di sensor-to-shooter. Il vincolo operativo dominante è la saturazione informativa multi-sensore e la compressione dei tempi di reazione, ulteriormente amplificati, nel contesto artico, dagli effetti della latitudine elevata sulla propagazione elettromagnetica, dalla variabilità ionosferica e dalle condizioni meteorologiche estreme, che degradano in modo selettivo le prestazioni dei sensori radar, dei link di comunicazione e dei sistemi di navigazione.

In particolare, fenomeni quali scintillazione ionosferica, ducting troposferico e riflessioni anomale sul pack glaciale introducono incertezze nella track quality e richiedono architetture di sensor fusion e track management adattive, specificamente tarate per ambienti ad alta latitudine.

L'Aeronautica Militare integra radar terrestri e aerotrasportati, sensori EO/IR (Electro-Optical/Infra-Red), SIGINT (SIGnal INTelligence) e assetti ISR in un'architettura AI-enabled orientata a track fusion, behavior-based threat assessment e anomaly detection. Le funzioni chiave includono multihypothesis tracking, track quality management e correlation cross-domain, con riduzione dei falsi positivi e incremento della persistenza delle tracce.

Nel contrasto a UAS/UCAS (Unmanned Aircraft System/Unmanned Combat Aerial System) e ad architetture cooperative multi-asset, le capacità Counter-UAS evolvono verso un approccio layered, comprendente Radio Frequence sensing, passive detection, jamming selettivo, spoofing GNSS e hard-kill. L'IA supporta classification, prioritization e dynamic resource allocation, consentendo la gestione di scenari di saturazione e swarm-like behavior senza sovraccaricare il livello decisionale umano.

In questo quadro, si inserisce quanto annunciato alla conferenza di Londra del 10 settembre 2025 da Helsing e Systematic, che hanno presentato lo sviluppo di

capacità europee di AI-powered swarm integrate nei sistemi C2. L'annuncio mostra come lo sciame cooperativo stia diventando una componente strutturale delle future architetture operative.
Il presente approccio è, però, orientato alla resilienza e al controllo dello spazio operativo: mentre ci si sta equipaggiando per comprendere, integrare e governare queste tecnologie, si sta già lavorando su modalità basate sull'IA per rendere inoffensive quelle avversarie, non solo contrastandole con mezzi cinetici o di jamming, ma intervenendo sulla loro logica di cooperazione, sulla fiducia tra gli elementi dello sciame e sui meccanismi decisionali distribuiti.
L'obiettivo è, quindi, duplice e complementare: sviluppare capacità sovrane sugli sciami cooperativi e, allo stesso tempo, costruire strumenti intelligenti per neutralizzarli in modo selettivo e controllato, trasformando una potenziale minaccia in un problema gestibile dal punto di vista operativo e decisionale.
Nel quadro delle minacce missilistiche ad alta velocità e manovrabilità, l'architettura integra multisensor correlation, cueing cross-domain e trajectory prediction probabilistica. Alle alte latitudini, la geometria delle traiettorie, la curvatura delle rotte polari e la variabilità delle condizioni ionosferiche impattano sui tempi di rilevamento e sulla qualità delle soluzioni di intercettazione, richiedendo modelli di predizione e cueing specificamente ottimizzati per profili polari. L'integrazione di dati spaziali, radar over-the-horizon e sensoristica aerotrasportata diviene pertanto un fattore discriminante per mantenere la coerenza del battle management in ambienti ad elevata complessità geofisica. L'IA supporta l'interceptor allocation e il battle management, incrementando il decision advantage in contesti time-critical, mantenendo il decisore umano al centro del processo di autorizzazione all'ingaggio.
I concetti di Loyal Wingman e di teaming uomo-macchina abilitano l'impiego coordinato di piattaforme manned e unmanned per compiti ad alto rischio, quali l'estensione di profondità ISR, electronic warfare (EW) e decoying. I sistemi unmanned operano in autonomia vincolata, con tasking dinamico, data relay e sensor extension, ampliando la profondità informativa e riducendo l'esposizione delle piattaforme con equipaggio. Nel teatro artico, tali concetti risultano particolarmente rilevanti per compensare le limitazioni di copertura radar, la ridotta persistenza degli assetti con equipaggio e l'elevata usura operativa dovuta alle condizioni ambientali estreme.
Una prova della validità di questa direzione è rappresentata dalla conferenza di Helsing AI sull'EFA, in cui viene mostrato come il teaming uomo-macchina non sia più un concetto prospettico, ma una linea di sviluppo già concreta. In tale contesto, l'Eurofighter viene descritto non come una piattaforma isolata, ma come il nodo centrale di un ecosistema cooperativo, capace di comandare e coordinare assetti unmanned attraverso l'IA. La conferenza chiarisce che l'obiettivo non è semplicemente integrare
nuovi sensori o incrementare le prestazioni della piattaforma, ma trasformare il caccia in una piattaforma AI-ready, in grado di orchestrare sistemi autonomi, gestire la complessità informativa e supportare il pilota nelle decisioni operative. L'IA viene,

quindi, presentata come moltiplicatore cognitivo, che consente il transito da una superiorità basata sulla singola piattaforma a una basata sulla cooperazione tra sistemi.
In questo senso, il Loyal Wingman e il teaming uomo-macchina assumono il ruolo di ponte operativo verso la sesta generazione: il velivolo manned resta il centro della responsabilità decisionale, mentre gli assetti unmanned diventano estensioni funzionali del sistema, impiegabili come sensori avanzati, jammer, relay, decoy o moltiplicatori di massa.
L'integrazione del dominio aereo con i domini marittimo, spaziale e cyber consente cueing reciproco, cross-validation delle tracce e riduzione dell'ambiguità informativa. In tale assetto, il dominio aereo fornisce il backbone di sorveglianza, correlazione e battle management, contribuendo in modo determinante alla coerenza della COP interforze e alla credibilità della deterrenza.

5. Dominio terrestre e sensoristica distribuita

Il dominio terrestre nel teatro artico riveste un ruolo strategico per la protezione dei nodi critici, in particolare landing station dei cavi sottomarini, infrastrutture energetiche, hub logistici e centri di controllo. L'Esercito Italiano assume una funzione primaria nella protezione fisica, nella capacità di early warning strutturato e di operare in ambienti caratterizzati da condizioni climatiche estreme e da frequente degradazione dei servizi GNSS.
Un elemento strutturale è rappresentato dall'impiego estensivo di Sistemi di Navigazione Inerziale su mezzi terrestri, UGV (Unmanned Ground Vehicles) e assetti ISR terrestri, al fine di garantire continuità operativa in ambienti GPS/GNSS-denied. L'INS consente navigazione autonoma, stabilizzazione dei sistemi d'arma e mantenimento della coerenza temporale e spaziale anche in presenza di jamming e spoofing, utilizzando sensori di movimento e computer per calcolare continuamente la posizione, l'orientamento e la velocità dell'oggetto in movimento, prescindendo da riferimenti esterni come il GPS. Il funzionamento dell'INS si basa sul principio della navigazione stimata (dead reckoning), che ha origine da posizione, velocità e orientamento noti e calcola, poi, gli aggiornamenti con integrazione di dati provenienti dai sensori interni. Il computer di navigazione elabora attraverso complessi algoritmi matematici i dati grezzi forniti dall'IMU (Inertial Measurement Unit), poi, integrati continuamente dal sistema. Eventuali minimi errori di misurazione nell'accelerazione, però, portano a errori di velocità e di posizione crescenti esponenzialmente. Per mitigare questo problema, gli INS moderni sono spesso sistemi ibridi che utilizzano la fusione dei sensori (spesso tramite un Filtro di Kalman). L'integrazione con odometri, radar locali, riferimenti terrestri e tecniche di sensor fusion riduce la
deriva e preserva l'affidabilità operativa.
Nel contesto artico, l'adozione di sensori FOG (Fiber Optic Gyroscopes), MEMS (Micro Electro Machine System) tattici selezionati e IMU (Inertial Measurement

Unit) rinforzate (gun-hardened) consente di assicurare robustezza meccanica, resistenza alle vibrazioni e stabilità anche su mezzi corazzati e piattaforme ad alta sollecitazione. Tali soluzioni supportano sia la mobilità tattica sia la stabilizzazione dei sistemi d'arma in movimento, aumentando la sopravvivenza e l'efficacia dei sistemi terrestri.

Analizzando i veicoli militari terrestri, l'INS svolge due funzioni operative principali: la navigazione tattica in ambienti GNSS-denied e la stabilizzazione dei sistemi d'arma. In scenari caratterizzati da jamming e spoofing, tipici del teatro artico, l'INS consente a mezzi corazzati, veicoli logistici e UGV di mantenere capacità di manovra e posizionamento anche in assenza di riferimenti satellitari affidabili.

La navigazione è basata su dead reckoning mediante integrazione di accelerazioni e velocità angolari, con mitigazione della deriva tramite odometri, radar locali e architetture di sensor fusion (filtri di Kalman), riducendo l'errore cumulativo di posizione.

Parallelamente, l'INS è integrato nei sistemi di controllo del fuoco per la stabilizzazione della torretta e del puntamento. I giroscopi misurano in tempo reale beccheggio, rollio e imbardata dello scafo, alimentando i loop di stabilizzazione dei servomotori per mantenere il cannone allineato sul bersaglio durante il movimento, abilitando il tiro in movimento ad elevata precisione. Le IMU impiegate devono essere progettate secondo standard "gun-hardened", per resistere a shock estremi generati dal rinculo del cannone e da esplosioni, garantendo continuità delle misure inerziali e affidabilità dei loop di stabilizzazione.

Le medesime architetture INS supportano anche l'impiego integrato di UAV (Unmanned Aerial Vehicle) tattici in supporto alle forze terrestri. In caso di perdita del GNSS, il drone passa alla guida inerziale pura, mantenendo la missione grazie a sensori a bassa deriva (FOG), con errori limitati per periodi dell'ordine di decine di minuti. L'INS è inoltre critico per il targeting, combinando posizione del drone e angoli della sensoristica EO/IR per la geolocalizzazione del bersaglio, dove la qualità angolare dell'INS è discriminante per ridurre errori di localizzazione a distanza.

Nel loro insieme, tali capacità rendono l'INS una componente strutturale per la resilienza operativa, la precisione del fuoco e l'integrazione manned-unmanned nel dominio terrestre artico.

Un secondo pilastro è rappresentato dalla sensoristica distribuita basata su DAS, che consente di trasformare infrastrutture in fibra ottica in una rete di sorveglianza passiva e persistente. Il DAS permette il rilevamento precoce di infiltrazioni, movimenti di mezzi ruotati e cingolati, attività di scavo e avvicinamenti a bassa quota, fornendo early warning in condizioni in cui sensori ottici e radar risultano degradati o vulnerabili.

Nonostante l'elevato potenziale operativo, i sistemi DAS presentano criticità legate all'elevato volume di dati e alla difficoltà di discriminare le firme rilevanti dal rumore ambientale, con conseguente incremento del rischio di falsi allarmi in scenari complessi. La qualità del dato dipende in modo critico dall'accoppiamento meccanico

tra fibra e terreno: installazioni non ottimali o in condotti determinano una significativa degradazione del segnale utile. Ulteriori limiti derivano dall'attenuazione ottica su lunghe distanze, che riduce la portata efficace del sistema.
L'integrazione di algoritmi di deep learning consente la classificazione automatica delle firme vibrazionali, la riduzione del rumore e il contenimento sistemico dei falsi positivi. L'impiego di fibre ad alta densità di scattering e tecniche di interramento diretto in materiali compattati migliora il rapporto segnale-rumore. Architetture di interrogazione a doppia estremità aumentano infine la resilienza della rete, garantendo continuità del monitoraggio anche in caso di danneggiamenti localizzati.
L'integrazione tra DAS, sensori elettro-ottici, radar terrestri e sistemi anti-drone, supportata da algoritmi di Machine Learning e Deep Learning, consente la classificazione automatica delle minacce, la riduzione dei falsi allarmi e la generazione di una picture terrestre orientata al pattern-of-life building e all'individuazione precoce delle anomalie. Questo approccio consente di superare i limiti della linea di vista, di operare in condizioni meteo estreme e di mantenere una capacità di sorveglianza continua con bassa osservabilità elettromagnetica.
Nel quadro interforze, l'Esercito Italiano opera in stretta sinergia con la Marina Militare, per la protezione delle landing station e dei nodi di connessione fondale-terra, e con l'Arma dei Carabinieri per le attività di law enforcement, attribuzione tecnica e contrasto alle minacce ibride. Tale integrazione consente di trasformare la protezione fisica in una capacità di deterrenza sottosoglia, fondata su rilevamento precoce, tracciamento persistente e risposta modulare.
In sintesi, il dominio terrestre costituisce l'ancoraggio fisico dell'architettura multi-dominio, assicurando la protezione dei punti di interfaccia critici (landing station, hub energetici e nodi C2). La combinazione di INS avanzati, sensoristica DAS e AI-enabled surveillance permette all'Esercito Italiano di garantire continuità operativa, resilienza alle interferenze elettroniche e protezione efficace dei nodi critici, riducendo ridondanze e concentrando l'efficacia sui fattori realmente discriminanti per il teatro artico.

6. Spazio e GNSS Resilience

L'efficacia dei domini aereo, marittimo e terrestre oggi non può più essere separata dal dominio spaziale.
Lo spazio non è soltanto un'infrastruttura di supporto, ma uno stato operativo emergente per l'intera Difesa, perché fornisce quei servizi abilitanti senza i quali nessun dominio può funzionare in modo coerente: PNT, sincronizzazione temporale globale, comunicazioni resilienti e ISR persistente.
Da questi dipendono direttamente la qualità delle tracce, la coerenza della COP e la continuità del processo decisionale.
Per Aeronautica, Marina ed Esercito questo significa che lo spazio è diventato il garante della stabilità operativa complessiva. Senza un PNT affidabile non esiste una navigazione sicura, non esiste una corretta sincronizzazione dei sensori e non può

esserci un C2 efficace. Senza un tempo comune non è possibile una vera integrazione multi-dominio. Il dominio spaziale è, quindi, un importante pilastro invisibile su cui poggia l'intera architettura operativa interforze e il suo valore distintivo nasce dalla sua prospettiva unica.

I satelliti osservano l'ambiente elettromagnetico "da fuori": non sono immersi nel campo come i sensori a terra, in mare o in aria, ma lo vedono dall'alto, con una geometria globale, stabile e non condizionata da orografia, clutter o mascheramenti locali. Questa distanza non è un limite, ma una forza, perché consente di cogliere la struttura complessiva dello spettro elettromagnetico e di comprendere non solo che qualcosa sta degradando, ma perché sta degradando.

Applicando l'IA ai payload RF, lo spazio diventa un vero sensore strategico dello spettro. I satelliti possono distinguere automaticamente tra disturbi naturali, interferenze accidentali e intenzionali, analizzandone l'estensione geografica, la coerenza spaziale e la dinamica temporale. Dove un radar, un sistema navale o un link di comunicazione percepiscono solo l'effetto, il dominio spaziale, grazie all'IA, contribuisce a identificarne la causa. È il passaggio da una percezione locale a una comprensione sistemica del dominio elettromagnetico.

Per l'Italia, questo è un elemento decisivo, perché consente di trasformare problemi tecnici in informazione operativa. Significa sapere dove il GNSS è affidabile e dove non lo è, distinguere se una degradazione è dovuta a fenomeni naturali o ad azioni ostili e capire quale dominio operativo ne sta subendo l'impatto principale.

In questo contesto, l'Aeronautica Militare, in coordinamento con le strutture nazionali, svolge un ruolo centrale nella SSA, nel monitoraggio delle interferenze GNSS e nell'integrazione dei dati spaziali nel data fabric interforze. Tuttavia, il valore di queste funzioni è pienamente interforze, perché ciò che nasce nello spazio alimenta direttamente le capacità operative dell'Esercito, della Marina e dell'Aeronautica, rafforzando la coerenza dell'intero sistema.

L'IA supporta GNSS interference classification, anomaly detection, pattern recognition e correlazione con dati RF ed elettromagnetici, abilitando contromisure adattive e riconfigurazione dinamica delle architetture PNT. In questo modo, si trasla da una dipendenza passiva dai servizi spaziali a una gestione attiva della loro affidabilità. L'obiettivo non è evitare ogni degradazione, ma governarla: sapere quanto si sta degradando una capacità, dove e con quali effetti, mantenendo operative le funzioni critiche.

Per l'Aeronautica, questo si traduce in una migliore qualità delle tracce, in una maggiore affidabilità per la navigazione, la difesa aerea e il C2. Per la Marina, significa garantire continuità alla navigazione oceanica, sicurezza alle operazioni subacquee e coerenza al coordinamento tra assetti di superficie, subacquei e aerei. Per l'Esercito, comporta una COP più affidabile, una sincronizzazione
temporale robusta per il C2 e una maggiore protezione contro minacce elettromagnetiche e anti-GNSS.

In sintesi, il dominio aereo costiuisce il backbone della sorveglianza, della correlazione

e del battle management, ma è il dominio spaziale, reso pienamente operativo dall'IA, a garantirne la resilienza temporale, navigazionale, elettromagnetica e informativa. Lo spazio diventa qualcosa di qualitativamente nuovo: non solo un fornitore di servizi, ma il dominio che osserva il sistema dall'esterno, qualifica l'affidabilità dell'informazione, spiega le cause delle degradazioni e protegge la coerenza decisionale dell'intera architettura interforze.

7. Cyber, informazione e Guerra Cognitiva

Il dominio cyber e informativo è un vettore primario della competizione sottosoglia. La presenza ostile, infatti, integra cyber operations, information manipulation e sfruttamento di vulnerabilità organizzative per degradare la COP e influenzare il decision-making della coalizione interforze.

L'Arma dei Carabinieri, nel ruolo di Stability Police, assume una funzione centrale nella protezione dell'integrità informativa, cognitiva ed economico-finanziaria del teatro, operando sui domini cyber, informativo e finanziario in modo integrato e orientato alla prevenzione delle manovre ibride. In tal modo, viene estesa la deterrenza anche agli ambiti non cinetici, riducendo la libertà di manovra dell'attore ostile nei domini immateriali.

A supporto di tale missione, l'Arma sviluppa il concetto operativo del C-FIC (Cognitive and Financial Intelligence Center), quale piattaforma AI-enabled di data fusion multi-dominio, orientata al monitoraggio e alla correlazione di flussi informativi, finanziari e tecnici. Per rendere operativo il CFIC, è previsto lo sviluppo di un modello di IA dedicato all'analisi integrata di tali flussi: in particolare, il sistema è progettato per operare pressoché in real time e per fornire, dapprima, una classificazione strutturata degli eventi (deepfake biometrici o schemi di riciclaggio), poi, la delimitazione spaziale e temporale delle anomalie e, infine, un livello di confidenza probabilistica, a supporto dei processi di escalation decisionale.

L'addestramento si fonda necessariamente su dataset compositi che integrano flussi finanziari sintetici

rappresentativi di schemi complessi di riciclaggio, contenuti video reali certificati e deepfake generati mediante tecniche avanzate, come GAN (Generative Adversial Networks) e modelli di diffusione, nonché dati degradati coerenti con le condizioni operative artiche. L'impiego sistematico di adversarial learning e di tecniche di data augmentation (rumore, bassa risoluzione, jitter, latenza simulata) consente di incrementare la robustezza del modello rispetto a contromisure avversarie, camouflage informativo-finanziario e degradazione della qualità del segnale.

