La recente decisione del Governo di ricorrere alla clausola di salvaguardia nazionale, per il biennio 2027-2028, garantisce uno spazio di flessibilità di circa 29 miliardi di euro. Le risorse aggiuntive saranno ripartite, in misura sostanzialmente equivalente, tra Difesa e sicurezza energetica: circa 14,4 miliardi per ciascun settore, pari allo 0,3% del PIL all'anno per la Difesa e allo 0,3% per la sicurezza energetica. Le crisi degli ultimi anni hanno dimostrato che un conflitto può trasformarsi in una crisi energetica, in un attacco alle infrastrutture che può produrre conseguenze economiche, in una campagna cibernetica che può colpire servizi essenziali, oppure nell'interruzione di rotte commerciali e catene di approvvigionamento dalle quali dipendono famiglie e imprese.

Sicurezza militare, sicurezza energetica e sicurezza economica sono quindi sempre più parti della stessa equazione.

È in questo contesto che va letto anche il ragionamento del Ministro della Difesa Guido Crosetto sulla destinazione delle risorse. Il punto non è soltanto quantificare quanto uno Stato spende per la Difesa, ma comprendere cosa rappresenti quella spesa. Ridurre il bilancio militare alla sola acquisizione di armamenti significa, infatti, non considerare una parte essenziale dello strumento attraverso il quale una Nazione protegge la propria sovranità e la propria capacità di agire.

Su cento euro destinati alla Difesa, ha ricordato Crosetto su X il 3 ottobre scorso, circa sessanta sono destinati al personale, dieci al funzionamento quotidiano e trenta agli investimenti. Dietro queste percentuali ci sono donne e uomini delle Forze Armate e dell'Arma dei Carabinieri, personale civile, addestramento, manutenzione, carburanti, infrastrutture e capacità operative. Ma ci sono anche ricerca, sviluppo tecnologico e una filiera industriale che coinvolge grandi gruppi e centinaia di piccole e medie imprese.

In aggiunta a queste motivazioni, la spesa per la Difesa non può essere considerata una variabile isolata del bilancio pubblico perché una parte di quelle risorse torna nel sistema economico attraverso occupazione, produzione, ricerca e innovazione. Al riguardo, il nostro Paese possiede una significativa base industriale e tecnologica e dispone di competenze consolidate nei settori aerospaziale, navale, elettronico, della sicurezza digitale e dei sistemi avanzati. Difendere questa capacità significa anche proteggere una componente della competitività nazionale.

La deterrenza nasce proprio da questa consapevolezza e la resilienza, allo stesso modo, non nasce nel momento in cui arriva una crisi ma viene costruita prima, attraverso investimenti, competenze, infrastrutture e una lungimirante visione strategica.

È questo il significato più profondo della decisione di utilizzare la clausola di salvaguardia per Difesa e sicurezza energetica.

Periodico bimestrale

ID

"INFORMAZIONI DELLA DIFESA"
Registrazione Tribunale Civile di Roma n. 105 del 19 marzo 1982

Direttore Editoriale
Diego Filippo Fulco

Direttore Responsabile
Massimiliano D'Elia
massimiliano.delia@difesa.it

Caporedattore
Aniello Fasano
aniello.fasano@difesa.it

Responsabile grafica e Progetti editoriali
Antonio Morlupi

Multimedia e Web
Antonio Di Ieva

Segreteria di Redazione
informazionidifesa@difesa.it

Redazione
redazioneID@difesa.it
06 469150471

Fotografie
Ministero della Difesa
123rf.com
Immagini e infografiche sono generate con Intelligenza Artificiale e modificate dalla redazione

Copertina
Generata con Ai e rielaborata da Antonio Morlupi

Sede
Ministero della Difesa
Palazzo Baracchini,
Via XX settembre 8
00187 - Roma

Abbonamento
Gli articoli pubblicati rispecchiano le idee personali degli autori e non riflettono il pensiero ufficiale del Ministero della Difesa

©Tutti i diritti riservati

Stampa
Teraprint srl - Roma

Numero chiuso in redazione
il 12/10/2026

MINISTERO DELLA DIFESA

Editore

DIFESA SERVIZI

Forest Stewardship Council FSC

sommario

In Evidenza 1

World News 4

DIFESA

Una sfida per la credibilità strategica dell'Unione Europea 8
di Gen. Luciano Portolano
Capo di Stato Maggiore della Difesa

La Difesa cambia passo 12
di Informazioni della Difesa

La nuova Difesa guarda sempre più al personale 20
di Informazioni della Difesa

Crosetto in Senato sulla riforma della Difesa 26
di Informazioni della Difesa

Le risorse per la Difesa. Gli strumenti dell'Unione Europeaa 28
di Informazioni della Difesa

SPECIALE HYBRID

È guerra ibrida 32
di Massimiliano D'Elia

OLTRE LA NOTIZIA - A tu per tu con Maurizio Molinari
La guerra ibrida è già in Europa 38
di Massimiliano D'Elia

La guerra dentro la mente 42
di Informazioni della Difesa

Overload informativo e le minacce di natura antropica 44
di Michele Zizza

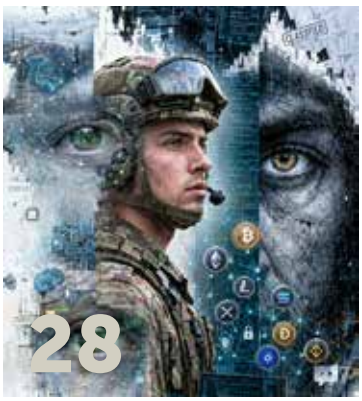
Ceuta e la strumentalizzazione politica delle migrazioni 48
di J Luigi M. Kunz Saponaro

TECNOLOGIE EMERGENTI

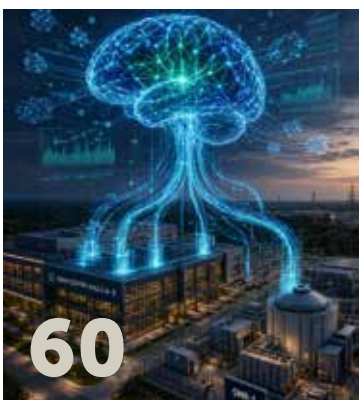
La guerra vista dalla "kill zone" 52
di Cecilia Sala