L'architettura funzionale integra Vision Transformer per l'analisi video e l'estrazione di segnali biometrici, modelli linguistici per l'analisi semantica e il fact-checking delle narrative, e Graph Neural

Networks (GNN) per l'analisi di grafici. Prima dell'impiego operativo, il sistema è sottoposto a rigorosi processi di validazione. In coerenza con il principio Human-in-the-Loop, l'IA opera come moltiplicatore analitico e di allerta, mentre la responsabilità

finale delle decisioni operative resta in capo all'operatore umano, che si assume la piena responsabilità dell'azione tramite protocolli stringenti.
Il C-FIC opera, inoltre, mediante knowledge graphs e architetture predittive per identificare pattern ostili che combinano campagne di disinformazione, attività cyber e flussi finanziari anomali. Scopo della potenza ostile, infatti, potrebbe essere quello di fomentare la narrazione politica che punta all'indipendenza dell'area artica, in modo da avere ampio spazio di manovra per attuare una campagna di ingerenza nella regione stessa.
Nel dominio informativo, il C-FIC integra Content Credentials (obbligatorie per siti istituzionali, notizie di stampa, post e commenti derivanti da autori verificati sui social media) per la validazione della provenienza dei contenuti e moduli avanzati di deepfake detection, inclusa analisi biometrica tramite rPPG (remote PhotoPlethysmoGraphy), analisi di coerenza ambientale e incongruenze emotive.
Tali capacità consentono di attribuire un punteggio di affidabilità ai contenuti e di ridurre l'efficacia delle campagne di information manipulation.
Nel dominio finanziario, l'impiego di GNN consente il monitoraggio avanzato dei flussi economici, l'individuazione di pattern di riciclaggio, smurfing e utilizzo di cripto-asset, nonché l'identificazione di tentativi di acquisizione predatoria di nodi strategici. L'integrazione con protocolli KYC (Know Your Customer) evoluti e con modelli di financial forensics consente di supportare processi di azione preventiva e contrasto alle manovre ibride.
Il C-FIC correla, dunque, i domini informativo e finanziario con indicatori fisici (energia, logistica, risorse umane), consentendo di rilevare pre-posizionamenti, sabotaggi preparatori e anomalie compatibili con campagne multifase. Questa integrazione cyber–fisico–cognitiva rafforza la capacità di anticipazione e riduce l'ambiguità operativa

8. Architetture IA, Data Fusion e Governance algoritmica

L'architettura multi-dominio è fondata su un approccio AI-enabled e data-centric, nel quale l'IA costituisce il layer di fusione, correlazione e supporto decisionale a livello interforze.
I modelli adottati includono reti neurali per segnali e immagini, modelli linguistici per l'analisi informativa e GNN per la correlazione multi-entità. Tali modelli supportano data fusion, anomaly detection e pattern recognition, incrementando qualità e persistenza della Common Operational Picture.
L'implementazione segue un'architettura ibrida central/edge: infrastrutture HPC (High Performance Computing) per fusione e previsione centrale, edge AI su sensori e piattaforme per pre-processing e feature extraction, con riduzione della latenza e maggiore resilienza in ambienti contestati e caratterizzati da connettività intermittente, tipici delle regioni artiche e ad alta latitudine.
La governance algoritmica è strutturata su MLOps (Machine Learning Operations), validazione continua, controllo di versione, audit trail e tracciabilità end-to-end.

Questi meccanismi garantiscono affidabilità operativa e sostenibilità istituzionale dell'impiego dell'IA.
Il controllo umano resta centrale: interfacce uomo-macchina ed explainability assicurano prevenzione dell'over-reliance e responsabilità finale delle scelte sempre in capo all'autorità umana.
L'interoperabilità con architetture alleate, tramite federazione dei dati, standard di interfaccia e secure data sharing, abilita data fusion coalizionale mantenendo sicurezza, controllo e tracciabilità.
Nel loro insieme, tali elementi configurano un'architettura AI-enabled orientata a superiorità informativa, supporto decisionale avanzato e resilienza dell'ecosistema digitale multi-dominio.

9. Subsea Security Group come strumento di deterrenza

Il Subsea Security Group costituisce uno strumento operativo modulare per la protezione delle infrastrutture di fondale e per la gestione delle minacce subacquee. Esso integra capacità navali, subacquee, unmanned e cyber/OT in un unico framework operativo orientato alla riduzione dell'incertezza e al supporto alla decisione.
La configurazione Sentry fornisce sorveglianza persistente e riduzione dell'ambiguità, attraverso la presenza di unità C2/OPV, USV e AUV/ROV per ispezione selettiva, data collection e deconfliction.
Gli obiettivi sono la realizzazione di pattern-of-life subacquei e l'identificazione precoce di deviazioni comportamentali.
La configurazione Guardian introduce capacità di intervento e protezione attiva, includendo una nave madre, team subacquei specializzati, AUV/ROV e una cyber/OT cell integrata. Consente di gestire simultaneamente più minacce e di supportare processi di attribuzione tecnica attraverso raccolta forense avanzata.
La configurazione Bastion rappresenta il livello massimo di assetto operativo, con capacità ASWpassive rinforzate, boe gateway temporanee, AUV multipli, capacità di repair in prontezza e integrazione con assetti di supporto logistico e legale/ROE (Rules Of Engagement). Questo assetto è orientato a garantire dominanza informativa del seabed, resilienza sistemica e riduzione strutturale del rapporto costo-beneficio per l'attore ostile.
Nel suo complesso, il Subsea Security Group contribuisce alla deterrenza non attraverso l'invulnerabilità fisica, ma mediante la capacità di detection precoce, attribuzione tecnica sostenibile e ripristino rapido, abilitando una gestione controllata dell'escalation.

10. Roadmap decennale e raccomandazioni strategiche

L'evoluzione delle capacità multi-dominio nel teatro artico richiede una roadmap strutturata su un orizzonte di medio-lungo periodo, orientata a garantire coerenza tra sviluppo tecnologico, dottrina, formazione e governance, con priorità temporali chiare e milestones capacitive misurabili.

Una prima direttrice riguarda il consolidamento delle infrastrutture di sensoristica distribuita, delle architetture di data fusion e delle piattaforme AI-enabled, con priorità alla protezione delle installazioni critiche e all'integrazione interforze, da conseguire come capacità iniziale entro il breve-medio termine. In tale ambito, una capacità chiave è rappresentata dalla realizzazione di una rete integrata di sensori seabed–terra, comprendente DAS, reti acustiche e nodi C2 federati, in grado di supportare pattern-of-life building e early warning strutturato sulle opere di fondale, costituendo il nucleo di una Full Operational Capability (FOC) per la protezione integrata del seabed nel medio periodo.
Una seconda direttrice è rappresentata dallo sviluppo delle capacità di interoperabilità con gli alleati, inclusa la federazione dei dati, la standardizzazione delle interfacce e la condivisione selettiva delle informazioni rilevanti per la costruzione di una COP coalizionale. In questo contesto, una capacità chiave consiste nell'implementazione di meccanismi di federazione dinamica dei dati ISR e seabed-related, abilitando lo scambio selettivo e near-real-time di tracce, indicatori e pattern comportamentali tra livello nazionale e alleato.
Una terza direttrice riguarda la formazione di profili ibridi, in grado di integrare competenze operative, cyber, data analytics e IA, riducendo il gap tra capacità tecnologiche e capacità organizzative.
Diviene fondamentale lo sviluppo di team interfunzionali specializzati in data fusion multi-dominio e supporto decisionale, in grado di operare stabilmente all'interno delle catene C2 e dei centri di analisi interforze. È qui che le Accademie e i centri di formazione rivestono un ruolo centrale.
Infine, è essenziale rafforzare i meccanismi di governance, includendo policy per l'impiego dell'IA, framework di responsabilità, procedure di audit e meccanismi di controllo umano, al fine di garantire sostenibilità istituzionale, accettabilità politica e stabilità strategica.
Nel loro insieme, tali direttrici consentono di costruire un assetto multi-dominio credibile, resiliente e sostenibile, in grado di garantire protezione delle infrastrutture critiche, superiorità informativa e supporto decisionale in un teatro caratterizzato da elevata complessità.

11. Limiti strutturali e ambiti di non applicabilità dell'IA nei contesti multi-dominio artici

In coerenza con l'impostazione data-centric e AI-enabled dell'architettura multi-dominio delineata nei capitoli precedenti, è tuttavia necessario esplicitare gli ambiti strutturali di non applicabilità dell'IA come decisore autonomo.
In particolare, nei processi di impiego della forza letale, nella selezione autonoma dei target cinetici e cyber, nella valutazione delle intenzioni strategiche, nella pianificazione politico-militare e nei contesti caratterizzati da vincoli fisici severi (ambienti GNSS-denied, whiteout, propagazione acustica degradata e basso rapporto segnale/rumore), l'IA non può superare limiti sistemici legati alla fisica dei sensori, alla non osservabilità diretta delle intenzioni, ai requisiti di responsabilità giuridica

e alla necessità di ricostruibilità formale delle catene decisionali.
Le capacità avanzate descritte nel documento, quali INS, SLAM adattati, tecniche avanzate di sensorfusion e impiego di AUV in ambienti degradati, consentono una mitigazione significativa degli effetti operativi associati alla deriva inerziale, alla perdita di riferimenti GNSS, alla degradazione della qualità delle osservazioni sensoriali e all'incremento dell'incertezza di localizzazione e tracciamento, ma non ne eliminano la natura strutturale, imponendo il mantenimento del controllo umano nelle funzioni escalation-critical e safety-critical. Analogamente, nel dominio informativo e cognitivo, i moduli di deepfake detection e di validazione dei contenuti, inclusi quelli integrati nel C-FIC, devono essere interpretati come strumenti di supporto analitico e di attribuzione probabilistica, in grado di fornire punteggi di affidabilità e indicatori di anomalia, ma non come meccanismi di certificazione automatica e definitiva della verità. La dinamica competitiva tra tecniche generative e tecniche di rilevazione, la vulnerabilità ad attacchi adversarial e la presenza strutturale di falsi positivi e falsi negativi rendono, infatti, tecnicamente non garantibile una validazione assoluta.
Inoltre, nelle valutazioni a forte componente umana, che includono HUMINT, interpretazione del comportamento, intenzioni e dimensione psicologica, l'avversario dispone di margini intrinseci di deception e manipolazione, potendo produrre segnali intenzionalmente ingannevoli per condizionare l'addestramento e l'impiego dei modelli, sfruttarne le vulnerabilità e indurre bias sistematici o errori di classificazione in modo deliberato. Anche in questo frangente, il giudizio umano resta non sostituibile perché fondato sullo studio del contesto culturale e sull'interpretazione qualitativa e valutazione critica delle incongruenze.
Ne consegue che, pur configurandosi come moltiplicatore essenziale per sensing, data fusion, anomaly detection e decision support, l'IA deve essere impiegata entro cornici architetturali vincolate, nelle quali i meccanismi human-in-the-loop assicurano il controllo umano, la responsabilità decisionale e la gestione dell'escalation per tutte le funzioni ad alto impatto legale, strategico ed escalationcritical.
Questi aspetti non rappresentano una limitazione contingente della tecnologia, ma un vincolo strutturale necessario a garantire affidabilità operativa, coerenza dottrinale, conformità normativa, stabilità strategica e sostenibilità istituzionale dell'architettura multi-dominio.

Conclusioni

Il quadro delineato evidenzia come il teatro artico sia caratterizzato da una competizione strutturale, nella quale la protezione delle infrastrutture critiche, la superiorità informativa e la capacità di attribuzione tecnica sostenibile assumono un valore direttamente connesso alla credibilità della deterrenza euro-atlantica. In questo scenario complesso, la risposta nazionale non può limitarsi alla somma delle capacità delle singole Forze Armate, ma deve evolvere verso un ecosistema operativo realmente integrato.

La Marina Militare si configura quale perno operativo del sistema, in virtù della sua capacità di garantire presenza persistente, controllo delle SLOC, protezione delle infrastrutture di fondale e integrazione delle capacità subacquee, unmanned e cyber/OT. La gestione del seabed, l'Underwater Domain Awareness e l'impiego del Subsea Security Group rappresentano moltiplicatori di efficacia che consentono di ridurre l'incertezza, anticipare le minacce e sostenere processi di attribuzione tecnica a supporto delle decisioni politico-strategiche. La sicurezza del "sistema nervoso" sottomarino, tuttavia, non termina sulla linea di costa, ma necessita di una protezione senza soluzione di continuità.

Nel contesto evidenziato, è qui che si realizza la saldatura strategica tra Esercito Italiano e Arma dei Carabinieri, che insieme costituiscono un baluardo unico contro le minacce fisiche e ibride. L'Esercito blinda il dominio terrestre adottando tecnologie d'avanguardia per operare in contesti estremi: grazie ai sistemi di Navigazione Inerziale, garantisce capacità di manovra e fuoco anche in ambienti GPSdenied (soggetti a jamming), assicurando la difesa fisica dei nodi critici come le landing station. Parallelamente, insieme alla Marina Militare l'impiego del DAS permette alla Forza Armata di trasformare i cavi in fibra ottica in una rete di sensori "invisibili" e distribuiti, capaci di rilevare infiltrazioni o sabotaggi fisici con precisione millimetrica. Questa cornice di sicurezza materiale trova il suo naturale completamento nell'azione dell'Arma dei Carabinieri, che estende la difesa alla dimensione cognitiva e legale. Agendo come Stability Police, i Carabinieri presidiano la "zona grigia" del conflitto ibrido attraverso il Cognitive & Financial Intelligence Center. Utilizzando algoritmi avanzati per l'analisi dei flussi finanziari e la deepfake detection, l'Arma identifica e neutralizza le campagne di disinformazione e le manovre economiche ostili che spesso preparano il terreno all'azione cinetica, garantendo, così, una protezione del territorio impermeabile non solo agli attacchi materiali, ma anche a quelli immateriali.

A chiudere il cerchio della sicurezza multi-dominio interviene l'Aeronautica Militare, che proietta la difesa nella terza dimensione e nello spazio. Il suo contributo è essenziale per la SSA e la resilienza dei servizi di navigazione e sincronizzazione (PNT). Senza la copertura dei sensori aerei e spaziali e senza la capacità di gestire i dati in arrivo dall'orbita, anche l'architettura informativa sottostante rischierebbe di perdere coerenza temporale e spaziale.

Il rafforzamento ulteriore delle capacità marittime e subacquee, inserito in una cornice interforze strutturata e continuativa, rappresenta pertanto una scelta strategica per garantire credibilità della deterrenza, protezione delle infrastrutture critiche e stabilità nel teatro artico. In questo assetto, la Marina Militare resta un fulcro operativo, ma è l'interforze a determinare il livello reale di efficacia, resilienza e credibilità dell'intera architettura di sicurezza multi-dominio.

La deterrenza strategica non può più essere affidata alla somma aritmetica delle singole capacità, ma deve evolvere verso una sinergia interforze profonda e strutturale, che agisca come un vero moltiplicatore di potenza. Tuttavia, in uno scenario

caratterizzato da una saturazione informativa senza precedenti e da minacce ibride che operano al di sotto della soglia di rilevamento tradizionale, questa integrazione rimarrebbe un concetto astratto senza il contributo determinante dell'Intelligenza Artificiale.
Quest'ultima si configura, infatti, come il "sistema nervoso" dell'intera architettura di difesa: è l'unico strumento in grado di fondere in tempo reale la mole eterogenea di dati provenienti dai sonar della Marina, dalle fibre ottiche dell'Esercito, dai satelliti dell'Aeronautica e dalle analisi forensi dei Carabinieri. Solo attraverso algoritmi di Data Fusion avanzata e Machine Learning è possibile correlare segnali deboli e apparentemente slegati (una vibrazione sismica, un'anomalia termica, un flusso finanziario sospetto), trasformandoli in una COP predittiva e azionabile. Il futuro dello scenario euro-atlantico dipenderà, dunque, dalla capacità di realizzare questo ecosistema cibernetico-militare, dove la tecnologia non sostituisce l'uomo, ma ne potenzia la velocità decisionale, garantendo all'Italia una postura di sicurezza resiliente, adattiva e tecnologicamente sovrana.

- ***Proiezione con video Accademia dell'Aeronautica Militare: https://youtu.be/6r-YdJQjMPc?t=13262 (3:41:20 – 3:46:00) (seconda parte dell'intervento da 3:57:00 a 4:04:45)***

- ***Proiezione con video Accademia Militare di Modena: https://youtu.be/6r-YdJQjMPc?t=13576 (3:46:20 – 3:50:30) (seconda parte dell'intervento da 4:05:15 a 4:11:30)***

- ***Proiezione con video Accademia Navale della Marina Militare: https://youtu.be/6r-YdJQjMPc?t=13836 (3:50:45 – 3:56:35) (seconda parte dell'intervento da 4:11:40 a 4:13:40)***


STEM
scenari di crisi simulata

SISTEMI DI NAVIGAZIONE INERZIALI

LE APPLICAZIONI OPERATIVE

- Sopravvivenza in zone "GPS-Denied" (Anti-J amming)
- Geo-localizzazione del bersaglio (Targeting)
- Volo Autonomo in Ambienti chiusi o complessi

INTEGRAZIONE CON ALTRI SENSORI

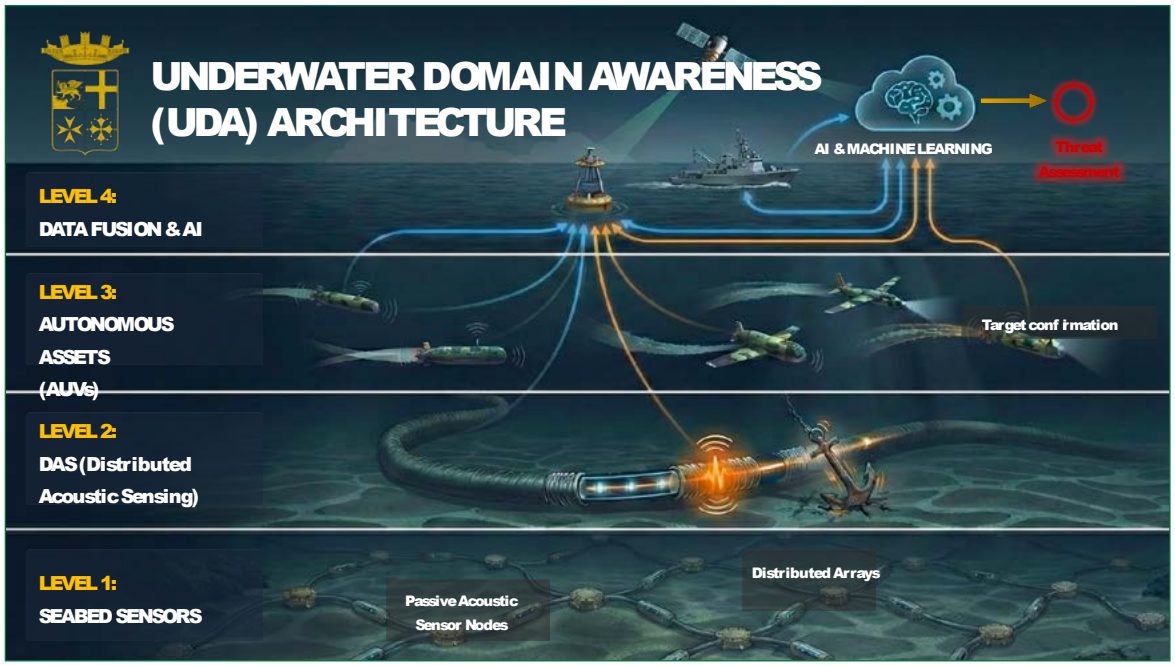
- INS + Optical Flow (VIO)
- INS + TERCOM (Radar Altimeter)