La digitalizzazione della guerra 56
di Informazioni della Difesa









Hanno collaborato:

MICHELE ZIZZA
Prof. Università degli Studi della Tuscia di Viterbo

J LUIGI M. KUNZ SAPONARO
Universidad Carlos III de Madrid - Departamento de Humanidades

CECILIA SALA
Giornalista «Chora News»

GIUSEPPE CALABRÒ
Prof. Università degli Studi della Tuscia

ANDREA CELESTI
Giornalista «Corrire della Sera»

GIANCLAUDIO TORLIZZI
Fondatore di «T-Commodity»

STEFANO PIAZZA
Giornalista «Panorama/La Verità»

VITTORIO EMANUELE PARSI
Prof. Università Cattolica del Sacro Cuore, Accademia dei Lincei

GEN. LUCIANO PORTOLANO
Capo di Stato Maggiore della Difesa

CARLO ALBERTO CARNEVALE MAFFÈ
Professore alla SDA Bocconi School of Management

GIOVANNI CAPRARA
Giornalista scientifico

ANTONIO LO CAMPO
Giornalista- Aerospazio

Dall'intelligenza artificiale al nucleare 60
di Giuseppe Calabrò

Il mare, nuova frontiera strategica dell'intelligenza artificiale 66
di Informazioni della Difesa

Rinnovabili e nucleare 70
di Andrea Celesti

Terre rare la vera battaglia è sul magnete 74
di Gianclaudio Torlizzi

GEOPOLITICA

Xi Jinping e il ritorno dell'uomo forte per una Cina destinata a dominare il XXI secolo 80
di Stefano Piazza

Il momento dell'Europa (e del Canada) 84
di Vittorio Emanuele Parsi

NEWS DIFESA

News Ministero 90

CHOD/NAD Conference 96

ECONOMIA

La deterrenza non è un arsenale ma una filiera 98
di Carlo Alberto Carnevale Maffè

SPAZIO

Tessuti intelligenti, innovazione italiana Intervista a Corinna Sperandini A.D. di Spacewear 102
di Aniello Fasano

Aviolancio italiano 108
di Giovanni Caprara

Zhuque-3 atterra con successo, anche la Cina ha i suoi razzi riutilizzabili 112
di Informazioni della Difesa

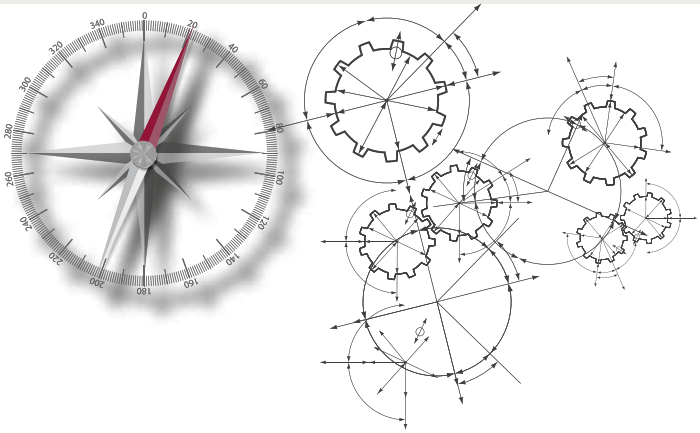
Guerre stellari 116
di Antonio Lo Campo











LA MAXI FERROVIA CINA UZBEKISTAN



31 agosto 2026

Xi Jinping punta a rafforzare l'influenza cinese in Asia centrale attraverso commercio, infrastrutture e sicurezza. Al vertice della Shanghai Cooperation Organization a Bishkek, la Cina ha posto al centro collegamenti ferroviari, energia, sicurezza alimentare e cooperazione digitale. Gli scambi con i cinque Paesi della regione hanno raggiunto i 106 miliardi di dollari. Strategica la ferrovia Cina-Kirghizistan-Uzbekistan, destinata a creare un nuovo corridoio verso Medio Oriente ed Europa e a ridurre la dipendenza dalle rotte marittime. Pechino cresce anche lungo il Corridoio di mezzo, mentre Mosca conserva un ruolo centrale nella sicurezza regionale.

LA TURCHIA ADERISCE AGLI ACCORDI ARTEMIS



1 settembre 2026

La Turchia ha aderito agli Accordi Aerospaziali Artemis quale 71esimo Paese firmatario. L'adesione rafforza il ruolo di Ankara nella cooperazione internazionale per l'esplorazione lunare e spaziale e apre alla partecipazione turca alle future missioni attraverso tecnologie, strumenti scientifici e CubeSat. La scelta si inserisce nel programma spaziale nazionale avviato dalla Turchia, che punta anche all'esplorazione della Luna. Ankara sta sviluppando AYAP-1, la prima missione turca verso un altro corpo celeste. L'ingresso negli Accordi Artemis impegna inoltre la Turchia a sostenere un'esplorazione dello spazio pacifica, trasparente e coordinata, nel rispetto dei principi internazionali.

GERMANIA AFD PRIMO PARTITO IN SASSONIA



6 settembre 2026

La vittoria dell'AfD in Sassonia-Anhalt segna una svolta politica di grande rilievo per la Germania. Il partito ha conquistato il 43,8% dei secondi voti, ottenendo 39 degli 83 seggi del Landtag. Un risultato che porta una formazione classificata dalle autorità tedesche in alcune articolazioni come estremista al centro degli equilibri istituzionali e rende più complessa la formazione di una maggioranza. La dimensione del consenso rappresenta inoltre un segnale significativo per il sistema politico nazionale, perché mostra la capacità dell'AfD di trasformare il malcontento elettorale in una forza parlamentare dominante a livello regionale. Il risultato "normalizza" le posizioni dell'estrema destra nelle istituzioni tedesche.



LA CRISI POLITICA SPAGNOLA PORTA ALLE ELEZIONI

5 ottobre 2026

Pedro Sánchez ha annunciato lo scioglimento delle Cortes e il ritorno alle urne il 29 novembre, dopo la crescente difficoltà del governo nel mantenere una maggioranza parlamentare. La decisione è arrivata dopo la bocciatura parlamentare delle misure sulla casa, in un quadro già segnato da tensioni con gli alleati e da una maggioranza fragile.

CACCIA ITALIANO ABBATTE DRONE IN LITUANIA



15 settembre 2026

Due Eurofighter F-2000 della Task Force Air «Baltic Thunder III» dell'Aeronautica Militare sono decollati dalla base di Šiauliai dopo l'ingresso di un drone nello spazio aereo lituano. L'intervento, avvenuto nella tarda serata del 14 settembre, si è concluso con la neutralizzazione del velivolo senza pilota. L'azione conferma la funzione della presenza italiana sul fianco orientale dell'Alleanza e, soprattutto, la capacità di trasformare la sorveglianza permanente in una risposta immediata a una possibile minaccia. La Task Force «Baltic Thunder III», attiva dal 31 luglio, garantisce la difesa dello spazio aereo di Estonia, Lettonia e Lituania. Per il sottosegretario alla Difesa Matteo Perego di Cremnago, l'episodio dimostra ancora una volta quanto sia fondamentale la presenza italiana sul fianco Est della NATO.

81ª ASSEMBLEA DELL'ONU



22 novembre 2026

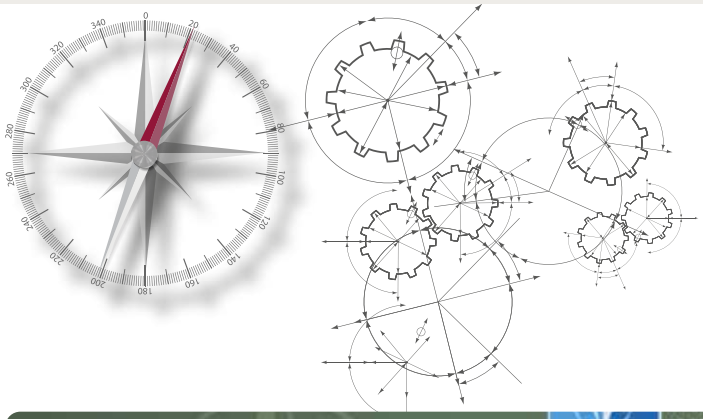
L'81ª Assemblea Generale delle Nazioni Unite si è chiusa dopo una settimana segnata da appelli alla pace, critiche al sistema internazionale e accuse tra governi. Il segretario generale Antonio Guterres ha chiesto di fermare i combattimenti e rispettare il diritto internazionale, sottolineando la necessità di un ruolo maggiore dell'Assemblea quando il Consiglio di Sicurezza non riesce ad agire. Il ministro degli Esteri Antonio Tajani ha ribadito che la pace resta la «stella polare» della politica estera italiana, mentre Donald Trump ha rivendicato i risultati della propria amministrazione. Acceso lo scontro sul Medio Oriente, con Trump e Netanyahu impegnati a difendere l'operato di Israele a Gaza. L'Assemblea ha così evidenziato le profonde divisioni del sistema multilaterale.

L'ITALIA APPROVA LA LEGGE SUL RITORNO AL NUCLEARE



29 settembre 2026

La legge sul nucleare sostenibile segna il ritorno dell'energia atomica nel quadro normativo italiano. La legge n. 169, delega il Governo a definire entro dodici mesi una disciplina organica per la produzione e l'utilizzo dell'energia nucleare. Il provvedimento riguarda l'intero ciclo del nucleare, dalla realizzazione degli impianti alla gestione del combustibile e dei rifiuti radioattivi, fino allo smantellamento delle strutture esistenti. La delega comprende inoltre ricerca e sviluppo, tecnologie avanzate e modulari, formazione e sicurezza. L'obiettivo è contribuire alla sicurezza e all'indipendenza energetica nazionale, sostenendo al tempo stesso una filiera industriale italiana ed europea.



VERTICE NATO COPENAGHEN: La sicurezza passa dalla capacità di essere pronti



DA Copenaghen i vertici militari dell'Alleanza hanno rilanciato la necessità di trasformare l'aumento dei bilanci della difesa in forze disponibili, scorte, tecnologie e infrastrutture capaci di sostenere una crisi prolungata.

Il 18 e 19 settembre, il Military Committee ha riunito a Copenaghen i 32 capi di Stato maggiore della Difesa della NATO, insieme ai comandanti strategici Alexus Grynkewich e Pierre Vandier, sotto la presidenza dell'Ammiraglio italiano Giuseppe Cavo Dragone. La riunione ha dato seguito alle decisioni del vertice di Ankara, accelerando il passaggio dagli stanziamenti alle capacità necessarie per la deterrenza e la difesa euro-atlantica. «Gli investimenti devono tradursi in forze pronte, capacità operative e piani realizzabili. Questo deve essere il cuore di una NATO 3.0 più forte e più equa», ha dichiarato Cavo Dragone. Tra le priorità ha indicato difesa aerea e antimissilistica, droni, sicurezza informatica e capacità spaziali, sottolineando la necessità di «accelerare la prontezza e la capacità di operare in tutti i domini».

La guerra in Ucraina ha mostrato quanto rapidamente possano essere consumate munizioni, droni e sistemi d'arma e quanto sia complesso sostituirli quando l'industria opera secondo ritmi da tempo di pace. La prontezza militare riguarda quindi non solo le forze disponibili, ma anche la capacità di mobilitarle, rifornirle e sostenerle nel tempo, insieme alla possibilità dell'industria di aumentare rapidamente la produzione. Gli investimenti devono tradursi in linee produttive, manutenzione, consegne e catene di approvvigionamento resilienti. Una capacità che non può essere prodotta o sostituita in tempi compatibili con le esigenze operative rischia infatti di rimanere solo sulla carta.