DISTRIBUTED ACOUSTIC SENSING

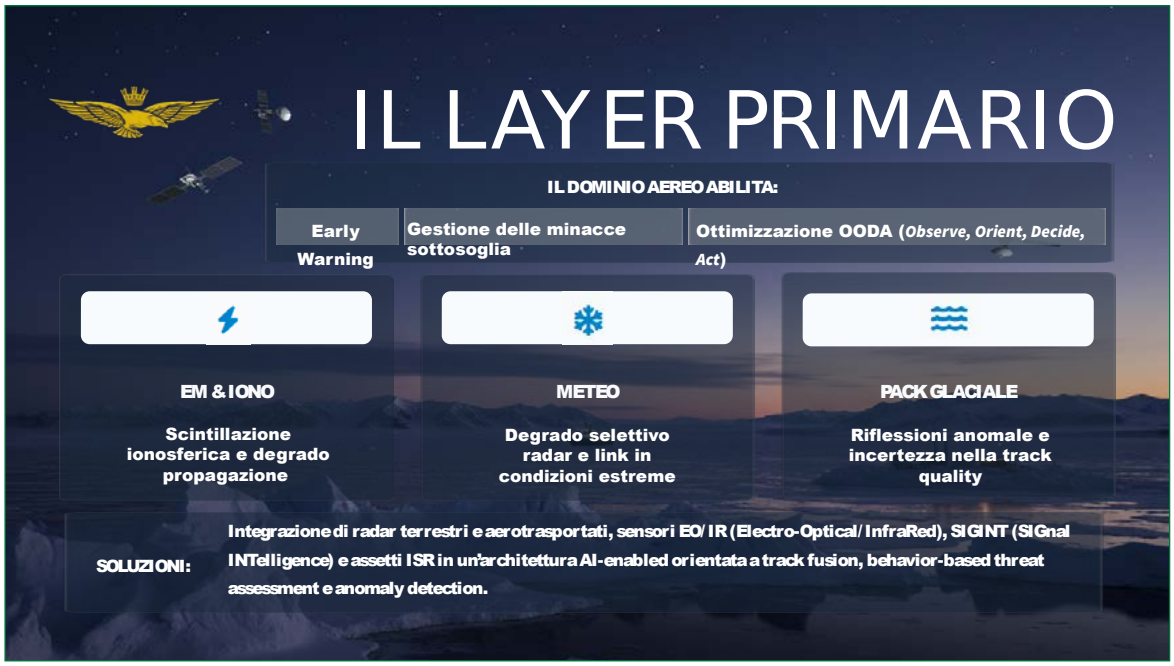
- Consapevolezza situazionale passiva
- Monitoraggio persistente “All-weather” e “All-terrain”
- Profondità di rilevamento ed early warning

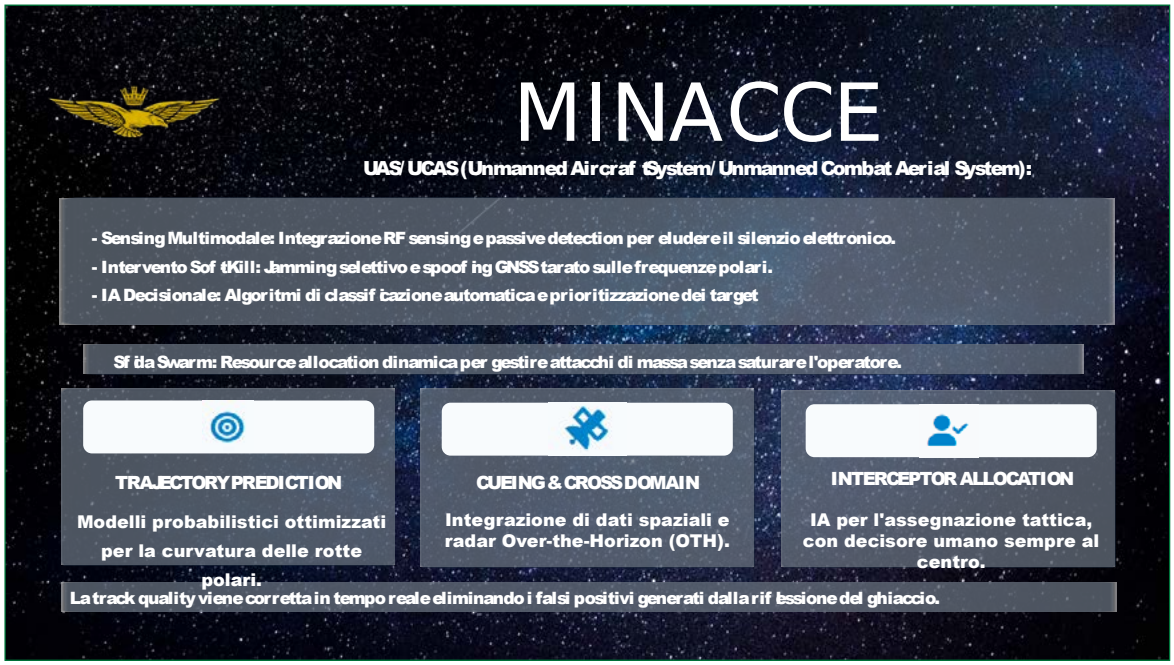
- Sensibilità Direzionale
- Dipendenza dal Tipo di Terreno
- Vulnerabilità al "Taglio Strategico"


Protezione delle critical underwater infrastructure (cui)
NUOVA DIMENSIONE DEL MEDITERRANEO
NEMICO OPERA NELLA GREY-ZONE: NAVI SCIENTIFICHE, MERCANTILI, DRONI DUAL-USE
SLOC, PIPELINES


UNDERWATER DOMAIN AWARENESS (UDA) ARCHITECTURE
AI & MACHINE LEARNING
Threat Assessment
LEVEL 4:
DATA FUSION & AI
LEVEL 3:
AUTONOMOUS ASSETS (AUVs)
Target confirmation
LEVEL 2:
DAS (Distributed Acoustic Sensing)
LEVEL 1:
SEABED SENSORS
Passive Acoustic Sensor Nodes
Distributed Arrays


Subsea security group
SENTRY
Monitoraggio & Early Warning
Offshore Patrol Vessel
AUVs/ROVs
GUARDIAN
Pattugliamento attivo & Risposta rapida
Cyber/OT Cell imbarcata
Team subacquei specializzati
BASTION
Intervento rinforzato
Capacità ASW rinforzate
Nave posacavi e boe


IL LAYER PRIMARIO
IL DOMINIO AEREO ABILITA:
Early Warning
Gestione delle minacce sottosoglia
Ottimizzazione OODA (Observe, Orient, Decide, Act)
EM & IONO
Scintillazione ionosferica e degrado propagazione
METEO
Degrado selettivo radar e link in condizioni estreme
PACK GLACIALE
Riflessioni anomale e incertezza nella track quality
SOLUZIONI:
Integrazione di radar terrestri e aerotrasportati, sensori EO/IR (Electro-Optical/InfraRed), SIGINT (SIGnal INTelligence) e assetti ISR in un'architettura AI-enabled orientata a track fusion, behavior-based threat assessment e anomaly detection.


MINACCE
UAS/UCAS (Unmanned Aircraft System/Unmanned Combat Aerial System):
- Sensing Multimodale: Integrazione RF sensing e passive detection per eludere il silenzio elettronico.
- Intervento Soft Kill: Jamming selettivo e spoofing GNSS tarato sulle frequenze polari.
- IA Decisionale: Algoritmi di classificazione automatica e prioritizzazione dei target
Sfida Swarm: Resource allocation dinamica per gestire attacchi di massa senza saturare l'operatore.
TRAJECTORY PREDICTION
Modelli probabilistici ottimizzati per la curvatura delle rotte polari.
CUEING & CROSS DOMAIN
Integrazione di dati spaziali e radar Over-the-Horizon (OTH).
INTERCEPTOR ALLOCATION
IA per l'assegnazione tattica, con decisore umano sempre al centro.
La track quality viene corretta in tempo reale eliminando i falsi positivi generati dalla riflessione del ghiaccio.

INTEGRAZIONE FINALE

Manned-Unmanned:
Impiego coordinato di *Loyal Wingman* per estendere ISR e guerra elettronica (EW).

UNMANNED:

- **Autonomia vincolata**
- **Data relay**
- **Tasking dinamico**
- **Sensor extension**

BACKBONE DEL DOMINIO AEREO:

Integrazione con dominio Marittimo, Terrestre, Spaziale e Cyber per una COP coerente e una deterrenza credibile nel teatro artico.

Munich, 19.11.2025

Helsing upgrades Eurofighter with Artificial Intelligence

Arctic-sentinel

Intelligence Center

Stability Police nella regione artica, 2036

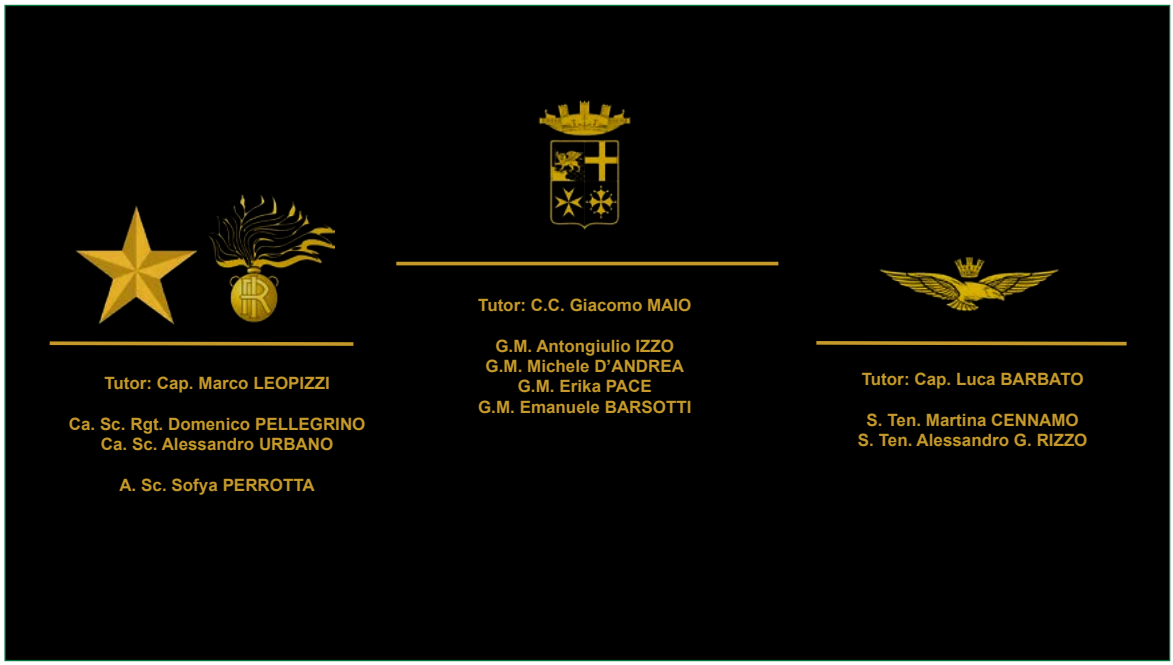
architettura

- **Modulo informativo**
  - Content Credentials
  - Analisi biometrica (rPPG)
- **Modulo finanziario**
  - GNN (Graph Neural Networks)
  - Know Your Customer
- **MODULO DI SENSORISTICA**
  - Analisi dati dei sensori terrestri

MODELLO AI

- **Modello**
  - Vision Transformers (ViT)
  - Large Language Models (LLM)
  - Graph Neural Networks (GNN)
- **Funzionamento**
  - Input: Stream video/audio, log finanziari, metadati social.
  - Output: Classificazione dell'evento (es. "deepfake biometrico", "flusso di riciclaggio"), delineazione spaziale e temporale (dove inizia e finisce l'anomalia, quando è stata rilevata), livello di probabilità percentuale.

Human-in-the-loop


Tutor: Cap. Marco LEOPIZZI
Ca. Sc. Rgt. Domenico PELLEGRINO
Ca. Sc. Alessandro URBANO
A. Sc. Sofya PERROTTA
Tutor: C.C. Giacomo MAIO
G.M. Antongiulio IZZO
G.M. Michele D'ANDREA
G.M. Erika PACE
G.M. Emanuele BARSOTTI
Tutor: Cap. Luca BARBATO
S. Ten. Martina CENNAMO
S. Ten. Alessandro G. RIZZO

Accademia Militare Esercito Italiano

Accademia Navale Marina Militare

Accademia Aeronautica

Accademia Militare Esercito Italiano - Allievi Ufficiali Arma dei Carabinieri

TERZO PANEL

"Applicazioni STEM a scenari di crisi simulati"

PARTE SECONDA

Presentazione del progetto del
Centro Alti Studi Difesa/Scuola Superiore Universitaria (CASD/SSU)
"AI LITERACY dall'esigenza all'offerta formativa"

STEM

CASD

"AI LITERACY dall'esigenza all'offerta formativa"

ENTE

Centro Alti Studi Difesa
Scuola Superiore Universitaria

"AI Literacy dall'esigenza all'offerta formativa"

Nel corso della nostra partecipazione al gruppo di lavoro che ha contribuito alla redazione della Strategia della Difesa per l'intelligenza artificiale, è emersa con chiarezza un'esigenza formativa specifica: progettare un intervento capace di mitigare gli effetti del divario di competenze, fenomeno tipico delle fasi di rapido sviluppo tecnologico.

I successivi approfondimenti ci hanno condotto alla proposta che presentiamo oggi, articolata attorno a tre obiettivi principali. In primo luogo, un obiettivo informativo: intendiamo illustrare il modello di progettazione didattica che stiamo sviluppando, caratterizzato dal ricorso al microlearning (particolare forma di e-learning) come modalità prevalente di erogazione. In secondo luogo, un obiettivo divulgativo: i contenuti prodotti saranno resi disponibili sulla nostra piattaforma e quindi accessibili a tutti gli enti della Difesa che ne avranno necessità. Infine, un obiettivo propositivo: alla luce dell'esperienza maturata, ci proponiamo di contribuire alla formazione di progettisti didattici delle F.A. chiamati ad affrontare progettualità analoghe.

Presentazione CASD

Colonello Giacinto D'URSO, Capitano di Fregata Gilberto PETRINI

Nel corso di questo intervento, oltre a delineare il contesto di riferimento, illustreremo il processo di progettazione del corso di alfabetizzazione all'intelligenza artificiale (AI literacy di livello basico), descriveremo gli strumenti metodologici adottati e presenteremo una dimostrazione dell'esperienza formativa prevista per i partecipanti. Per quanto riguarda il contesto, la principale sfida riguarda la costruzione di un'offerta formativa sull'intelligenza artificiale che sia il più possibile estesa

all'interno dell'organizzazione della Difesa, costantemente aggiornata e adattabile alle esigenze dei diversi pubblici di riferimento. Si tratta di una formazione che deve essere profondamente integrata con le soft skills, al fine di promuovere lo sviluppo di un autentico mindset digitale.

L'obiettivo è duplice: da un lato, ridurre il divario generazionale; dall'altro, favorire un'integrazione responsabile delle nuove tecnologie, promuovendone un uso etico, consapevole ed efficace. È importante sottolineare come questa sfida non sia unidirezionale, ma coinvolga l'intera organizzazione: la leadership, le strutture intermedie e la base, inclusi i più giovani, che spesso dimostrano una particolare familiarità con questi strumenti. In questo contesto, occorre gestire un ampio spettro di atteggiamenti, che spaziano dall'eccessiva fiducia alla diffidenza nei confronti delle nuove tecnologie.

Per affrontare in modo strutturato tale sfida, presso il CASD abbiamo condotto, nei mesi scorsi, un'attività di ricerca utilizzando strumenti di valutazione dell'AI literacy già presenti in letteratura. A partire da questi strumenti, è stato elaborato un questionario somministrato ai frequentatori e al personale permanente del nostro Ateneo. Circa 300 partecipanti hanno preso parte all'indagine, costituendo un campione che riteniamo rappresentativo per eterogeneità di genere, status (militare e civile), livello di istruzione e ruolo professionale, includendo professori universitari, manager, dirigenti militari e personale con differenti livelli funzionali.

I risultati principali della rilevazione possono essere sintetizzati come segue: a fronte di un livello di AI literacy percepita mediamente elevato — con una prevalenza di autovalutazioni collocate nelle fasce "buono" e "ottimo" — la misurazione oggettiva delle competenze evidenzia prestazioni mediamente più contenute, con oltre la metà del campione situata nei livelli più bassi di competenza effettiva. Inoltre, solo una minoranza dei partecipanti mostra un allineamento tra percezione e competenza reale, mentre una quota significativa tende a sovrastimare o, in misura minore, a sottostimare le proprie capacità.

Queste evidenze — che indicano come spesso le persone ritengano di possedere competenze superiori a quelle effettivamente detenute — hanno rafforzato la nostra convinzione circa la necessità di un intervento formativo in grado di intercettare bisogni di apprendimento eterogenei. Tali bisogni vanno oltre le sole competenze tecniche: la formazione specialistica in ambito di intelligenza artificiale deve infatti poggiare su una solida base generalista, riconducibile al concetto di AI literacy.

A partire da queste premesse, abbiamo riunito le risorse disponibili all'interno del CASD — progettisti didattici formati internamente e subject matter expert — avviando una prima fase di progettazione che ha condotto alla definizione della struttura del corso. Questo è stato articolato in quattro aree principali: un'area cognitiva, dedicata alle conoscenze; un'area operativa, focalizzata sull'utilizzo delle applicazioni, modulata in funzione del livello dell'audience; un'area di valutazione critica e sulle soft skills/digital mindset; e infine un'area incentrata sull'etica ed il rispetto di policy e norme per un uso consapevole e responsabile delle nuove tecnologie.

Questo corso non è stato progettato secondo modalità tradizionali, ma è il risultato di un processo di co-progettazione con sistemi di intelligenza artificiale. Tale scelta non risponde a una logica dimostrativa o meramente tecnologica, bensì a un'impostazione metodologica consapevole e coerente con gli obiettivi didattici prefissati.
L'intelligenza artificiale è stata infatti impiegata come strumento di supporto e di amplificazione delle capacità creative del progettista didattico, non in sostituzione del suo ruolo. Parallelamente, ha consentito una significativa accelerazione dei tempi di sviluppo, mantenendo tuttavia una supervisione umana costante lungo tutte le fasi del processo: dalla progettazione alla realizzazione, fino alla verifica e validazione finale, affidata a un apposito comitato scientifico.
Per quanto attiene al workflow adottato, il processo ha avuto inizio con la selezione e validazione delle fonti bibliografiche. Successivamente, mediante applicativi potenziati dall'intelligenza artificiale, si è proceduto alla generazione di contenuti multimediali, tra cui mappe concettuali, infografiche, podcast audio e video. A questa fase è seguita la definizione dello storyboard — inteso come una vera e propria sceneggiatura didattica — e la successiva realizzazione delle lezioni.
Le unità formative così prodotte sono state integrate all'interno della piattaforma Moodle, dove sono state arricchite con attività pratiche, momenti riflessivi e materiali di approfondimento. L'intero progetto è stato condotto in coerenza con i principali riferimenti normativi e standard internazionali, tra cui il quadro europeo delle competenze digitali (Digicomp 3.0 che include l'intelligenza artificiale), i più recenti standard per i sistemi di gestione dell'IA e la normativa nazionale di settore.
Questa esperienza ha consentito di evidenziare alcuni vantaggi significativi della co-progettazione essere umano–intelligenza artificiale: in primo luogo, la capacità di coniugare creatività e intuizione umana con la potenza analitica delle macchine, favorendo la generazione di soluzioni innovative; in secondo luogo, il miglioramento dell'efficienza, grazie alla riduzione dei tempi di sviluppo e all'ottimizzazione delle risorse; infine, la promozione di un approccio inclusivo, basato sull'integrazione di prospettive diverse nella risoluzione di problemi complessi.
Venendo ora alle scelte metodologiche, il corso è stato sviluppato adottando il microlearning, una specifica declinazione dell'e-learning basata su unità formative brevi — le cosiddette "pillole" — della durata indicativa di 5–8 minuti ciascuna. Tali unità sono progettate per essere fruite in modo flessibile, anche in mobilità, e rispondono non a una logica di semplificazione dei contenuti, bensì a un principio di precisione didattica, attraverso la scomposizione di temi complessi in moduli cognitivamente sostenibili. Il ridotto carico cognitivo, unito all'elevato grado di multimedialità e interattività, rende questa metodologia particolarmente efficace sia per la formazione professionale (tenendo conto anche dei principi andragogici dell'adult learning) sia come momento di apprendimento propedeutico all'attività in presenza, di rinforzo o consolidamento successivo alla stessa.
Per la realizzazione del corso, ci siamo avvalsi di una "cassetta degli attrezzi" selezionata sulla base di studi di settore e di esperienze maturate nella formazione

interna degli instructional designer. In particolare, la progettazione e strutturazione delle unità formative è stata supportata da strumenti di intelligenza artificiale generativa; la gestione e l'organizzazione delle fonti, previamente validate dal comitato scientifico, mediante NotebookLM ha consentito una rapida produzione di contenuti editoriali e multimediali; ulteriori strumenti sono stati impiegati per la creazione di video-lezioni, talvolta presentate con il ricorso ad avatar digitali.
La fase finale di assemblaggio delle unità didattiche è stata realizzata mediante un authoring tool professionale, che ha permesso di integrare in modo efficace contenuti interattivi e multimediali. È importante sottolineare come, nella maggior parte dei casi, siano stati utilizzati strumenti accessibili e sostenibili, spesso in versione gratuita o sperimentale.
Dal punto di vista dell'esperienza utente, il corso è stato progettato per garantire un'interfaccia semplice e intuitiva, che accompagna il discente lungo un percorso flessibile e personalizzabile. Ogni microlezione prevede una struttura base ricorrente: definizione dei micro-obiettivi formativi, testo introduttivo, video-lezione di 5-8 minuti in media, attività di consolidamento delle conoscenze apprese e, ove necessario, la presentazione di casi d'uso integrati con esercitazioni interattive — incluse simulazioni decisionali — e quiz formativo.
Particolare attenzione è stata dedicata all'interattività e al coinvolgimento attivo dell'utente, attraverso quiz diversificati, attività di associazione e strumenti di gamification, nonché esercizi riflessivi finalizzati allo sviluppo del pensiero critico.
Al termine del percorso, è previsto un test di valutazione complessiva (sempre di carattere formativo, con feedback per le risposte date, siano esse corrette o meno, nonché la possibilità per il discente di ripeterlo finché non raggiunge la sufficienza prevista), generato con AI Assistant dell'authoring tool sulla base di tutto il materiale del corso, ma sempre sottoposto a revisione/validazione umana. Il corso viene quindi erogato attraverso la piattaforma didattica del CASD basata sul Learning management System Moodle residente sul PSN - Polo Strategico Nazionale.
In sintesi, i principali punti di forza del progetto possono essere ricondotti a tre dimensioni: un significativo incremento dell'efficienza progettuale rispetto ai metodi tradizionali; la capacità di produrre rapidamente contenuti multimediali diversificati e ad alto livello di engagement; e, soprattutto, il mantenimento di una revisione/supervisione umana dei contenuti generati dall'IA integrale lungo tutto il processo.
In conclusione, riteniamo opportuno sottolineare come l'AI literacy non rappresenti una competenza tecnica specialistica, bensì una condizione abilitante. In quanto tale, non può essere improvvisata: deve essere strutturata, standardizzata, scalabile e integrata nei sistemi formativi esistenti.
Se vogliamo disporre di personale in grado di utilizzare l'intelligenza artificiale in modo consapevole, critico ed etico, è necessario intervenire innanzitutto sulle modalità con cui lo formiamo. E, soprattutto, è necessario farlo con tempestività.

Proiezione con video: https://youtu.be/6r-YdJQjMPc?t=18723 (5:12:20 – 5:31:45)

AI Literacy

Dall'esigenza all'offerta formativa

OBIETTIVO

INFORMATIVO
(modello di progettazione didattica adottata)

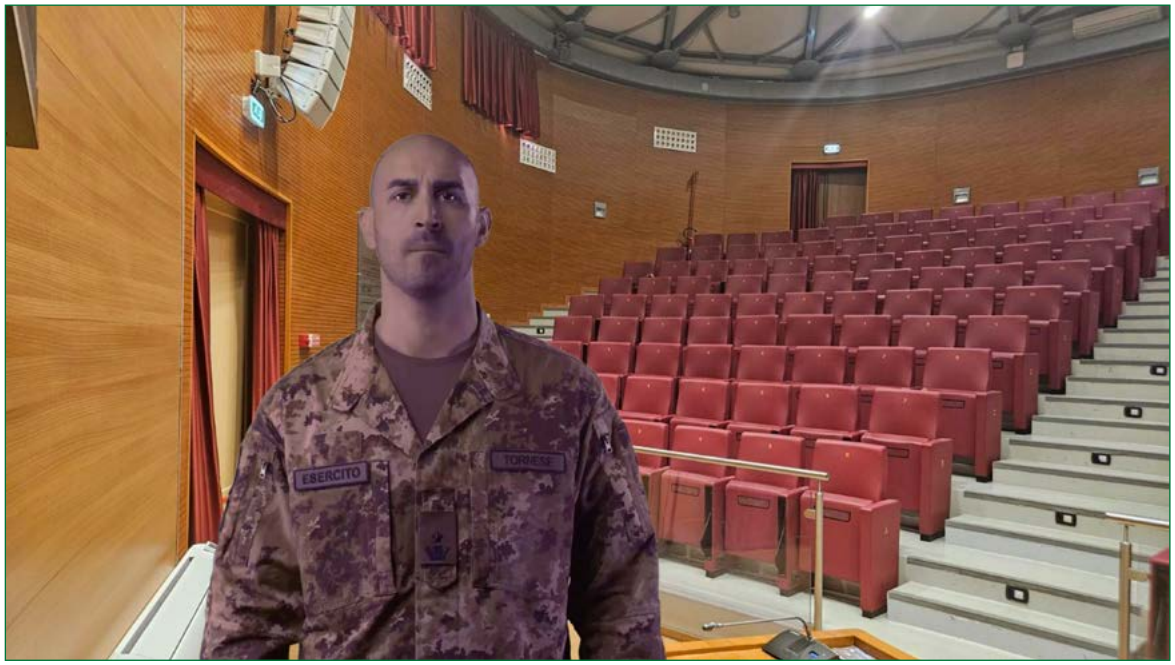
DIVULGATIVO
(contenuto e-learning disponibile ambito difesa)

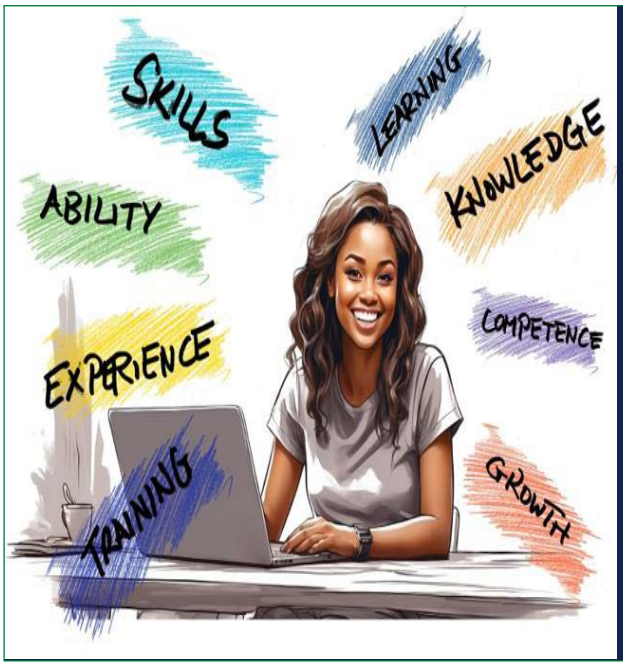
PROPOSITIVO
(corsi di formazione per progettisti didattici per e-learning)


INDICE DEGLI ARGOMENTI
Contesto
Progettazione
di un corso di IA literacy
Strumenti utilizzati
Output prodotto

CONTESTO


La SFIDA dell'IA Literacy
Superare il divario generazionale
Favorire l'integrazione responsabile
Promuovere un uso consapevole, efficace ed Etico
NotebookLM


ESERCITO



Necessità di interventi formativi capaci di intercettare bisogni di apprendimento eterogenei.

7

PROGETTAZIONE

Corso AI literacy

Co-design con l'IA

Questo corso non è stato progettato nel modo tradizionale

METODO

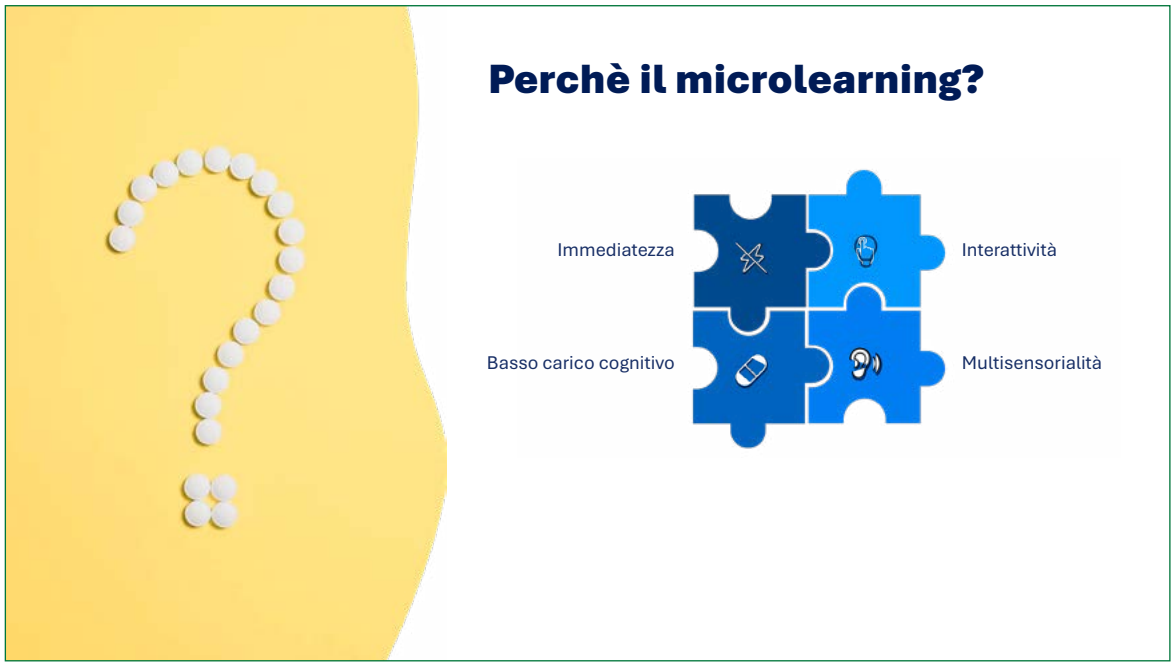
Approccio Learning Design Driven

Il Ruolo dell'IA

L'Intelligenza Artificiale non sostituisce il progettista didattico, ma ne amplifica le capacità operative e creative.

Validazione umana

Ogni contenuto generato è stato sottoposto a revisione critica e validazione da parte di esperti didattici.



REALIZZAZIONE

Strumenti utilizzati

CASSETTA DEGLI STRUMENTI AI-POWERED

- **CO-DESIGN IA** (ChatGPT – Copilot) FREE License
- **GESTIONE FONTI** (NotebookLM) FREE
- **AVATAR VIDEO** (Heygen) License
- **INFOGRAFICHE** (Napkin) FREE
- **PRODOTTI EDITORIALI** (CanvaAI – MS365) FREE License

OUTPUT

Il corso in microlearning "AI literacy"


Live demo


IA Literacy: progettare la formazione del futuro con l'IA
La sfida e i 4 pilastri dell'alfabetizzazione
Navigare la complessità dell'IA
Contrastare il rischio di fake news e il social divide con una base conoscitiva condivisa.
Cognitivo
Comprendere le basi
Capacitivo
Uso responsabile delle tecnologie
Critico
Valutazione critica
Etico
Implicazioni etiche nel lavoro
Il metodo: co-design "IA-Augmented"
Workflow di Sintesi
Produzione Pillole (SCORM, Video, Podcast, Infografiche) per LMS Moodle
+17%
di memorizzazione
Il microlearning aumenta la retention rispetto ai formati tradizionali, riducendo il carico cognitivo.
Validazione Umana
(Co-Designer)
Processore Digitale
(Assistente IA)
L'IA come Co-Designer, non come decisore.
Strumenti come ChatGPT e NotebookLM supportano la sintesi e la struttura, ma l'uomo valida.
Risultati del Co-Design "IA-Augmented"
4x
Efficienza Progettuale
Drastica riduzione dei tempi di produzione mantenendo il 100% di validazione umana.
Approccio IA-Augmented
Risultato
Produzione
4 volte più veloce
Formati
6+
(Video, Podcast, Infografiche)
Validazione
100% Supervisione Umana


CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA
Grazie per l'attenzione


Scuola Navale Militare


“Francesco MOROSINI”
DISCIPLINE
ESERCITO
MASIELLO

Quarto Panel

"Formazione Militare, Discipline STEM e Intelligenza Artificiale: una sintesi compiuta?"

STEM

Intervista al Comandante per la Formazione, Specializzazione e Dottrina dell'Esercito Generale di Corpo d'Armata Antonello VESPAZIANI

Generale di Corpo d'Armata
Antonello VESPAZIANI

Il militare del futuro: le materie STEM nei percorsi formativi attuali per preparare personale in grado di operare in scenari dominati dall'AI: Come sta cambiando l'identità del soldato italiano grazie alla Sofimatica e all'alfabetizzazione digitale?

La vera forza dell'Esercito è da sempre la sua componente umana. L'attuale scenario geo-strategico impone un processo di trasformazione dello Strumento militare anche per quanto attiene alla formazione. Proprio la Formazione, la Specializzazione, la Selezione e il Reclutamento del personale di Forza Armata fanno capo al COMFORDOT (Ufficiali, Sottufficiali e Volontari). Si è proceduto ad un'alfabetizzazione all'I.A. per il personale effettivo, mediante il ricorso ai cosiddetti MOOC, disponibili sul Portale Multimediale di Forza Armata (PMFA), che consente ai circa 80.000 iscritti di potersi aggiornare in autonomia, utilizzando i MOOC mentre per chi ricopre incarichi specifici (insegnanti/istruttori militari, responsabili della didattica…), sono disponibili corsi di formazione ed aggiornamento che già contemplano l'uso dell'I.A. nella fase di apprendimento e nella generazione di corsi ad alto contenuto tecnologico. Contestualmente, si sta procedendo ad ammodernare le aule, rendendole parte integrante del processo di formazione, che come tutti sappiamo comprende l'ambiente formativo, composto dalle aule, dai docenti e dai discenti, oltre che dai contenuti. Per ognuno degli ambiti appena citati a partire dalle Scuole Militari, fino ai corsi post laurea, si fa uso dell'I.A., in ogni sua possibile declinazione, senza tralasciare gli aspetti umanistici che ci portano ad affrontare i temi della SOFIMATICA.

Cultura organizzativa: trasmettere ai giovani allievi (e al personale in servizio) la consapevolezza che la competenza tecnologica è ormai inscindibile dalla capacità operativa. "Come state facendo in modo che tutto il personale, dai giovanissimi ai veterani, conosca e utilizzi e l'uso dell'IA?"

Come anticipato precedentemente, l'ambiente formativo innovativo, prevede che tutto il personale sia compartecipe alla propria formazione, mediante uso degli strumenti tecnologici a disposizione e, prima ancora, dell'approccio all'innovazione che è condizione ineludibile per non essere lasciati indietro. La rapidità d'evoluzione

del contesto geopolitico è comparabile ad una immaginaria "linea del fronte ", in continuo movimento. Per non essere tagliati fuori, come in una campagna operativa, tutto il personale (dai più recentemente arruolati, a chi si approssima alla quiescenza), deve essere in grado di interagire (più o meno, a seconda del proprio ruolo) con l'I.A. che come abbiamo sentito è a disposizione, da un lato, mentre, dall'altro, può essere immaginata come un ponte che tutti devono attraversare per approdare ad un nuovo livello di conoscenze che permetteranno di ambientarsi nei nuovi scenari di riferimento. Il COMFORDOT promuove la diffusione di questa cultura mediante la divulgazione della conoscenza di base (alfabetizzazione) dell'I.A. per tutto il personale iscritto al PMFA[1] (poco meno di 80.000). Naturalmente, detta conoscenza delle discipline STEM, a seconda dei ruoli e dei livelli di studio viene opportunamente declinata dai programmi ministeriali delle Scuole Militari (arricchiti dai Campi digitali) e nei corsi universitari, che prevedono insegnamenti STEM anche per le discipline cosiddette umanistiche.

Dalla teoria all'impiego: Il valore delle competenze scientifiche non solo per i tecnici, ma come base culturale comune per tutte le Forze Armate. "Tra simulazione virtuale e addestramento reale: come l'Ambiente Addestrativo Globale permette di prepararsi a scenari complessi riducendo costi e impatto ambientale?"

Per ridurre il gap tra la teoria e l'effettivo impiego sul campo delle nozioni apprese, l'Esercito punta al conseguimento di un "Ambiente Addestrativo Globale Integrato", al contempo luogo fisico e spazio virtuale nel quale attivare, secondo necessità, le specifiche capacità degli ambienti reali e simulati, per creare eventi esercitativi complessi, realistici ed efficaci in termini di ritorno addestrativo. L'impiego delle tecnologie di simulazione addestrativa consente anche di contemperare le esigenze di contenimento dei costi e di tutela dell'ambiente con la limitata disponibilità nazionale di aree addestrative e poligoni idonei alla condotta di attività sempre più complesse, con sistemi d'arma sempre più performanti in termini di gittate e potenza di fuoco. Oltre a ricercare sinergie con nazioni alleate e partner per l'uso di aree addestrative anche al di fuori del territorio nazionale, l'Esercito ha provveduto a orientare importanti risorse al potenziamento dell'architettura di simulazione addestrativa già esistente negli ambienti live (persone reali - Staff e Unità- si confrontano in un ambiente reale: poligoni e aree addestrative), virtual (persone reali, armi e mezzi reali/virtuali in ambiente sintetico condiviso e constructive (Staff reali operano con sistemi reali di Comando e Controllo in ambiente sintetico).