Sul piano tecnologico, l'Alleanza punta sulla difesa aerea e antimissile integrata, sui sistemi senza pilota e relative contromisure, sui domini cyber e spaziale, sulla mobilità strategica e sulla protezione delle infrastrutture critiche. La direzione è quella di una difesa multidominio, capace di collegare sensori, sistemi di comando, piattaforme e armamenti.

L'esercitazione Ramstein Flag 2026, nell'ambito di Eastern Sentry, ha integrato attività aeree, terrestri, marittime, cyber e spaziali. Eastern Sentry è stata sviluppata dopo le violazioni dello spazio aereo alleato registrate nel 2025 e comprende nuove tecnologie e tattiche per contrastare i droni.

La sicurezza è minata inoltre da sabotaggi, cyberattacchi, violazioni dello spazio aereo e minacce alla resilienza delle società alleate. Cavo Dragone ha richiamato la necessità di mantenere la coesione tra gli Stati membri, mentre l'attenzione dell'Alleanza si estende al Nord Europa e all'Artico, sempre più rilevanti per la sicurezza euro-atlantica.

Il passaggio indicato a Copenaghen è dunque dalla disponibilità finanziaria alla capacità operativa: trasformare le risorse in forze, munizioni, droni, intercettori, sensori, sistemi di comando e infrastrutture realmente pronti all'impiego.



L3HARRIS.COM

>>>0629_LHX_FF>>>

LHX01
LHX02
LHX03

W E

L3HARRIS®

THE TRUSTED DISRUPTOR

GEN. LUCIANO PORTOLANO
Capo di Stato Maggiore della Difesa



Una sfida per la credibilità strategica dell'Unione Europea



La crisi libanese e la fine di UNIFIL aprono nuovi scenari per la sicurezza regionale. L'ipotesi di una missione PSDC potrebbe rafforzare le istituzioni libanesi e le LAF, offrendo all'UE un banco di prova per tradurre ambizioni strategiche in capacità operative, bilanciando obiettivi, risorse e consenso politico

Le conseguenze della crisi economica e istituzionale che da anni affligge il Libano, sommate alle tensioni generate dal confronto tra Israele e Hezbollah e alle più ampie dinamiche di instabilità che attraversano il Medio Oriente, hanno riportato il Paese dei Cedri al centro del dibattito internazionale.

In tale contesto, l'attenzione crescente dell'Unione Europea, verso il dossier libanese, assume un significato che va ben oltre la gestione di una specifica crisi regionale. Per Bruxelles, la capacità di contribuire alla stabilità del Mediterraneo e del Medio Oriente non rappresenta più soltanto un esercizio di politica estera, ma una componente essenziale della tutela degli interessi strategici europei e della credibilità dell'Unione quale Global Security Provider.

In tale prospettiva, la disponibilità a un possibile coinvolgimento in Libano nell'ambito della Politica di Sicurezza e Difesa Comune (PSDC) - più volte evocata dall'Alto Rappresentante per gli Affari Esteri e la Politica di Sicurezza Kaja KALLAS - assume un valore che va oltre la mera dimensione operativa.

In questo quadro, nel recente vertice politico italo-francese è emersa la necessità di evitare un vuoto di sicurezza causato dalla cessazione di UNIFIL (dicembre 2026), così come l'intenzione congiunta di promuovere una coalizione internazionale di sostegno al Libano, in coordinamento con UE e ONU, con l'obiettivo di rafforzare la sovranità del Paese e sostenere le Lebanese Armed Forces (LAF).

I colloqui hanno posto in evidenza l'esigenza di un mandato chiaro, centrato sull'integrità territoriale del Libano e sul principio del monopolio delle armi nelle mani delle forze armate statali, unitamente alla possibilità di promuovere una conferenza internazionale per formalizzare l'iniziativa.

Questi sviluppi si inseriscono in un contesto già caratterizzato da profonde trasformazioni dell'architettura di sicurezza regionale. Infatti, per quasi vent'anni, la missione UNIFIL ha rappresentato il principale pilastro della presenza internazionale nel Libano meridionale, contribuendo a contenere le tensioni lungo la Blue Line e a preservare uno spazio minimo di dialogo tra le parti in una delle aree più sensibili del Medio Oriente.

Le trasformazioni intervenute nell'architettura di sicurezza mediorientale hanno tuttavia evidenziato i limiti di un modello pensato per una realtà strategica ormai mutata. La crescente complessità del quadro securitario - con l'annunciata conclusione della missione UNIFIL - l'emergere di nuove minacce e il deterioramento del sistema politico libanese indicano oggi la necessità di adottare modelli assistenziali caratterizzati da maggiore flessibilità politico-operativa, affiancando al tradizionale peacekeeping strumenti di capacity building più orientati al rafforzamento delle istituzioni di sicurezza locali. Un'impostazione che, muovendo dalla pluriennale esperienza della UE in ambito PSDC, riflette una lezione ormai consolidata: la stabilità sostenibile non può essere garantita esclusivamente dalla presenza di contingenti stranieri, ma richiede istituzioni locali capaci di esercitare efficacemente le proprie funzioni. La costruzione di capacità nazionali rappresenta quindi non soltanto uno strumento operativo, ma una vera e propria scelta strategica, orientata a creare le condizioni affinché gli attori locali possano progressivamente assumere la responsabilità della propria sicurezza.

In questa prospettiva, una missione europea potrebbe rappresentare l'evoluzione naturale di un approccio che, senza sostituire il ruolo delle Nazioni Unite, punti a sostenere le istituzioni statali libanesi - anche attraverso il supporto alle Lebanese Armed Forces - per favorire una maggiore resilienza complessiva dello Stato nel lungo periodo.