[1] Il PMFA è il fulcro della formazione digitale, articolato in cinque aree sinergiche che si identificano in altrettanti 5 portali digitali: Formazione continua, (corsi di libero accesso), Supporto alla docenza (strumenti e materiali didattici per docenti), Corsi e-learning (corsi tutorati e gestiti), Formazione linguistica (corsi per l'apprendimento delle lingue), Dottrina e gestione della conoscenza (per la diffusione della cultura militare e mediateca). Infine un portale integrato, l'ei-portfolio, per promuovere pratiche innovative e condivisione di esperienze, favorendo la creazione di network dedicati. I portali sono attualmente allocati all'interno del Portale Multimediale della Difesa (ELD) ed a sistema con i Portali Interforze e di altre FF.AA.

Hi-Tech e insegnamento: "Quali sono le tecnologie che stanno davvero rivoluzionando il modo in cui i futuri ufficiali imparano il mestiere?"

Per quanto concerne gli strumenti cosiddetti Hi-Tech, si passa dai laboratori dei campi digitali, Hackathon digitali delle Scuole Militari ai moduli di insegnamento previsti nelle Università partner, che provvedono a fornire insegnamenti quali Intelligenza artificiale e apprendimento automatico, Advanced machine learning, Bioinformatics e tantissimi altri, tutti facenti parte del progetto Digital Education Hub. Gli insegnanti possono già usufruire dei software presenti sul Portale della Formazione[2], mediante

i quali sono e saranno sempre più in grado di erogare formazione tecnologicamente avanzata, al passo con gli sviluppi nel settore specifico.

Skill shortage: la doppia sfida della scuola: colmare il gap tra domanda e offerta di competenze, ma anche aggiornare costantemente i propri formatori rispetto a tecnologie e soluzioni in continua evoluzione. "Con il progetto SFIDA 2 entrano in campo gli avatar: come si trasforma il ruolo del docente quando la didattica diventa immersiva e assistita dall'IA?"

Con l'acquisizione di software di ultimissima generazione, l'Esercito si sta dotando di tool capaci di fornire supporto ai docenti, che saranno sempre più in grado di realizzare la necessaria "curvatura didattica" generando insegnamenti "tailorizzati" a studenti di età ed esperienze molto diverse, spaziando dalla pedagogia all'andragogia. Utilizzando l'AI quale strumento dialogico nell'intento di rendere immediatamente fruibili le nozioni, mentre ci si addestra all'impiego delle nuove tecnologie, i docenti, insieme con i loro avatar, saranno in grado di stabilire una relazione dialogica con i discenti, capace di realizzare appieno la didattica immersiva prevista dalla Formazione Digitale Integrata, che è parte integrante del progetto della Difesa denominato SFIDA 2 (Sistema di Formazione Integrata Digitale Avanzata),

[2] IA per la Didattica

L'IA viene applicata in diversi ambiti per il supporto ai docenti e agli istruttori:

- LMS Moodle-IA: (Learning Management System) su base software chiamato Moodle (acronimo di Modular Object-Oriented Dynamic Learning Environment) per l'erogazione dei corsi. All'interno possiamo avere il supporto I.A. per:
  - gestione automatizzata dei corsi e autogenerazione dei quiz (vista demo on-line all'interno di un corso di manovra del Corso di S.M.);
  - sistema antiplagio e proctoring avanzato per l'anti-copiatura;
  - assistente chatbot IA per il supporto all'interno dei corsi (vista demo on-line all'interno di un corso di manovra del Corso di S.M.).
- Tool di authoring: Uso di tool avanzati per la generazione di contenuti con ausilio di I.A. Applicativi software come Articulate 360 potenziato con I.A., permette la generazione di micro-elearning, lezioni e corsi e-learning in modo speditivo e automatico, a partire da contenuti come PDF o file di testo (vista la demo per creazione di un corso multimediale ed interattivo, immediatamente fruibile, a partire da un PDF in soli in 10 min), altri come iSpring permettono la generazione automatica di contenuti video a partire da una re-generation di Power Point, consentendo quindi anche la generazione di quiz e presentazioni interattive a partire dal contenuto.
- Generazione video/avatar: creazione di video personalizzati con l'ausilio di I.A. partendo da vari formati (PowerPoint, PDF, storyboard, prompt/URL), anche multilingua, con la possibilità di usare un AVATAR anche personalizzato, per generare video in modo veloce ed immediato con elai. (vista demo per creare un video con avatar a partire da una presentazione di storia militare in Power Point).
- Gestione licenze: processo strutturato per assegnazione delle licenze ai docenti, con metodologia circolare, a progetto ed a tempo.

i cui 4 key point sono:

- **Recommendation system:** suggerimento di corsi e contenuti in base alle competenze ed all'orientamento sull'incarico da ricoprire;
- **Active recall optimization:** ottimizzazione della retention delle conoscenze tramite contenuti mirati anche in base all'analisi dei feedback;
- **Chatbot:** supporto formativo e personalizzato adattabile sulle necessità comunicative del singolo;
- **Summarization:** sintesi di documenti complessi, creazione di pillole di contenuto, consultazione facilitata anche in mobilità.

Intervento del Comandante delle Scuole della Marina Militare Ammiraglio di Squadra Stefano BARBIERI

L'IA non è futuro: è già scenario operativo

Ammiraglio di Squadra
Stefano BARBIERI

Le nuove generazioni di militari considerano Intelligenza Artificiale e competenze STEM non come una prospettiva futura, ma come una realtà già operativa, indispensabile per la difesa del territorio, la sicurezza dei mari e dello spazio aereo.

Ho seguito con profondo interesse gli esercizi presentati dagli allievi delle Scuole militari, delle Scuole Sottufficiali e delle Accademie nel corso della mattinata. Nel complimentarmi con loro per il lavoro svolto, osservo con piacere che non si è trattato di semplici proiezioni teoriche, ma di riflessioni concrete e operative sull'impiego dell'Intelligenza Artificiale e delle competenze STEM per assolvere i compiti fondamentali delle Forze Armate. Nelle loro presentazioni abbiamo visto l'IA applicata alla difesa del territorio, alla gestione dello spazio aereo e alla sicurezza dei mari. Soluzioni differenti, sviluppate da punti di vista differenti, sulla base di conoscenze differenti, ma accomunate da un fatto evidente: i nostri allievi sono già pienamente consapevoli che la tecnologia, i dati e l'Intelligenza Artificiale sono parte integrante dello scenario operativo e che il loro peso è destinato a crescere in modo rapido e significativo. Quando si confrontano con questi temi i nostri allievi non pensano ad un futuro remoto ma ad una dimensione già presente che devono e vogliono imparare a comprendere e governare.

La vera sfida: integrare l'IA senza delegare la decisione

La formazione militare deve creare leader capaci di dialogare con la macchina, non di delegarle il comando: comprendere quando l'IA è utile, quando può sbagliare e quando non va seguita è una competenza strategica.
La formazione militare, nella sua storia, ha sempre saputo adattarsi alle grandi rivoluzioni tecnologiche. Ogni innovazione ha richiesto nuove conoscenze, nuove competenze e, di conseguenza, nuovi modelli formativi, pena il ribaltamento dei vantaggi acquisiti. Oggi ci troviamo di fronte a una trasformazione simile alle

precedenti, ma con caratteristiche peculiari. Le discipline STEM e l'Intelligenza Artificiale non rappresentano soltanto nuovi strumenti, ma un nuovo paradigma cognitivo: cambiano il modo di analizzare i problemi, di elaborare le informazioni, di supportare il processo decisionale.
In questo contesto, gli Istituti di Formazione militari si confrontano con molteplici sfide triplice trasversali a tutte le Forze Armate.
Una delle sfide principali è costituita dall'integrazione dell'IA nel processo decisionale. Dobbiamo formare leader capaci di dialogare con la macchina, non di delegarle la scelta. Nel nostro lavoro non possiamo permetterci la postilla a bordo schermo "l'Intelligenza Artificiale può sbagliare". Dobbiamo sapere quando e perché la tecnologia può sbagliare; dobbiamo sapere se impiegarla e come farlo.
L'impiego dell'Intelligenza Artificiale rappresenta infatti anche una sfida cognitiva. Come ci ricorda Daniel Kahneman, psicologo, studioso dei processi decisionali e Premio Nobel per l'Economia, la natura umana è predisposta ad accettare soluzioni semplici provenienti da fonti percepite come affidabili.
Formare all'uso corretto dell'Intelligenza Artificiale significa quindi insegnare non solo come usarla, ma anche quando non fidarsene, sviluppando consapevolezza, spirito critico e capacità di mettere in discussione la risposta "facile".
Questo è particolarmente rilevante in un contesto in cui molte tecnologie sono sviluppate e possedute in ambito privato, con logiche, tempi e obiettivi che non sempre coincidono con quelli della Difesa. La capacità di valutare, comprendere e governare questi strumenti diventa quindi un requisito strategico.

Tecnologia sì, ma con il fattore umano al centro

La sintesi tra formazione militare, STEM e IA è efficace solo se rafforza – e non indebolisce – il fattore umano: leadership, etica, giudizio e responsabilità restano insostituibili e sono il vero vantaggio competitivo delle Forze Armate.
La protezione del "fattore umano" è senza dubbio un'altra delle sfide che dobbiamo affrontare, forse ancora più delicata delle altre. Dobbiamo continuare a coltivare e rafforzare quelle qualità umane che nessun algoritmo potrà mai replicare: leadership, etica, capacità di giudizio, pensiero critico, iniziativa, spirito di corpo, coraggio morale.
Questi elementi restano il cuore della formazione militare e devono convivere armoniosamente con le competenze tecnologiche.
In questo quadro, l'introduzione dell'Intelligenza Artificiale nel processo didattico degli istituti militari trova un terreno particolarmente fertile. L'Intelligenza Artificiale consente di affrontare l'insegnamento delle hard skills da prospettive nuove ed efficienti, liberando spazio e risorse per concentrarsi sulle soft skills, come la leadership appunto, che da sempre sono al centro della formazione militare.
La variabile tempo: la formazione deve essere apripista
La rapidità dello sviluppo tecnologico non consente alla formazione militare

di attendere i feedback dal campo prima di innovare: è necessario anticipare il cambiamento, agire da front runner e adattare progressivamente i modelli formativi, perché il rischio di arrivare in ritardo è inaccettabile.

È di focale importanza riflettere sulle tempistiche dei processi in atto. Il modello tradizionale formazione prevede la valorizzazione dei feedback dal campo per orientare le modifiche e le integrazioni agli iter formativi. Nel campo dell'intelligenza artificiale e delle disruptive technologies in generale non possiamo adottare questo approccio.
La rapidità dello sviluppo tecnologico impone alla formazione militare di essere apripista, di agire da front runner, immaginando il futuro, introducendo innovazioni e adattandole progressivamente. Il rischio di essere in ritardo è semplicemente troppo alto.

Conclusione

Torno all'argomento del panel, "formazione militare, discipline STEM e IA: una sintesi compiuta?", per dare la mia risposta: la sintesi tra formazione militare e discipline STEM è un processo in divenire. Potremo confermarne l'efficacia se permetterà al nostro personale di non subire la tecnologia, ma di dominarla.
Ai nostri frequentatori chiedo di continuare a essere curiosi, di studiare con passione le discipline scientifiche, senza mai dimenticare che queste competenze sono al servizio del nostro Paese, della pace e della sicurezza comune.

Intervento del Comandante delle Scuole dell'Aeronautica Militare Generale di Squadra Aerea Francesco VESTITO

Generale di Squadra Aerea
Francesco VESTITO

Sono onorato di partecipare a questa Conferenza, importante occasione di confronto e approfondimento, che consente di sviluppare in modo coordinato, insieme alle altre Forze Armate, una riflessione condivisa su temi strategici per l'innovazione e per il futuro del Paese.

L'Aeronautica Militare sta proseguendo con determinazione nel percorso di sviluppo e integrazione delle discipline STEM in molteplici ambiti della propria attività. Basti pensare a quanto stiamo investendo nella ricerca, nella sperimentazione e nella formazione del personale, affinché l'IA diventi uno strumento affidabile a supporto delle decisioni, dell'addestramento, della manutenzione predittiva e della gestione dei sistemi complessi. È un impegno che portiamo avanti con visione, responsabilità e attenzione etica, consapevoli che l'innovazione tecnologica è un fattore strategico per la sicurezza del Paese e per la crescita delle competenze STEM delle nuove generazioni.

Sono rimasto profondamente affascinato dai temi su cui abbiamo lavorato nei mesi precedenti e dall'elevato livello dei lavori realizzati dagli allievi degli Istituti di Formazione e Scuole Militari nell'ambito delle discipline STEM, che testimoniano un impegno, una preparazione e una maturità intellettuale di assoluto rilievo.

Nello specifico, ho trovato particolarmente interessante lo scenario di "emergenza epidemiologica", che ho potuto seguire direttamente in quanto coordinato dagli Allievi della Scuola Marescialli dell'AM, che ci mette di fronte ad un tema molto importante e che può essere oggetto di future ricerche e discussioni: "la qualità dei dati e la sovranità informativa".

l'IA è tanto affidabile quanto i dati che la alimentano. Il rischio non è solo tecnico, ma strategico. Se i dati non sono controllati, verificati o pienamente accessibili, si crea dipendenza da attori esterni e si perde capacità decisionale autonoma. In ambito Difesa questo è particolarmente sensibile, perché la qualità del dato diventa un fattore di sicurezza nazionale.

L'uso della tecnologia ed in particolare l'AI può analizzare pattern, prevedere scenari, ottimizzare processi, ma non possiede intenzionalità, valori o responsabilità morale. Complementarietà non sostituzione! Il rischio non è che l'IA "decida", ma che gli

umani smettano di decidere, rifugiandosi nell'autorità dell'algoritmo. È un rischio culturale prima ancora che tecnologico.
Bisogna mantenere comprensibile l'importanza del processo decisionale, spiegarne i criteri e mantenere chiara la responsabilità umana.
L'uso della tecnologia e dell'IA può potenziare enormemente le capacità decisionali, ma solo se rimane uno strumento nelle mani di persone formate, consapevoli e responsabili…. E con questo spirito, confermo l'impegno dell'Aeronautica Militare a proseguire con determinazione in questo percorso di innovazione e responsabilità!
Sono ora disponibile per affrontare i temi che mi sono stati anticipati.

Dalla teoria all'impiego: Il valore delle competenze scientifiche non solo per i tecnici, ma come base culturale comune per tutte le Forze Armate.

Le discipline STEM, o STEAM senza mai dimenticare l'importanza della A di Art, rappresentano i pilastri su cui si basano la ricerca scientifica, l'innovazione industriale, lo sviluppo di nuove tecnologie, la sicurezza e la difesa e la competitività di un Paese. Sono discipline che formano competenze critiche per affrontare sfide come l'Intelligenza Artificiale, la robotica, la cyber-sicurezza, l'aerospazio, l'energia e molto altro.
In seno alla nostra Forza Armata le STEM sono oramai centrali per la progettazione e gestione dei sistemi aeronautici, l'addestramento avanzato, la manutenzione predittiva, l'analisi dei dati operativi, lo sviluppo di tecnologie emergenti come l'IA e autonomia dei sistemi.
Dallo scorso anno 2025, l'Aeronautica Militare ha costituito una "Board" strategica tra personale esperto degli Alti Comandi necessaria a definire una visione strutturata e condivisa in ambito Interforze sulle discipline STEM e in particolare sull'IA. E' necessario definire percorsi operativi, attribuire responsabilità e identificare KPI (Key Performance Indicators) per monitorare in modo efficace l'avanzamento delle attività. Nella "Board" ogni partecipante è chiamato a incanalare le competenze specifiche della propria organizzazione, mettendole a sistema a beneficio del lavoro comune.

Hi-Tech e insegnamento: qual è l'impatto delle nuove tecnologie sulla formazione delle nuove leve? Quali vengono più utilizzate e qual è il ruolo dell'AI.

Nell'ambito della Formazione è necessario analizzare l'impatto dell'innovazione su formazione, addestramento e apprendimento continuo attraverso le tre direttrici principali:
Formazione all'IA: sviluppare competenze trasversali, valutando di inserire tali competenze come parte integrante della preparazione militare di base;
Formazione operativa: addestrare il personale all'uso pratico di sistemi IA, preparando scenari realistici e abilitando l'efficacia sul campo;
Evoluzione della didattica: stimolare l'apprendimento attraverso metodologie nuove,

ad esempio con attività di ricerca autonoma, interrogando l'IA.
L'innovazione tecnologica consente di ottimizzare i processi decisionali e migliorare l'efficacia operativa, garantendo anche interoperabilità avanzata nei domini operativi. Dai velivoli di quarta generazione siamo passati alle piattaforme di quinta, come il Joint Strike Fighter F-35, e già guardiamo oltre, verso il Global Combat Air Program (GCAP): un sistema di sesta generazione, non più solo un velivolo, ma una piattaforma aerospaziale integrata, capace di gestire sciami di droni, intelligenza artificiale, big data e operazioni in ambiente multi-dominio. In tale ambito guardiamo con attenzione anche al progetto innovativo internazionale FITS4TOP (Future Integrated Training System for TOP Pilots), sviluppato dalla Leonardo e cofinanziato dall'Unione Europea, nato per potenziare le attuali capacità Live,Virtual and Costructive del syllabus addestrativo dei piloti militari, attraverso un "sistema di sistemi" che sfrutta hardware e software avanzati, intelligenza artificiale, realtà aumentata. FITS4TOP si configura come un ambiente addestrativo estremamente digitalizzato, supportato da capacità di supercalcolo e cyber-resilience in cui l'allievo si addestra in volo, fronteggiando eventuali minacce aeree, marittime e terrestri. Tuttavia queste tecnologie dirompenti ampliano le nostre capacità operative, ma al tempo stesso richiedono personale dotato di formazione avanzata, flessibile e multidisciplinare. Perché, nonostante il progresso, l'elemento umano resta il pilastro fondamentale di ogni operazione militare: la tecnologia è un moltiplicatore, ma la vera forza risiede nelle persone. Questo aspetto è talmente importante che la nostra attenzione si rivolge non solo alle giovani leve ma anche a tutta la restante parte del personale in servizio nella FA. Infatti, a titolo esemplificativo ma non esaustivo mi sia permesso di citare l'iniziativa che da qualche mese abbiamo intrapreso presso l'ISMA di Firenze in tema di Innovazione Digitale rivolta alla componente dirigenziale dell'AM attraverso un programma di "cross contamination", tra le grandi aziende del settore, l'Ambiente Accademico e la Forza Armata.

Skill shortage: la doppia sfida della scuola: colmare il gap tra domanda e offerta di competenze, ma anche aggiornare costantemente i propri formatori rispetto a tecnologie e soluzioni in continua evoluzione.

Questa è una riflessione centrata! Parliamo giustamente di skill shortage come di una doppia sfida. E' necessario:

- colmare il divario tra domanda e offerta di competenze. Le imprese, le amministrazioni e le Forze Armate chiedono profili tecnici sempre più avanzati, mentre la scuola fatica a produrli con continuità. Questo mismatch non è episodico: è strutturale;
- aggiornare costantemente i formatori. È il punto più critico. Le tecnologie evolvono più velocemente dei programmi scolastici e, spesso, più velocemente delle competenze di chi dovrebbe insegnarle. Se i docenti non vengono messi nelle condizioni di aggiornarsi, il sistema si blocca a monte.