Un impegno che, per l'Unione Europea,



UNIFIL

Istituita nel 1978 e rafforzata dopo il conflitto del 2006 attraverso la Risoluzione 1701 del Consiglio di Sicurezza ONU, UNIFIL opera nel Libano meridionale con il compito di monitorare la cessazione delle ostilità e sostenere le autorità



La PSDC rappresenta uno degli strumenti principali dell'azione esterna della UE nel campo della gestione delle crisi. Essa costituisce lo strumento attraverso il quale la UE conduce missioni e operazioni civili e militari al di fuori dei propri confini, con attività che spaziano dall'addestramento delle F.A. di Paesi partner alla riforma del settore della sicurezza, fino alle operazioni

assumerebbe un valore soprattutto nella sua dimensione strategica. Da tempo, infatti, Bruxelles rivendica l'ambizione di giocare un ruolo più incisivo nella sicurezza internazionale, ma la credibilità di questa aspirazione dipende dalla capacità di tradurre gli orientamenti politici in iniziative concrete. In questo senso, il Libano potrebbe rappresentare un banco di prova significativo, offrendo l'occasione di dimostrare la capacità dell'Unione di assumere responsabilità proporzionate al proprio peso politico, armonizzando strumenti diplomatici, economici (tra cui lo European Peace Facility - EPF), civili e militari in un approccio integrato coerente alla gestione delle crisi.

EPF è uno strumento extra-bilancio della UE con il quale è possibile finanziare missioni militari e il rafforzamento delle capacità dei Partner, anche attraverso la fornitura di equipaggiamenti militari

Sul piano istituzionale, la possibilità di assumere un ruolo centrale nella gestione della crisi libanese rappresenterebbe per la UE anche un'occasione per consolidare l'evoluzione degli strumenti europei di Comando e Controllo, con particolare riferimento al Military Planning and Conduct Capability (MPCC) che, negli ultimi anni, ha progressivamente rafforzato il proprio ruolo affermandosi come principale struttura di riferimento in ambito UE per la pianificazione e la condotta delle missioni e operazioni militari dell'Unione.

Al tempo stesso, è necessario mantenere un approccio realistico. Il Libano resta un contesto altamente complesso, in cui dinamiche interne e regionali si intrecciano costantemente. Nessuna missione internazionale, indipendentemente dalle risorse impiegate, può realisticamente affrontare in modo risolutivo problematiche che affondano le proprie radici nella struttura politica del Paese e negli equilibri strategici del Medio Oriente. Da questo punto di vista, il principale rischio sarebbe rappresentato dal possibile disallineamento tra ambizione politica e sostenibilità operativa. Un maggiore coinvolgimento genererebbe aspettative elevate, sia all'interno dell'Unione sia presso i partner regionali, che, in assenza di risultati concreti, potrebbe ampliare ulteriormente il tradizionale divario tra ambizione politica e capacità di attuazione che ha spesso caratterizzato il dibattito sulla difesa europea.

Inoltre, occorre considerare che il successo di un intervento PSDC dipende in larga misura dalla capacità degli Stati membri di mantenere una visione condivisa degli obiettivi da perseguire. La politica di sicurezza e difesa dell'Unione si fonda, infatti, sul consenso politico tra governi nazionali, elemento che rappresenta al tempo stesso la sua forza e il suo principale limite. Un'azione efficace richiederebbe pertanto non soltanto adeguate risorse operative, ma soprattutto una convergenza strategica sufficientemente solida da garantire continuità nel tempo.

In questo senso, la convergenza franco-italiana emersa nel vertice di Antibes costituisce un segnale politico rilevante, poiché contribuisce a rafforzare la coesione europea su un dossier tradizionalmente complesso.

In questo contesto, il valore aggiunto di un'iniziativa europea passerebbe anche dall'efficace coordinamento con le varie attività di supporto già esistenti nella regione e dalla conseguente valorizzazione delle esperienze maturate dai singoli Stati membri, tra cui l'Italia. La lunga partecipazione a UNIFIL e la missione MIBIL hanno consentito al nostro Paese di sviluppare una conoscenza approfondita del teatro e di consolidare rapporti di fiducia con le istituzioni libanesi e con i partner internazionali presenti nell'area. Un eventuale rafforzamento del

ruolo europeo si collocherebbe in continuità con l'approccio tradizionalmente sostenuto dall'Italia, fondato sulla centralità del multilateralismo, sul rafforzamento delle istituzioni locali e sulla convinzione che la sicurezza del Mediterraneo rappresenti una componente essenziale della sicurezza europea.

In definitiva, l'ipotesi di una missione PSDC in Libano non dovrebbe essere interpretata esclusivamente come una risposta a una specifica crisi regionale. Essa rappresenta piuttosto un indicatore della direzione intrapresa dall'Unione Europea in materia di sicurezza e difesa. Se negli anni passati tali temi occupavano una posizione marginale nel progetto europeo, oggi essi sono stabilmente al centro delle riflessioni strategiche dell'Unione. Il Libano potrebbe offrire l'opportunità di tradurre questa evoluzione politica in un'iniziativa concreta, capace di coniugare sostegno alla stabilità regionale e rafforzamento del ruolo internazionale dell'Unione. La sfida, come spesso accade nelle questioni strategiche, non sarà tanto quella di definire l'ambizione, quanto di garantire la coerenza tra obiettivi, risorse e volontà politica necessarie per conseguirli.



ATTO di INDIRIZZO del Ministro della Difesa

2026

Pdf Atto di Indirizzo del Ministero della Difesa 2026

AI Generate

LA DIFESA CAMBIA PASSO

Difesa, innovazione e velocità: la sfida è adattarsi prima della minaccia

Dalla difesa aerospaziale allo spazio, dalla dimensione subacquea al cyber, dall'intelligenza artificiale alla base industriale, la priorità diventa ridurre il tempo tra l'evoluzione della minaccia, la decisione e la capacità di produrre un effetto operativo



La Difesa deve poter cambiare alla stessa rapidità con cui evolve la minaccia. È questa una delle considerazioni che attraversano l'Atto di Indirizzo per l'avvio del ciclo integrato di programmazione della performance e di formazione del bilancio di previsione per l'E.F. 2027 e la programmazione pluriennale 2028-2029„ firmato dal Ministro della Difesa Guido Crosetto, e che orientano la trasformazione dello Strumento militare italiano. Il documento non si limita a indicare nuovi programmi di acquisizione, ma interviene sul modo con cui la Difesa dovrà sviluppare capacità, organizzare le proprie risorse e trasformare l'innovazione tecnologica in uno strumento operativo.