Questa doppia sfida diventa anche più complessa perchè:

- le tecnologie emergenti (IA, robotica, cybersecurity, data science) cambiano ogni 6–12 mesi e la scuola (così come gli Istituti di Formazione), invece, ha cicli di aggiornamento molto più lenti;
- le aziende e le istituzioni chiedono competenze che spesso non esistono ancora nei percorsi formativi tradizionali;
- i docenti non possono essere lasciati soli: serve formazione continua, risorse, tempo e un ecosistema che li sostenga.

Se l'obiettivo della Difesa Italiana è quello di garantire una preparazione strategica, al passo con le sfide emergenti, il rinnovamento della formazione procede inevitabilmente con un adeguamento alle evoluzioni culturali e tecnologiche, consolidando percorsi dedicati alle operazioni multi-dominio ed interforze.

Intervista al Vice Comandante Generale e Comandante delle Scuole dell'Arma dei Carabinieri Generale di Corpo d'Armata Marco MINICUCCI

Generale di Corpo d'Armata
Marco MINICUCCI

Cosa diventerà il Carabiniere nell'era dell'AI, nell'era delle tecnologie? Cambierà in qualche modo, c'è qualcosa che trasformerà l'idea di Carabiniere?

Innanzitutto desidero portare il saluto del Comandante Generale dell'Arma dei Carabinieri, Generale di Corpo d'Armata Salvatore Luongo, e ringraziare il Sottosegretario alla Difesa, Sen. Isabella Rauti, per l'opportunità offerta con questo evento.

Abbiamo oggi ascoltato degli Allievi delle Scuole Militari, delle Scuole Sottufficiali, delle Accademie e sono rimasto impressionato, quasi stupito, da un particolare: nel parlare oggi dell' Intelligenza Artificiale, questi ragazzi sono stati capaci, attraverso la loro esposizione - frutto non di Intelligenza Artificiale, ma della loro passione e delle loro motivazioni - di trasferirci di fatto il significato vero del concetto di risorsa umana, che esprime un valore insostituibile in ogni epoca della storia dell'umanità e lo sarà anche per il futuro. Ci hanno esposto i loro progetti sui quali hanno studiato e si sono impegnati - spesso da soli e/o con l'aiuto dei superiori gerarchici - con una capacità che mi ha non solo stupito, come detto, ma anche entusiasmato e per la quale meritano i complimenti da parte di tutti quanti noi. Hanno accettato la sfida di interfacciarsi con l'Intelligenza Artificiale, approfondendo le ricadute conseguenti al suo utilizzo e alla diffusione nel nostro tessuto sociale, offrendo a tutti noi un risultato di assoluto interesse speculativo: l'Intelligenza Artificiale sa cosa fa, ma il perché lo fa lo sa l'uomo, la risorsa umana che c'è dietro e gli Allievi ce lo hanno dimostrato in maniera chiara.

Fatta questa doverosa premessa, veniamo ora più direttamente al tema della domanda. L'Arma dei Carabinieri vede nell'Intelligenza Artificiale un'opportunità che ovviamente non può sostituire il Carabiniere, che su strada garantisce e garantirà sempre la sicurezza in favore del cittadino, soprattutto quella sicurezza "percepita", fatta di prossimità, di contatto umano - che nessuna macchina può surrogare - di attenzione e capacità di risposta alle esigenze e alle richieste per piccoli e grandi problemi dei cittadini. Ci può però aiutare. Quindi è il mezzo, senza sentimenti o emozioni, ma che ci dà la possibilità, anche sul piano temporale, di ottimizzare procedure ovvero di offrire soluzioni più performanti per venire incontro alle

esigenze dei cittadini.
Ad esempio, la tecnologia digitale consentirà di avvalersi di modalità di presentazione di una denuncia ancora più efficienti e, quindi, di ridurre notevolmente i tempi di attesa, che spesso caratterizzano tanto la prenotazione di un esame clinico quanto la verbalizzazione di una denuncia. Parimenti, migliorerà la capacità investigativa in relazione alle diverse e particolari tipologie di scenari in cui potrà imbattersi la pattuglia intervenuta. Il Carabiniere conserverà l'attitudine al contatto fisico con il cittadino, non può affidare totalmente all'Intelligenza Artificiale l'interlocuzione con il malcapitato per stilare una denuncia, perché il contatto umano è fondamentale, perché è fondamentale comprendere i sentimenti, i timori, gli stati d'animo dei cittadini che stanno denunciando, guardandoli negli occhi. Ma l'Intelligenza Artificiale, in questo momento, è un'opportunità epocale da cavalcare per migliorare tutti i processi di lavoro e, quindi, avere la possibilità di mettere sul territorio molti più Carabinieri a fronte di quanti oggi, all'interno delle caserme, sono invece gravati da altrettanto indispensabili attività burocratiche, che i sistemi di I.A. potranno svolgere al loro posto.
Questa è la visione operativa, su come sarà il ruolo del Carabiniere, ma poi come si traduce nella formazione?
Che cosa deve cambiare ovvero qualcosa è cambiato?
Necessariamente, sta cambiando. Innanzitutto ci siamo resi conto che la formazione deve assumere una veste molto più pratica che teorica. Al riguardo, le nuove Linee Programmatiche per l'Arma dei Carabinieri[1] si coniugano esattamente con quelle strategiche illustrate dal Ministro dell'Istruzione e del Merito, prof. Giuseppe Valditara.
Nelle nostre Scuole le materie tecnico-professionali sono state sin qui oggetto di una metodica didattica impostata su di un approccio prevalentemente teorico. Stiamo cambiando il paradigma, stiamo incominciando a fare in modo che, ad esempio, attività come il sopralluogo su una scena del crimine sia insegnamento pratico e contestualmente anche teorico, facendo discendere dall'attività pratica tutto ciò che di nozionistico devono sapere il Carabiniere, il Sottufficiale dei Carabinieri, l'Ufficiale: dopo le Scuole, giunti a destinazione, ognuno con il proprio ruolo, devono essere da

[1] Le nuove Linee Programmatiche contemplano:
a. una formazione nell'Arma intesa come strumento in adattamento continuo e di tipo integrato e multidisciplinare, capace di abbracciare le dimensioni operativa, tecnico-militare, geopolitica, economica, giuridica e comunicativa, in cui il Carabiniere andrà ad esplicare la sua azione;
b. la ridefinizione dei relativi core curricula formativi di base, per tutti i ruoli, anche attraverso il confronto interforze, internazionale e la conoscenza dei modelli organizzativi civili più moderni (partnership con istituti accademici e agenzie di law enforcement internazionali), nonché ispirandoli ad una nuova policy di formazione del personale, orientata all'integrazione, allo sviluppo di competenze specifiche di dominio e alla capacità di comprendere, e quindi influenzare, l'ambiente multidominio;
c. per i momenti della formazione avanzata, focus di integrazione interforze e moduli formativi dedicati alle competenze cross-domain per la gestione di scenari operativi complessi (proprio con questo spirito ed "approccio interforze", sono stati già disposti addestramenti specifici nell'ambito di attività congiunte con il COMFOTER dell'E.I.);
d. l'obiettivo di migliorare il livello specialistico della formazione e l'efficacia delle simulazioni di addestramento e delle operazioni sul campo mediante l'utilizzo di sistemi di Intelligenza Artificiale e della realtà aumentata.

subito produttivi.
Abbiamo pensato che la migliore risposta alla domanda "Che cosa vuoi dal Carabiniere che ti assegniamo dal giorno dopo in cui è arrivato al tuo comando?" potesse arrivarci soprattutto da coloro che impiegano il Carabiniere sul territorio. È stato condotto un brainstorming, formulando domande e raccogliendo le risposte, le abbiamo esaminate utilizzando NotebookLM (un sistema avanzato di assistenza[2], che - a differenza di ChatGPT - non si alimenta con informazioni e dati dal web, ma va ad analizzare e sintetizzare solo il patrimonio informativo reso disponibile dall'utente). Da quelle risposte fornite dai Comandanti di Stazione, siamo così addivenuti all'individuazione di programmi didattici e skills, che stiamo definendo per formare il Carabiniere del futuro, che sappia utilizzare con scioltezza e sicurezza le nuove procedure, attraverso sistemi e applicativi evoluti che troverà installati sulle apparecchiature in dotazione alle Stazioni e sulle autoradio. E quindi il nuovo paradigma è un'attività formativa molto più aperta alle esperienze pratiche, al training on the job. Attività questa che abbiamo già applicato alla Scuola Marescialli e alla Scuola Ufficiali, dove i nostri Marescialli e i nostri Ufficiali, ancora discenti, sono aggregati per un un anno sul territorio, per imparare praticamente ciò che devono fare.
L' utilizzo dell'Intelligenza Artificiale all'interno delle Scuole ovviamente modificherà e/o implementerà anche sistemi e materie di insegnamento[3].
Il cyber and digital training istituzionale assicurerà un'intensa attività di:

- formazione di base attraverso insegnamenti, differenziati tra loro e con diversi gradi di approfondimento in relazione al percorso formativo intrapreso, nell'ambito:
  - delle discipline informatiche (informatica d'arma, cyber security e indagini digitali; geopolitica e cyberspazio, sicurezza strategica, multidominio e internet of things);
  - della cattedra di Etica, leadership e comunicazione, con simulazioni relazionali sviluppate utilizzando l'intelligenza artificiale;
- formazione successiva, fatta di corsi di specializzazione, di aggiornamento e di alta formazione che accompagnano la vita dei carabinieri lungo tutto il loro servizio attivo.

[2] Funziona con il modello linguistico Gemini e genera riassunti, guide di studio, mappe mentali, sintesi audio e risponde a domande specifiche, trasformando documenti o appunti in uno strumento di studio (e lavoro) molto più potente. Il suo utilizzo è previsto per tutti i Carabinieri, attraverso l'accesso alla piattaforma "Google Workspace", che offre soluzioni innovative per dare ausilio sia alla formazione (sia al lavoro), garantendo elevati standard di sicurezza, usabilità e performance.
[3] Di fondamentale importanza sarà la nuova formazione specialistica ed il successivo aggiornamento nel settore cyber a cura dell'Istituto Superiore di Tecniche Investigative, per il personale già in possesso di specifici titoli di studio STEM e/o dotato di particolare predisposizione, di cui dovranno dotarsi le componenti investigative dell'Organizzazione territoriale e speciale. Parimenti, avuto riguardo all'uso di tecniche inferenziali di Intelligenza Artificiale e di quantum computing, è stato disposto un approfondimento per la creazione di specifici percorsi formativi condivisi con il mondo della ricerca universitaria e scientifica e le altre articolazioni della Difesa, nonché di scambi professionali con aziende nazionali anche collegate alla Difesa. Sempre nell'ottica di sfruttare le potenzialità offerte dall'uso dell'Intelligenza Artificiale e della realtà aumentata e di ampliare a tale scopo l'attività di scouting all'interno dell'Istituzione, è prevista anche la possibilità di competizioni cyber negli Istituti di formazione.

Tutto questo è molto interessante, in inglese lo definiremmo anche learning by doing. Può farci ora qualche esempio di come applicate le nuove tecnologie o insegnate ad applicare le nuove tecnologie per indagare, ad esempio, in materia di protezione dell'ambiente oppure dei beni culturali.

Iniziamo dalla protezione dell'ambiente. Occorre premettere che, nel 2017[4], l'Arma dei Carabinieri ha assorbito il Corpo Forestale dello Stato e, quindi, si è preliminarmente resa necessaria un'intensa attività di riorganizzazione dell'Istituzione, per accogliere professionisti di grande livello, che ci hanno arricchito di capacità e preparazione specialistica importantissime.

Il Comando Unità Forestali, Ambientali e Agroalimentari dell'Arma dei Carabinieri, in particolare, sta sovrintendendo alla progettazione esecutiva di un sistema di addestramento immersivo (FFAS 2 – Forest Fire Area Simulator Evolution 2), presso il Centro di Addestramento di Castel Volturno (CE), basato su tecniche di AI generativa a supporto della formazione integrata in favore dei frequentatori dei corsi di specialità forestale, con il quale viene fornito un addestramento 3D, improntato anche sul coinvolgimento emotivo delle esperienze multisensoriali, che possono verificarsi in contesti critici simulati (Serious Games) come ad esempio in tema di incendi boschivi: i Carabinieri non spengono gli incendi, ma indagano per capirne le cause e individuare il punto di innesco, dunque il punto di partenza è importantissimo[5].

Per quanto attiene alla tutela del patrimonio culturale, è un ambito di specializzazione dell'Arma, che gode da tempo di un indiscusso riconoscimento a livello internazionale. Per l'alta professionalità dei Carabinieri nel settore, l'Italia è citata in gran parte del mondo e richiesta dalle Organizzazioni Internazionali per attività formative e sul campo[6]. Il sistema che viene utilizzato dai Carabinieri del Comando Tutela Patrimonio Culturale è stato più volte premiato e denominato Stolen Works of Art Detection System (S.W.O.A.D.S.) e serve a scandagliare il web, a individuare le opere d'arte che possono assomigliare a quelle che sono state trafugate, quindi denunciate. Ma anche qui, se non c'è la risorsa umana, se non c'è il Carabiniere esperto, non si riuscirà mai a fare il match tra ciò che mi restituisce il web e l'opera d'arte veramente rubata.

---

[4] Il D.Lgs. 19 agosto 2016, n. 177 ha razionalizzato le funzioni di polizia, disponendo l'assorbimento del Corpo Forestale dello Stato nell'Arma dei Carabinieri. Per l'effetto, personale, mezzi e competenze sono stati acquisiti in gran parte dall'Arma dei Carabinieri, a partire dal 1° gennaio 2017.

[5] Il sistema sarà, altresì, utile per formazione in materia di dissesto idrogeologico e valutazione stato fitosanitario di specie di interesse forestale.

[6] A seguito della proposta che il Ministro Franceschini ha lanciato a "EXPO-2015" nel corso della Conferenza internazionale dei Ministri della Cultura tenutasi il 31 luglio 2015, che ha coinvolto 80 Paesi e che si è conclusa con una dichiarazione di condanna della violenza contro il patrimonio culturale mondiale, il Comando Generale dell'Arma dei Carabinieri il 17 ottobre 2015 ha istituito la Task Force Carabinieri "Unite4Heritage", i "Caschi blu della cultura". Alla luce delle precedenti esperienze svolte in aree di crisi (2002-2003 Kosovo e 2003-2006 Iraq), per competenza in materia e in forza del ruolo riconosciuto al Comando, a livello internazionale, per le attività di recupero effettuate anche in favore dei Paesi esteri, il Comando Carabinieri Tutela Patrimonio Culturale è stato individuato per costituire la componente Carabinieri della suddetta Task Force italiana, che è stata formalmente istituita il 6 febbraio 2016 con la sottoscrizione dell'accordo tra l'Unesco ed il Governo italiano. La Task Force Carabinieri è un'unità in grado di svolgere, sia sul territorio nazionale, sia in ambito internazionale, interventi a tutela del patrimonio culturale, in caso di calamità naturali, conflitti armati o crisi internazionali. Il dispositivo opera ad integrazione del Team nazionale di esperti selezionati dal Ministero della Cultura (Mic), specialisti nei settori dell'archeologia, della storia dell'arte, e del restauro.

Ma c'è anche un altro fronte investigativo di assoluta attualità, sorto a seguito del rapido diffondersi, a livello globale, delle transazioni digitali per il trasferimento di valori monetizzabili: mi riferisco alle criptovalute, le cd. monete digitali, ritenute uno dei principali strumenti di riciclaggio e di abusivismo finanziario, che vedono l'Arma impegnata sia sul piano operativo sia su quello formativo del proprio personale. Per rispondere a questa nuova sfida di criminalità informatica (nella quale confluiscono, oltre ai crimini legati alle criptovalute, anche la vendita di valute contraffatte, dati relativi a carte di pagamento o documenti d'identità, le truffe e frodi sul web e dark web), è stata istituita nel 2021 una Sezione specializzata del Comando Antifalsificazione Monetaria, team investigativo di eccellenza nel campo: questa Unità utilizza tecnologie e software avanzati per analizzare la blockchain e deanonimizzare i wallet; i "tecno-carabinieri" tracciano così le transazioni, sequestrano asset digitali e convertono valute virtuali confiscate in euro.

Tale expertise viene altresì valorizzata, attraverso il supporto specialistico in campo nazionale, in favore dei Comandi territoriali dell'Arma e dell'Autorità Giudiziaria, e, sul piano formativo, con sessioni didattiche e divulgative nei corsi di tecniche investigative per il personale, seminari e convegni, anche di respiro internazionale, condividendo il patrimonio di conoscenze ed esperienze con le Istituzioni comunitarie, nonché con gli omologhi organismi delle Forze di Polizia straniere[7].

[7] Meritano, infine, di essere menzionati i tools di A.I. realizzati per le investigazioni scientifiche. Il Raggruppamento Carabinieri Investigazioni Scientifiche (RaCIS) ha aderito, quale partner, al proposal progettuale "Horizon" denominato DETECTOR, finanziato dalla Commissione Europea e coordinato dall'Ente di ricerca ellenico CERTH, al quale partecipano complessivi 13 partner europei, che si pone come obiettivo lo sviluppo di tools AI opportunatamente addestrati per la rilevazione di deepfakes audio e video nel web. Ancora, con il progetto NARCOSIS (Non-tArgeted foRensic multidisCiplinary platfOrm for inveStigatIon of drug-related fatalitieS), sempre finanziato dalla Commissione Europea e al quale partecipano 18 Partner europei, si sta sviluppando un tool, basato su sistemi di Intelligenza Artificiale e condiviso a livello europeo, in grado di classificare, ricercare e interpretare i dati analitici grezzi (spettri Raman, di Massa, NMR, etc.) relativi alle nuove sostanze ad azione psicoattiva e ai loro precursori.

Intervista del Presidente del Centro Alti Studi Difesa Scuola Superiore a Ordinamento Universitario Generale di Corpo d'Armata Stefano MANNINO

Generale Mannino, lei è qui in qualità di Presidente del Centro Alti Studi Difesa, voi vi dedicate all'alta formazione, sia per i militari che per i civili, cioè formate dirigenti in tutti i contesti. Quindi formate anche i decisori, che devono essere in grado di comprendere e gestire una complessità crescente, nel senso di capire quali sono i trend geopolitici, quale è la direzione dell'evoluzione di determinate tendenze che hanno un impatto per la sicurezza e poi trasformarle in raccomandazioni a disposizione di chi deve effettuare scelte strategiche. Non deve essere facile, mi perdoni. Ci racconti quali sono le sfide che deve quotidianamente affrontare.