Terra, mare, aria, spazio e cyber non costituiscono più dimensioni separate, ma parti di un unico ambiente operativo nel quale assumono crescente rilevanza anche lo spettro elettromagnetico, l'ambiente subacqueo e quello cognitivo. La disponibilità di dati, la capacità di elaborarli, l'intelligenza artificiale e le tecnologie emergenti si integrano con fattori tradizionalmente considerati esterni alla dimensione militare, come energia, infrastrutture, catene di approvvigionamento e resilienza industriale.

L'esperienza dei conflitti recenti, a partire dalla guerra in Ucraina, ha accelerato questa trasformazione. Il conflitto ha mostrato la rapidità con cui possono cambiare tattiche, tecnologie e modalità d'impiego. La diffusione dei sistemi a pilotaggio remoto ha prodotto cicli di innovazione dell'ordine delle settimane, nei quali software, sensori, algoritmi e modalità operative possono essere modificati mentre la capacità è già impiegata sul terreno. La capacità militare, di conseguenza, non coincide più soltanto con il possesso di piattaforme tecnologicamente avanzate, ma comprende la

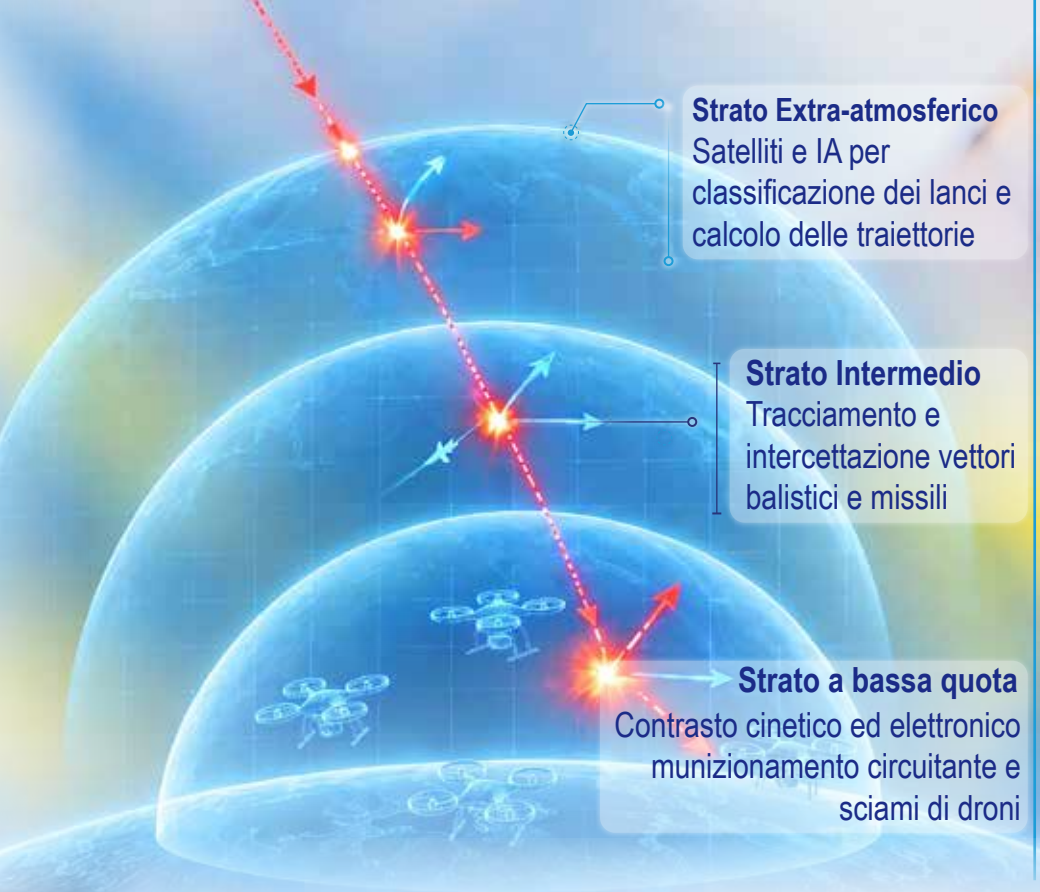
EVOLUZIONE DEI CONFLITTI



Il tempo utile per comprendere, decidere e reagire si è drasticamente ridotto. La competizione ibrida ha eroso definitivamente la distinzione tra guerra e pace: le pressioni operano sotto la soglia del conflitto per colpire reti, infrastrutture e istituzioni.

IL SALTO CULTURALE E OPERATIVO

	Difesa tradizionale	Difesa contemporanea
Focus strategico	Proiezione fuori area e gestione di crisi circoscritte	**Protezione del territorio**, deterrenza ad alta intensità e **resilienza nazionale**
Natura della minaccia	Esclusivamente cinetica e convenzionale	**Ibrida, continua** e **multidominio** (cyber, spazio, cognitivo e dimensione subacquea)
Velocità di adattamento	Cicli di sviluppo tecnologico misurati in anni o mesi	**Innovazione tattica** sul campo misurata in settimane
Modello tecnologico	Dipendenza da poche piattaforme premium e costose	Mix di **alta tecnologia** integrata con **massa scalabile** ed **economica** (cheap to cheap)



Lo scudo aerospaziale multilivello

Cupola protettiva modulare e interoperabile, con IA per ottimizzare il rapporto costo-efficacia. L'Italia come fulcro della difesa europea continentale



Dominio Spaziale

Rafforzamento delle capacità e nuove soluzioni organizzative: Corpo Spaziale della Difesa e/o Agenzia Spaziale.



Presidio subacqueo

Protezione delle dorsali energetiche e dati vitali. Sviluppo del PNS per l'innovazione tra Difesa, industria e ricerca



Contrasto ibrido e resilienza cognitiva

Postura cyber proattiva e Centro Nazionale ed Europeo contro la guerra ibrida, per proteggere reti e filiere da disinformazione e IA



Tecnologia & dati

Trasformazione digitale, integrazione responsabile dell'IA, superamento del divario tra scoperta e adozione

Capitale umano

Reclutamento agile, riduzione età media, competenze STEM e cyber, Focus sulla specificità dello status militare (tutele, benessere, addestramento realistico in poligoni adeguati)

Base industriale

Osmosi rapida tra industria civile e militare. Procurement europeo, requisiti comuni e logica di sperimentazione continua (cross-esperience)

Comprensione condivisa e Comando/controllo Multidominio

Vedere prima, decidere prima, agire prima

SATCOM & reti resilienti

Joint: superamento dei compartimenti stagni per effetti sincronizzati

SATCOM & reti resilienti

Inter-agenzia: integrazione con Difesa civile, Carabinieri e Sistema Paese

SATCOM & reti resilienti

CDEC: Comunità di Difesa dell'Europa continentale

SATCOM & reti resilienti

NATO: consolidamento del pilastro europeo dell'Alleanza atlantica

AI Generate

Ecosistema integrato. La Difesa non agisce come somma di parti separate, ma come una piattaforma di integrazione dello Stato per superare le frammentazioni interne e rafforzare la deterrenza

possibilità di adattarle, aggiornarle e produrle con una velocità compatibile con quella della minaccia.
Uno degli elementi più significativi dell'Atto riguarda il rapporto tra qualità e quantità. La superiorità tecnologica rimane essenziale, ma non può prescindere dalla disponibilità numerica delle capacità e dalla possibilità di sostenerle nel tempo. Un confronto ad alta intensità richiede munizionamento, scorte, manutenzione, ricambi e una capacità industriale in grado di reintegrare rapidamente ciò che viene consumato.
Il documento parla esplicitamente di un ritorno della massa, ciò non significa sostituire i sistemi avanzati con soluzioni meno sofisticate, ma affiancare alle piattaforme di maggiore complessità sistemi più semplici, economicamente sostenibili e facilmente moltiplicabili. Il rapporto tra costo della minaccia e costo della risposta diventa così, un elemento della sostenibilità operativa, soprattutto quando le difese devono affrontare attacchi caratterizzati da numeri elevati e cicli di impiego ravvicinati.
Una delle priorità individuate dall'Atto riguarda la difesa aerospaziale multilivello, concepita attraverso lo sviluppo dello Scudo della Difesa Nazionale ed Europeo. Missili balistici, sistemi ipersonici, droni d'attacco e munizionamento circuitante che possono essere impiegati contemporaneamente, creando condizioni di saturazione. La risposta richiede, pertanto, una rete nella quale sensori, satelliti, intelligence, sistemi di comando e controllo e capacità di ingaggio possano operare come un unico sistema. In questa architettura, l'intelligenza artificiale può contribuire a comprimere il tempo necessario per acquisire, classificare e correlare le informazioni, supportando il passaggio dalla rilevazione della minaccia alla scelta della risposta. La questione non riguarda, quindi, soltanto le prestazioni del singolo sistema d'arma, ma la capacità di mettere in rete sensori, dati e piattaforme, individuando, di volta in volta, la soluzione più efficace e sostenibile.
La stessa impostazione viene applicata allo Spazio, la cui rilevanza è direttamente collegata alla capacità delle Forze Armate di operare nei domini tradizionali. Osservazione della Terra, navigazione, comunicazioni e comando e controllo dipendono, infatti, da infrastrutture spaziali che costituiscono una componente essenziale della superiorità informativa.
L'Atto indica la necessità di consolidare la postura nazionale nel dominio spaziale, attraverso il rafforzamento delle competenze e delle capacità disponibili e la prospettiva di nuove soluzioni organizzative, tra cui la progressiva creazione di un Corpo Spaziale della Difesa e/o di un'Agenzia Spaziale.
Nel periodo transitorio, il ricorso a operatori commerciali dovrà consentire di assicurare continuità a servizi strategici mentre maturano le capacità nazionali. Il principio è particolarmente evidente per le comunicazioni satellitari, per le quali l'Atto prevede una soluzione ponte in attesa del progressivo sviluppo di una capacità nazionale autonoma.
Un'altra area nella quale la Sicurezza nazionale dipende sempre più da infrastrutture difficilmente controllabili è quella subacquea. Cavi per le telecomunicazioni, collegamenti energetici e altre infrastrutture strategiche attraversano i fondali e rappresentano elementi essenziali per il funzionamento delle economie moderne.
La loro protezione non può essere affidata esclusivamente alla presenza fisica lungo migliaia di chilometri. Diventano, quindi, centrali la capacità di sorveglianza, l'acquisizione dei dati e l'impiego di sensori e sistemi autonomi, in modo da comprendere, in tempo reale, ciò che accade sotto la superficie senza dover presidiare staticamente l'intera rete infrastrutturale.
In questa prospettiva si inserisce il "Polo Nazionale della Dimensione Subacquea", che l'Atto individua come elemento da consolidare attraverso l'integrazione tra Difesa, industria, università e ricerca. La dimensione subacquea diventa, così, non soltanto un settore operativo, ma un ecosistema tecnologico nel quale conoscenza scientifica, capacità industriale e sicurezza delle infrastrutture concorrono allo stesso obiettivo.
La trasformazione interessa anche gli spazi nei quali il confronto può svilupparsi senza assumere immediatamente la forma di un conflitto militare convenzionale. Cyberattacchi, sabotaggi, interferenze, manipolazione delle informazioni e campagne di influenza possono essere utilizzati per indebolire un Paese, colpire infrastrutture e condizionare i processi decisionali operando sotto la soglia del conflitto aperto.
Il documento indica, quindi, il rafforzamento delle capacità cyber e di contrasto alla guerra



ibrida, con lo sviluppo di un'Arma Cyber e la prospettiva di istituire un "Centro Nazionale ed Europeo per il Contrasto alla Guerra Ibrida" (previsto nel disegno di Legge presentato alla IV Commissione Esteri e Difesa del Senato). L'obiettivo è rafforzare il collegamento tra Difesa, istituzioni, ricerca, mondo accademico, industria e partner internazionali, superando la separazione tra settori che, nella competizione contemporanea, tendono invece a sovrapporsi.