Generale di Corpo d'Armata
Stefano MANNINO

Grazie. Innanzitutto, buon pomeriggio a tutti. Rubo due minuti alla mia risposta per unirmi anch'io ai saluti e ringraziamenti ai giovani frequentatori di tutti gli Istituti e Scuole di Formazione delle Forze Armate, presenti o collegati in streaming. Oggi, in maniera plastica, hanno dimostrato che la famosa "resistenza al cambiamento", di cui si è parlato in maniera approfondita nel corso di questa mattinata, non riguarda loro bensì le generazioni a noi più vicine. Nella realtà, infatti, il problema del ritardo nell'adozione delle cd. "tecnologie emergenti e dirompenti", tra cui l'Intelligenza Artificiale è probabilmente la più nota ma non l'unica, è dovuto a una resistenza di ordine culturale delle generazioni più datate, non particolarmente inclini alla rapida innovazione tecnologica che contraddistingue il nostro tempo. Siamo pertanto noi, la classe anagrafica più matura, che deve fare lo sforzo maggiore per comprendere le sfide e le opportunità del nuovo contesto, in cui siamo chiamati a gestire scenari dove le tecnologie dirompenti ed emergenti rappresentano al tempo stesso un catalizzatore dell'innovazione tecnologica e un acceleratore della complessità sistemica.
In questo ambito, permettetemi di condividere con voi la mia oramai ultradecennale esperienza nel campo della formazione militare, prima come Comandante dell'Accademia Militare di Modena, poi della Scuola Ufficiali dell'Esercito di Torino e ora dell'Istituto di alta formazione interforze, il CASD, che si colloca al vertice dell'ideale struttura a piramide della formazione militare nazionale. La mia esperienza mi dice che i nostri frequentatori, di ogni ordine e grado, ovvero le generazioni che si sono

succedute nel tempo, sono naturalmente predisposte a recepire le nuove tecnologie, e quindi potenzialmente già pronte a giocare un ruolo attivo in questo mondo sempre più digitalizzato. Sta pertanto solamente a noi decisori trarne le dovute conseguenze, per capire come poter accelerare i processi di inserimento dell'innovazione tecnologica ad alto contenuto digitale all'interno di un'organizzazione complessa quale quella militare. Confesso che incontri quali quello odierno, giunto oramai alla sua terza edizione, offrono un'occasione di confronto, aggiornamento, apprendimento e di stimolo unica. Inoltre, non è da nascondere il fatto che, finalmente, dopo anni di incontri tematici tenuti sulla verticale delle singole Forze Armate, oggi sono presenti Ufficiali che vestono divise con cinque colori diversi, a significare che la connotazione interforze è oramai un dato acquisito nel percorso di integrazione e sviluppo dello Strumento Militare.
Ciò detto, qual'è il messaggio che deve passare oggi, soprattutto ai giovani? Che le sfide che abbiamo di fronte, non solo quelle di natura tecnologica ma anche e soprattutto quelle a connotazione geopolitica, sono sfide sistemiche a complessità crescente. Viviamo in contesti estremamente fluidi, imprevedibili, irrazionali, instabili, mutevoli, pericolosi, appunto scenari a complessità crescente, che esporranno i nostri ora giovani frequentatori ma un domani futuri comandanti e quindi decisori, a problematiche straordinariamente impattanti per il Paese. Bene, per arrivare preparati a quel momento, sono necessari conoscenza, competenza e lavoro di squadra. Oggi, in questa sala conferenze, è proprio rappresentato un esempio di quello che possiamo definire "Sistema Paese", a dimostrazione che unendo le migliori energie, i migliori talenti e adottando lungimiranti, condivise e complementari politiche d'innovazione si può arrivare all'obiettivo. Il potenziale umano, che è quello oggi di fronte a noi, c'è ed è pronto a giocare la propria parte.

Presidente, il Centro Alti Studi Difesa, il CASD, che cos'è per chi non lo conosce?

Usando le parole pocanzi utilizzate da Paolo Benanti, possiamo dire che il CASD è la palestra cognitiva della Difesa e del Sistema Paese; la palestra, cioè, dove si preparano i dirigenti a gestire la complessità dell'oggi ma con uno sguardo al futuro. Una complessità, come dicevo prima, in crescendo, perché il mondo intorno a noi cambia e cambia velocemente. Come lo facciamo? Con un approccio cd. di "open innovation", cioè aperto alla contaminazione reciproca tra ecosistemi diversi, nazionali e internazionali: Difesa, Istituzioni, Industria, Università e Centri di ricerca, media, società. Significativi sono i numeri: in questo anno accademico, oltre ai frequentatori militari nazionali sono presenti colleghi provenienti da ben 51 Paesi alleati e amici, mentre più di un terzo del totale generale è rappresentato da studenti provenienti dal mondo civile.

Generale Mannino, in concreto, cosa si insegna al Centro Alti Studi Difesa?

La missione del CASD è quella di svolgere corsi post-laurea nell'ambito dell'alta formazione della classe dirigente militare, anche se comunque aperta al mondo civile; per la componente militare, è destinata a Ufficiali nei gradi da Maggiore fino a Generale (o gradi equipollenti). L'insegnamento è multidisciplinare per sua natura e fonde conoscenze/competenze tecnico-professionali (hard skills) con quelle trasversali (leadership e soft skills), incentivando il lavoro di gruppo e focalizzando l'attenzione sul livello strategico.
Inoltre, essendo una Scuola Superiore Universitaria, il CASD si dedica anche alla Ricerca di natura accademica, in particolare negli ambiti della Cyber Security, delle Relazioni Internazionali e Geopolitica, delle Scienze dell'Organizzazione e degli Studi Giuridico-Legali.
Per quanto riguarda le discipline STEM, il CASD si occupa dell'impatto che le tecnologie dirompenti ed emergenti - in particolare Intelligenza Artificiale, Big Data e Quantum – hanno sulla sicurezza e difesa nazionali.
Oltre agli impatti di natura capacitiva delle citate tecnologie, il CASD si occupa anche delle conseguenze del loro utilizzo quale straordinario strumento di natura geopolitica. Studiamo, infatti, quello che le stesse stanno presentando quale "conto da pagare", cioè il risvolto negativo della medaglia del progresso e dell'innovazione. Mi riferisco alle minacce, e relativi potenziali rischi, portati alla sicurezza nazionale. Come noto, la sicurezza nazionale viene declinata come tutto ciò che può, attraverso minacce dirette o indirette, intaccare l'integrità, l'indipendenza e la sovranità di un Paese. In questo contesto si inserisce la spinta competizione geopolitica in atto per il controllo delle tecnologie emergenti. Gli unici attori statuali internazionali che oggi sono in grado di controllare la cd. "triade digitale", Stati Uniti e Cina, cioè coloro i quali detengono il controllo contestuale dell'hardware/software, dei dati/big-data e delle infrastrutture fisiche/virtuali per il trasporto dei flussi di informazione, si stanno confrontando in una spinta competizione strategica per il controllo delle tecnologie di frontiera e delle relative supply chains (terre/minerali rari), in una partita geopolitica che sta ridisegnando architetture di sicurezza e alleanze economiche secondo una rinnovata spinta alla polarizzazione.
Per capire i pericoli per la nostra sicurezza e le nostre società, vorrei riportare qualche dato statistico che rende l'idea della magnitudo del problema in esame. I tecnici ci dicono che al 31 dicembre 2025 nel cd. Internet-of-think sono stati scambiati 175 Zeta-Byte (Z-Byte) di dati di varia natura (email, immagini, sms, etc.). Lo Z-Byte è l'unità di misura dei big-data, dove 1 Z-Byte è pari a un sestilione di Giga-Byte, cioè un 1 seguito da 21 zeri; un dato in continua crescita esponenziale. Questi 175 Z-Byte sono stati scambiati da circa 56 Miliardi devices digitali (cellulari, iPad, PC, etc.), utilizzati da circa il 67% della popolazione mondiale, dove ogni singolo utente è al tempo stesso produttore e consumatore di dati, senza nessun controllo da parte degli Stati. In sintesi, chiunque ha potenzialmente libero acceso a questi

175 Z-Byte e può, in maniera inconsapevole, essere manipolato attraverso attività di disinformazione. Tutto questo ha a che fare con un potenziale controllo della società che è estremamente pericoloso perché chi controlla i dati, le reti virtuali/fisiche e i flussi, ha la capacità di modificare la percezione del reale. Ecco quindi che quando parliamo di "guerra cognitiva" ci si riferisce a questi potenziali pericoli portati alla società e, quindi, alla sicurezza nazionale. Al CASD, studiamo e analizziamo tutto questo, per fornire ai futuri dirigenti gli strumenti di comprensione e competenza oramai indispensabili per affrontare queste tematiche in maniera consapevole e professionale. Quello che facciamo al CAS è sostanzialmente cercare di portare all'attenzione dei nostri frequentatori gli eventi e/o i fenomeni che entrano in gioco in questa partita complessa e pericolosa.

Mi scusi, solo per riportarla a quello che lei fa quotidianamente e per chiudere il suo intervento, tutto questo poi va, come posso dire, a pesare e a trasformare il concetto stesso di leadership, perché il leader è colui che è in grado di muoversi in un contesto così complesso, raccogliere informazioni, compiere scelte, identificare gli strumenti utili per farlo. Insomma, quando vuoi creare nuove competenze e nuove figure di leader, bisogna partite dal contesto geopolitico per poi arrivare al percorso di formazione.

Esattamente, ha usato la parola giusta: geopolitica. La geopolitica oggi si sta trasformando, si sta spostando da una geopolitica fisica, quella classica legata al territorio, verso una geopolitica del digitale, che è esattamente quello di cui abbiamo appena discusso. La geopolitica del digitale ci dice che il futuro sarà incentrato sull'accesso/controllo delle informazioni, del controllo/diniego delle risorse energetiche, perché per far operare le tecnologie digitali, ora e sempre più nel futuro, servirà energia, tanta energia che, di contro, sarà sempre meno disponibile. In conclusione, non è lontano lo scenario in cui i prossimi conflitti saranno scatenati esattamente per l'accesso/diniego alle risorse energetiche.
Concludo con una raccomandazione per i nostri giovani frequentatori: non vi fermate alle apparenze, siate curiosi, cercate sempre di leggere tra le righe degli avvenimenti… nulla succede per caso…e ricordate che la formazione deve essere continua e dovrà essere una vostra precisa responsabilità individuale!

Intervento dell'Ispettore delle Scuole della Guardia di Finanza Generale di Corpo d'Armata Vito AUGELLI

Didattica assistita dalla tecnologia: nuove frontiere dell'Intelligenza Artificiale

Generale di Corpo d'Armata
Vito AUGELLI

È per me un onore intervenire in questo prestigioso forum, che rappresenta un qualificato momento di sintesi tra la formazione militare, le discipline "Science, Technology, Engineering and Mathematics" (S.T.E.M.) e l'Intelligenza Artificiale.

Oggi l'intelligenza artificiale non è più una prospettiva teorica, ma una realtà operativa che sta già incidendo in modo concreto sulle metodologie didattiche, rendendole sempre più efficaci e tecnologicamente assistite.

La Guardia di Finanza investe in maniera significativa sulla formazione professionale tipica di una forza di polizia economico-finanziaria: per il 2026 sono stati assegnati fondi pari a circa il 20% del budget annuale dell'intera Amministrazione.

I nostri reparti di istruzione, che contano nel complesso circa 9.000 unità, tra personale in formazione (6.000) e permanente (3.000), hanno intrapreso tale evoluzione attraverso una profonda transizione digitale, avviata, in particolare, nell'ultimo biennio, mediante una rapida dematerializzazione dei testi di studio e delle sinossi.

In parallelo, sono stati distribuiti notebook individuali a tutti i frequentatori dei corsi ordinari dell'Accademia di Bergamo e della Scuola Ispettori e Sovrintendenti dell'Aquila. Si tratta di oltre 4.500 dispositivi, acquisiti grazie ai fondi del Piano Nazionale di Ripresa e Resilienza, destinati alla transizione digitale della Pubblica Amministrazione.

Ancora più articolata è stata la reingegnerizzazione dei processi operativi e gestionali degli Uffici addestramento e studi delle varie scuole.

Attraverso il "Sistema Integrato di Gestione e Monitoraggio Allievi" (SIGMA), sviluppato internamente e già in via di sperimentazione, tutte le fasi del processo formativo – dalla gestione delle lezioni all'aggiornamento delle graduatorie, fino agli aspetti amministrativi legati ai compensi dei docenti – sono state integralmente digitalizzate. Il sistema si fonda su un codice sorgente aperto, che ne consente

l'aggiornamento continuo e l'adattamento alle specifiche esigenze dei vari reparti di istruzione.
Le sperimentazioni dell'intelligenza artificiale sono condotte da tutti gli istituti di formazione. In particolare, la Scuola di polizia economico-finanziaria ha adottato metodologie innovative che combinano le potenzialità dell'IA con la didattica e-learning, nell'ambito sia dei corsi nazionali (rivolti nel 2025 a una platea pari ad oltre 25.000 appartenenti al Corpo), sia di corsi internazionali destinati al personale di autorità, forze di polizia e agenzie di "law enforcement" estere. Una platea, quest'ultima, che nel solo 2025 ha raggiunto 4.350 discenti provenienti da 38 Paesi, sia UE che extra UE.
Le forme più avanzate di sperimentazione sono portate avanti dalla Scuola Ispettori e Sovrintendenti dell'Aquila, con lodevole intraprendenza e spirito innovativo, anche in ragione della necessità di gestire numeri senza precedenti: attualmente sono oltre 4.200 gli allievi frequentatori dell'Istituto.
In particolare, da quest'anno, gli allievi ispettori possono contare su un significativo supporto allo studio grazie all'utilizzo dell'applicativo "Notebook-LM", disponibile gratuitamente tra gli strumenti di intelligenza artificiale. Tale sistema elabora esclusivamente i documenti caricati dall'utente, riducendo sensibilmente i rischi di contenuti non attendibili tipici di analoghi software ("chatbot") aperti all'ambiente web.
I materiali di studio (appunti, testi, sinossi, ecc.) possono inoltre essere rielaborati in schemi di sintesi, mappe concettuali, presentazioni, "flash card", brevi video e "podcast" audio, facilitando il ripasso e la memorizzazione dei contenuti. Un'evoluzione rilevante, che mira a un auspicabile miglioramento del rendimento medio dei discenti e, di riflesso, a un rafforzamento delle competenze professionali.
Inoltre, nel mio ruolo di Ispettore dei reparti di istruzione, ho avvertito la necessità di diffondere in tempi rapidi un'"alfabetizzazione" di base sull'intelligenza artificiale e, in questa direzione, sono stati avviati corsi informativi a beneficio degli ufficiali istruttori, articolati ciascuno in 25 moduli intensivi, che consentono di arricchire la conoscenza iniziale e di acquisire un livello intermedio di utilizzo consapevole.
Al contempo, nel percorso addestrativo dei marescialli allievi, è prevista la frequenza di specifici laboratori dedicati all'intelligenza artificiale e alla digital forensics, con l'obiettivo di affiancare alla formazione teorica una solida componente pratica, che ha già portato allo sviluppo "in house" di diverse applicazioni, alcune delle quali illustrate nel panel precedente ("GDFCoach" e "A.R.C.A.").
Prima di concludere, desidero richiamare alcuni profili che attengono all'importanza del fattore umano anche quando parliamo di intelligenza artificiale.
Nel pieno rispetto del principio antropocentrico sancito dall'"Artificial Intelligence Act" europeo (n. 1689/2024) e recepito dalla normativa nazionale (L. n. 132/2025), la nostra didattica continuerà a preservare il ruolo centrale dell'"human in the loop", in particolare nelle fasi di validazione degli output e nei processi decisionali.
Siamo inoltre consapevoli degli effetti collaterali connessi a un uso estensivo

dell'intelligenza artificiale generativa. Per questo motivo, tali strumenti sono bilanciati da una formazione mirata sul pensiero critico, sull'analisi sistemica e, quando necessario, anche da un ritorno alle metodologie tradizionali ("carta e penna") per la risoluzione dei problemi.
Affido, quindi, la chiusura dell'intervento alle immagini che illustrano l'evoluzione più recente dei nostri docenti avatar, oggi fruibili presso i reparti di istruzione del Corpo anche in versione multilingue.

La performance dell'avatar multilingue che cambia idioma in tempo reale è davvero impressionante. Come mai avete sentito l'esigenza di far evolvere così tanto i docenti avatar?

L'esigenza è maturata alcuni anni fa, in particolare nel periodo 2020-2022, quando, da Comandante della Scuola di polizia economico-finanziaria del Corpo, ho avuto, tra l'altro, la responsabilità di organizzare la didattica a distanza per i primi frequentatori stranieri dei nostri corsi e-learning.
Ben presto tali frequentatori, anche grazie all'importante attività di divulgazione svolta dalla nostra rete di esperti presso le rappresentanze diplomatiche e consolari (oggi sono 30 gli ufficiali distaccati all'estero), sono passati da alcune centinaia a diverse migliaia. I corsi riguardano:
- il contrasto patrimoniale alla criminalità organizzata, attraverso gli istituti del sequestro e della confisca, le misure di prevenzione personali e patrimoniali, le indagini finanziarie e la cooperazione internazionale;
- il contrasto al finanziamento del terrorismo, mediante l'identificazione e il tracciamento dei flussi finanziari, la regolamentazione del sistema bancario e finanziario, la cooperazione internazionale e l'applicazione di sanzioni economiche;
- il sistema dei presìdi antiriciclaggio previsti dalla normativa unionale e nazionale.
Il materiale didattico, inizialmente predisposto in inglese, francese e spagnolo in formato PowerPoint, veniva reso disponibile su una piattaforma GdF condivisa.
Successivamente, tale materiale è stato trasformato in contenuti video preregistrati e, da ultimo, in video multilingue generati dall'intelligenza artificiale.

Terza Conferenza Nazionale

Le discipline STEM nella Difesa

"La sfida dell'intelligenza artificiale e la sicurezza comune"

Didattica assistita dalla tecnologia: nuove frontiere dell'intelligenza artificiale

Venezia, 4 febbraio 2026

L'importanza della formazione per la Guardia di Finanza

20%

Budget Annuale

Quota del budget totale della Guardia di Finanza destinato alla formazione

1 di 8

Transizione digitale dei Reparti di Istruzione

Dematerializzazione

Libri e sinossi digitali

4500 notebook individuali

Distribuiti con fondi PNRR

SIGMA

Sistema Integrato di Gestione e Monitoraggio Allievi

2 di 8

Sperimentazioni IA negli Istituti di Formazione

Scuola di Polizia Economico-Finanziaria

Metodologie innovative che combinano IA con didattica e-learning.

Corsi Nazionali

Oltre 30.000 appartenenti al Corpo nel 2025

Corsi Internazionali

Personale di autorità, forze di polizia e agenzie di "*law enforcement*" estere

4350

Partecipanti 2025

Unità formate nei corsi internazionali

38

Paesi Coinvolti

Provenienti da U.E. ed extra U.E.

3 di 8

Super assistenza allo studio

NotebookLM

Elabora **solo documenti caricati dall'utente**

Nessun rischio di allucinazioni

- Schemi di sintesi e mappe
- Video brevi e PowerPoint
- Flash card per il ripasso
- Podcast audio

4 di 8

Alfabetizzazione e formazione

Corsi per Ufficiali formatori

25 moduli in full immersion

Da zero a **livello intermedio**

1. Evoluzione della I.A. Generativa
2. Cos'è e come funziona l'I.A. Generativa
3. Principali L.L.M.
4. Prompt Engineering
5. Didattica Superassistita da NotebookLM
6. Gems, Gpts e automazioni
7. AI Agent

5 di 8

Alfabetizzazione e formazione

Corsi per Ufficiali formatori

25 moduli in full immersion

Da zero a **livello intermedio**

1. Evoluzione della I.A. Generativa
2. Cos'è e come funziona l'I.A. Generativa
3. Principali L.L.M.
4. Prompt Engineering
5. Didattica Superassistita da NotebookLM
6. Gems, Gpts e automazioni
7. AI Agent

5 di 8

Alfabetizzazione e formazione

Laboratori per Marescialli Allievi

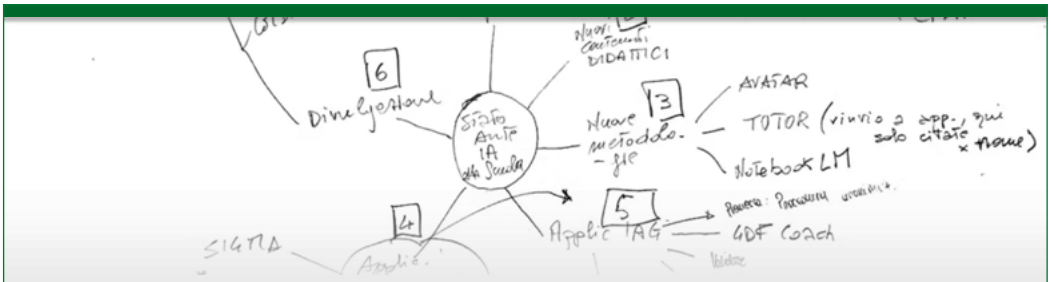
- **Laboratorio IA**
- **Laboratorio Digital Forensics**

Corso teorico

Applicazioni pratiche

Applicazioni come "GDFCOACH" e "A.R.C.A."

6 di 8



Aspetti umani e umanistici

- ✓ **Critical Thinking**
- ✓ **Systemic Thinking**

Il Modello ibrido

Integrazione, non Sostituzione: **processo cognitivo classico & super assistenza IA.**

L'IA non deve rimpiazzare il processo cognitivo, ma potenziarlo.

7 di 8

Docenti avatar poliglotti

Un docente avatar multilingue basato su intelligenza artificiale che **illustra in modo chiaro e personalizzato le lezioni delle materie previste dall'ordinamento didattico, integrando** la didattica tradizionale.

Generazione automatica
Fornendo testi e documenti relativi alla materia, viene generato un video fedele al materiale di riferimento.

Supporto multilingue
Spiegazione strutturata dei contenuti disciplinari con supporto in diverse lingue.

8 di 8

Guardia di Finanza

NEC RECISA RECEDIT

Grazie per l'attenzione


Scuola Navale Militare "Fr
LE DISCIP
STE
NELLA
Isabel


ancesco MOROSINI”
LINE
FESA

Conclusioni del Sottosegretario di Stato alla Difesa Sen. Isabella RAUTI

L'Intelligenza Artificiale è la sfida delle sfide: è un fattore moltiplicatore che rende efficaci le altre tecnologie, dal quantum computing ai big data, dal cyber ai sistemi autonomi. Se padroneggiata e governata, garantisce un vantaggio strategico e competitivo in tutti i domini: tradizionali, nuovi ed emergenti.

Il significato sostanziale della Terza Conferenza STEM coincide con questa impostazione: affrontare l'Intelligenza Artificiale non come un tema tecnico settoriale ma come un abilitatore che riguarda la sicurezza comune, la qualità delle decisioni, il rapporto tra uomo e macchina, il futuro della deterrenza e della sovranità tecnologica.

L'Intelligenza Artificiale è una chiave essenziale per interpretare i nuovi scenari e governarne la complessità. In un contesto internazionale segnato da instabilità crescente, accelerazione dell'innovazione e competizione strategica globale, le nuove tecnologie non costituiscono più soltanto un insieme di strumenti, ma un ambiente operativo e cognitivo entro il quale si ridefiniscono funzioni, responsabilità e priorità delle Istituzioni preposte alla difesa dello Stato.

In questo quadro, la Difesa si conferma non solo come utilizzatrice di innovazione ma come soggetto che forma, educa, seleziona ed organizza competenze. Abbiamo maturato la consapevolezza che la Difesa è STEM per nascita e vocazione, perché opera da sempre nel punto di intersezione tra sapere scientifico, capacità tecnologica e responsabilità decisionale. La sua piramide formativa — Scuole Militari, Scuole Sottufficiali, Accademie delle Forze Armate e Centro Alti Studi della Difesa (CASD) forma un capitale umano qualificato e con visione strategica. Questo patrimonio rafforza l'efficacia dello strumento militare e contribuisce in modo diretto alla sicurezza nazionale, all'innovazione e alla competitività complessiva del Sistema Paese.

L'utilizzo delle nuove tecnologie richiede competenze specialistiche e la formazione in ambito Difesa come asset strategico si sta evolvendo in chiave interforze ed interoperabile per adattare lo strumento militare alle nuove sfide e minacce.

Le discipline STEM costituiscono una vera e propria infrastruttura immateriale della sicurezza nazionale. Senza competenze scientifiche e tecnologiche non vi è autonomia tecnologica; senza autonomia tecnologica diminuisce la libertà di scelta; senza capacità di scelta si indebolisce la sovranità. In un mondo multidominio, la conoscenza assume il valore di fattore di resilienza, di deterrenza e di libertà. Da questo punto di vista, il nesso tra STEM e sicurezza non è contingente ma strutturale: la formazione scientifica diventa una condizione per la tutela delle Istituzioni, per la protezione delle infrastrutture critiche e per la capacità dello Stato di governare il cambiamento.

La trasformazione degli scenari strategici rende questa consapevolezza ancora più piena. Le Forze Armate operano in contesti nei quali ai domini tradizionali di terra, mare e cielo si affiancano il cyberspazio, lo spazio extra-atmosferico, l'ambiente subacqueo e quello cognitivo. Le minacce assumono crescente natura ibrida, di forma persistente e sotto

Sottosegretario di Stato alla Difesa Sen. Isabella RAUTI e allievi

soglia, combinando attacchi cyber, manipolazione delle opinioni e delle informazioni ed interferenze sui processi decisionali. In tale contesto, il vantaggio strategico non dipende soltanto dalla disponibilità di mezzi, ma dalla capacità di integrare informazioni, interpretare scenari e assumere decisioni tempestive e fondate.

L'Intelligenza Artificiale è il baricentro di questa trasformazione. Essa non rappresenta una tecnologia tra le altre, ma una discontinuità profonda, capace di incidere sul modo di analizzare i dati, anticipare gli scenari, pianificare le operazioni, proteggere le infrastrutture critiche e sostenere il ciclo decisionale. In questo senso, l'IA può essere definita un moltiplicatore cognitivo e un motore di capacità: il suo impiego rende la Difesa più autonoma, più efficace, più tempestiva, perché trasforma i dati in capacità operative e rende possibile una più elevata qualità della consapevolezza situazionale.

L'Intelligenza Artificiale è un moltiplicatore cognitivo ed un motore di capacità: il suo impiego rende la Difesa più efficace perché trasforma i dati in capacità operative e supporta il processo decisionale. Ma il vero cambio di passo non è nell'impiego delle tecnologie ma nel governo delle tecnologie; con un approccio adattivo e predittivo, mantenendo sempre il soldato al centro dell'ecosistema della Difesa. Siamo in una fase di competizione globale anche sul quantum e sulle tecnologie emergenti e dirompenti, che comportano enormi vantaggi militari ed economici ma anche una responsabilità morale. Un uso eccessivo e delegato dell'Intelligenza Artificiale generativa comporta costi cognitivi e rischi di perdita della capacità creativa e di giudizio. Come ha ricordato Papa Leone XIV, cedere alle macchine le funzioni vitali del pensiero è un rischio: per questo i saperi umanistici restano un'ancora di salvezza per il libero pensiero. L'IA agisce come strato abilitante dei principali ambiti di frontiera della Difesa. Il Quantum Computing, senza Intelligenza Artificiale, resterebbe una potenza computazionale astratta; con l'IA diventa risorsa strategica per affrontare problemi complessi, dalla sicurezza delle comunicazioni alla simulazione avanzata. I big

data, se lasciati come mera accumulazione quantitativa, non producono alcun vantaggio; attraverso l'IA si trasformano in conoscenza operativa, previsione, orientamento e supporto decisionale. I droni, infine, cessano di essere semplici piattaforme remote e diventano sistemi cooperativi, capaci di interagire in ambienti complessi e multidominio. Governare l'IA significa dunque governare l'intero ecosistema tecnologico della Difesa, preservando sempre la centralità dell'operatore umano, del soldato, del decisore, all'interno del sistema.
Accanto alle opportunità, la Conferenza ha affrontato con lucidità anche i rischi. Un'Intelligenza Artificiale non governata non si limita a produrre errori: può amplificare distorsioni, falsificazioni e manipolazioni, fino a far apparire vero quello che non lo è. Ciò riguarda la disinformazione, i deepfake, le forme più sofisticate di guerra cognitiva, la manipolazione delle percezioni e delle opinioni. Per la Difesa, il governo delle nuove tecnologie non è dunque un capitolo accessorio dell'innovazione, ma una responsabilità centrale verso la Nazione, perché investe la protezione delle informazioni, la resilienza delle infrastrutture critiche, la sicurezza dei dati, la tenuta delle Istituzioni e la libertà dei cittadini. Ne deriva la necessità di un approccio proattivo, capace di arginare i rischi e valorizzare le potenzialità.
Il tema del quantum computing ha assunto, in questo quadro, un rilievo particolare. Esso si presenta come nuovo terreno di competizione tra Stati e come uno dei confini lungo i quali si ridisegneranno gli equilibri globali. Chi governerà queste leve disporrà di vantaggi militari, industriali ed economici significativi. Per questa ragione il quantum non può più essere percepito come ambito riservato a cerchie specialistiche, ma come fattore destinato a incidere sulla sicurezza delle comunicazioni, sulla protezione delle informazioni e sulla sovranità tecnologica. La competizione sulle tecnologie emergenti comporta, dunque, una responsabilità non solo strategica ma anche morale: quella di prepararsi con lungimiranza, di costruire capacità e di evitare che il ritardo tecnologico si traduca in vulnerabilità strutturale.
Uno dei risultati più significativi della Conferenza è stato l'emergere del ruolo dei giovani. Il contributo offerto dagli studenti - nativi digitali - è stato di alto livello e fortemente stimolante. Non si è trattato di una semplice partecipazione, ma di una presenza viva, competente, capace di alimentare il dibattito e di offrire una prospettiva originale sulle tecnologie emergenti. In questa presenza si è resa evidente una verità fondamentale: investire sui giovani significa gettare le premesse di ogni sviluppo futuro. Il capitale umano del domani si forma oggi, e la qualità della sicurezza futura dipenderà dalla qualità della formazione che sapremo offrire a chi sarà chiamato a operare in contesti sempre più complessi, integrati e tecnologicamente sofisticati.
In sintesi: formiamo professionisti completi della Difesa, non robot, capaci di pensiero critico, di creatività, di visione con senso di responsabilità.
Il rapporto tra giovani, apprendimento e nuove tecnologie impone una riflessione ulteriore, più sottile: quella sui costi cognitivi di un uso eccessivo e delegato dell'Intelligenza Artificiale generativa. Se la tecnologia diventa sostitutiva e non abilitante, se la delega del pensiero si fa automatica, si rischia di indebolire la capacità critica, la creatività, il giudizio

e, in ultima analisi, la libertà stessa della persona. Per questo l'Intelligenza Artificiale deve essere padroneggiata come strumento potente ma non considerata come un sostituto dell'intelligenza umana.

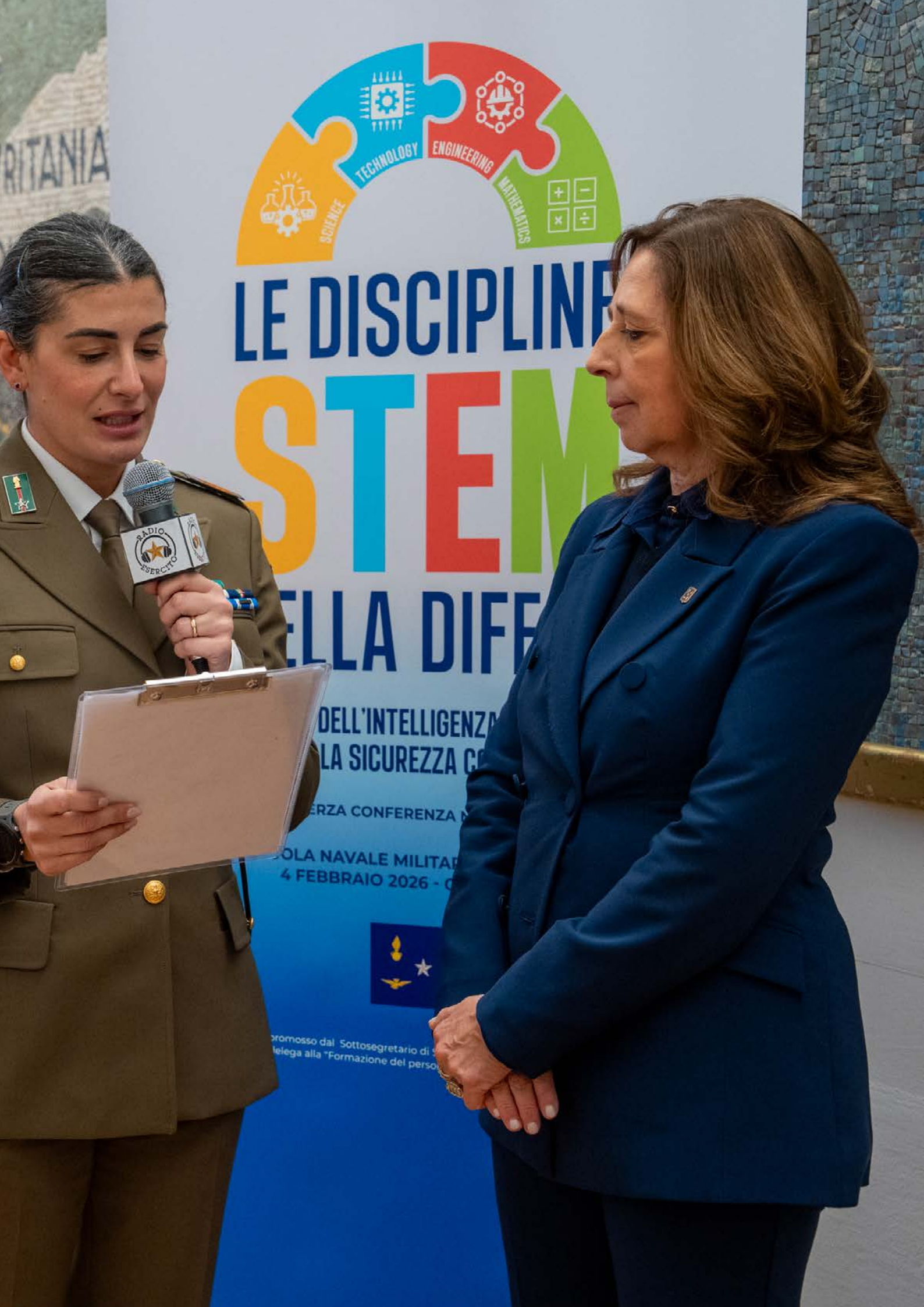
In tale prospettiva, l'integrazione delle STEM con i saperi umanistici diventa una scelta non accessoria ma necessaria. Le STEM devono ampliarsi in STEAM, assumendo il contributo dell'arte, della filosofia, della storia. I saperi umanistici non si contrappongono alle tecnologie: ne costituiscono, piuttosto, una delle condizioni di governo responsabile; aiutano a comprendere limiti, conseguenze, implicazioni e responsabilità dell'innovazione e consentono di preservare il giudizio umano, la libertà interiore e la capacità di scelta. In questo senso, la Conferenza ha richiamato con forza l'idea di un nuovo umanesimo tecnologico, nel quale il fattore umano governa il processo e non viene governato.

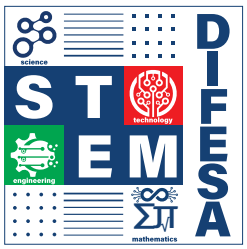
Investire nelle STEM quindi è una scelta di "Sistema Paese": significa rimuovere stereotipi e condizionamenti di genere; allineare domanda ed offerta lavorativa; e costruire competenze per professionisti del futuro. Il pensiero STEM non può prescindere dai saperi umanistici (STEAM) per un equilibrato neo umanesimo tecnologico in cui gli strumenti siano al servizio dell'uomo senza sostituirlo; in una necessaria visione etica ed antropocentrica.

Questa impostazione- come accennato nell'introduzione ai presenti atti - è pienamente coerente con il quadro normativo nazionale ed europeo che disciplina l'Intelligenza Artificiale. L'Italia si è dotata della Legge 132 del 2025 che promuove un uso antropocentrico, trasparente e sicuro dei nuovi sistemi, in raccordo con il quadro europeo. Si tratta di una scelta che unisce etica, sicurezza e competitività e che riporta l'innovazione nel perimetro dell'interesse generale. La regolamentazione, in questa prospettiva, non frena lo sviluppo ma è la pre-condizione della sua legittimità e della sua sostenibilità. Anche da questo punto di vista, la Conferenza di Venezia ha indicato una linea netta: la tecnologia deve essere governata, non subita; orientata, non assolutizzata.

Le discipline STEM sono oggi una leva essenziale della sicurezza nazionale, perché incidono sulla protezione delle informazioni, sulla resilienza delle infrastrutture critiche, sulla capacità di deterrenza, sulla sovranità tecnologica e sulla libertà del Paese. Ma nessuna tecnologia, per quanto avanzata, potrà sostituire il nucleo essenziale della responsabilità umana. L'Intelligenza Artificiale può moltiplicare capacità, accelerare processi, potenziare l'efficacia della Difesa; non può però sostituire il giudizio, la creatività, la coscienza del limite e la libertà della persona. Per questo la Difesa del futuro non forma robot ma professionisti completi, capaci di unire competenza, pensiero critico, visione e senso di responsabilità. È in questa centralità dell'uomo che si gioca, oggi, la vera sfida dell'Intelligenza Artificiale e della sicurezza comune. Ed è garantire la sicurezza di tutti l'obiettivo principale della Difesa.


SPAGNA


TECHNOLOGY
ENGINEERING
SCIENCE
MATHEMATICS
LE DISCIPLINE
STEM
RADIO ESERCITO



PROGETTO GRAFICO E IMPAGINAZIONE

28° reggimento "Pavia"

IMMAGINI

MARINA MILITARE - Raffaele Tampano, Maurizio Flamini

STAMPA

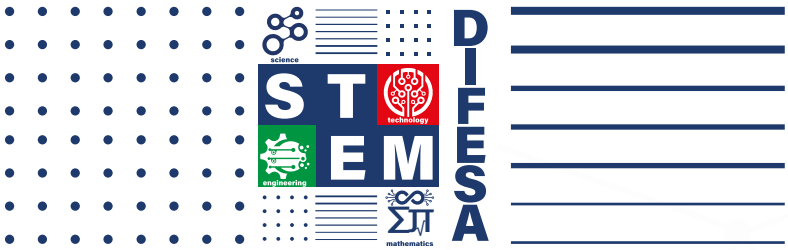
Aeronautica Militare

Comando Servizi Supporto Enti di Vertice

Sezione Grafica e Fototecnica

Pubblicazione del
Ministero della Difesa

Sottosegretario alla Difesa
con delega alla
"Formazione del personale civile e militare della Difesa"


science
STEM
technology
engineering
mathematics
DIFESA