La trasformazione tecnologica non può produrre effetti se non viene accompagnata da un'evoluzione del capitale umano. L'Atto considera il personale una capacità operativa e individua la necessità di intervenire sugli organici, sull'età media e sulle competenze disponibili.

La Difesa dovrà confrontarsi con una domanda crescente di professionalità nei settori dell'intelligenza artificiale, del cyber, dello spazio, dell'intelligence, delle tecnologie digitali, della logistica e dell'energia. Questa evoluzione richiede anche nuove modalità di reclutamento e formazione, capaci di integrare competenze militari e specialistiche.

Alla stessa esigenza risponde la prospettiva di una Riserva pronta, modulabile e integrata nello Strumento militare, nella quale possano confluire personale addestrato e professionalità provenienti anche dal mondo civile, scientifico e industriale. L'obiettivo è disporre di una capacità aggiuntiva rapidamente mobilitabile, in grado di aumentare la massa disponibile in funzione delle esigenze operative.

Uno dei passaggi più significativi riguarda il rapporto tra Difesa e industria perchè la base industriale della Difesa viene considerata una vera e propria capacità operativa. La possibilità di produrre, riparare, aggiornare e sostituire sistemi, componenti e munizionamento diventa una condizione della deterrenza, tanto quanto la disponibilità delle piattaforme.

La guerra ad alta intensità ha, infatti, mostrato i limiti di filiere costruite esclusivamente sulla minimizzazione delle scorte e sulla produzione "just in time". La resilienza richiede, invece, capacità produttive disponibili, subfornitori integrati, accesso alle materie prime e possibilità di aumentare rapidamente i volumi quando la situazione lo impone.



Questo principio incide anche sul procurement dove accelerare gli approvvigionamenti non significa soltanto ridurre i tempi amministrativi, ma intervenire sui requisiti, sull'interoperabilità e sugli standard, creando condizioni nelle quali più operatori industriali possano contribuire alla stessa architettura tecnologica. In questo quadro assumono rilievo anche gli strumenti europei, tra cui il programma SAFE, inseriti nella più ampia strategia di rafforzamento della base industriale e tecnologica della Difesa.

La velocità di trasformazione deve, infine, riguardare il trasferimento dell'innovazione dal laboratorio al campo. Intelligenza artificiale, calcolo avanzato, sistemi autonomi e tecnologie quantistiche sono destinati a incidere sulla pianificazione, sull'addestramento, sulla logistica e sui processi decisionali.

L'esperienza ucraina costituisce, anche sotto questo profilo, un elemento di riflessione. Il documento evidenzia, di fatto, la necessità di accorciare il ciclo che collega ricerca, sperimentazione, produzione e impiego operativo, favorendo un rapporto più diretto tra utilizzatori, industria e mondo della ricerca. Una tecnologia deve poter essere modificata e aggiornata sulla base delle esigenze riscontrate sul terreno, senza attendere necessariamente i tempi tradizionali dei grandi programmi.

Per ottenere questo risultato, deve cambiare anche il processo di pianificazione con un modello continuo e adattivo, nel quale le priorità possano essere aggiornate anche nel corso dell'anno, in funzione dell'evoluzione dello scenario e le risorse indirizzate verso gli obiettivi considerati strategici. La riduzione dei tempi amministrativi assume così una dimensione direttamente operativa perché se una minaccia o una tecnologia possono evolvere nell'arco di poche settimane, un processo decisionale, costruito esclusivamente secondo cicli molto più lunghi, rischia di non essere più adeguato al contesto nel quale deve operare.

La questione centrale diventa, quindi, il fattore tempo per cui, vedere prima, comprendere prima, decidere prima, produrre prima e adattarsi prima sono condizioni della capacità di poter prevenire e contrastare una minaccia che può evolvere più rapidamente dei tradizionali e ormai desueti cicli di pianificazione.

ATTO di INDIRIZZO del Ministro della Difesa

2026

Pdf Atto di Indirizzo del Ministero della Difesa 2026



LA NUOVA DIFESA GUARDA SEMPRE PIÙ AL PERSONALE

Tutele, benessere e nuove competenze

L'Atto di Indirizzo 2026 del Ministro della Difesa mette il personale al centro della trasformazione dello Strumento militare con una serie di interventi su trattamento economico e previdenziale, welfare, alloggi, sanità, formazione, carriere e reclutamento



Nell'Atto di Indirizzo per l'avvio del ciclo integrato di programmazione della performance e di formazione del bilancio di previsione per l'esercizio finanziario 2027 e la programmazione pluriennale 2028-2029, il personale viene indicato come una delle condizioni essenziali per rendere efficace, sostenibile e realmente impiegabile lo Strumento militare.
L'Atto sottolinea che il militare deve mantenere una condizione di prontezza, impiegabilità e disponibilità al servizio anche in presenza di rischio, fatica, disciplina e sacrificio superiori a quelli richiesti alla generalità dei cittadini. Da questa condizione deriva, secondo il documento, la necessità di rafforzare le tutele sul piano professionale, economico, previdenziale, sociale e giuridico.
Sul trattamento economico, l'Atto non stabilisce percentuali di aumento né nuove cifre in busta paga, indica invece la necessità di adeguare il trattamento alle professionalità e all'impegno effettivamente richiesti. Per la componente operativa, e in particolare per quella combat, dovrà essere studiato un trattamento distinto da quello del pubblico impiego ordinario. Il documento richiama anche i vincoli dell'orario, compreso il riferimento alle 36 ore settimanali, ritenuti poco compatibili con la piena disponibilità richiesta dallo status del militare.
In materia previdenziale, si pensa di valutare la possibilità di commisurare trattamento, contribuzione ed età pensionabile al "montante orario", cioè all'impegno effettivamente prestato, anziché considerare esclusivamente età e anzianità. È importante, al riguardo, distinguere l'indirizzo dalla norma: il montante orario non costituisce una nuova regola pensionistica già approvata perché il documento parla espressamente di una possibilità che dovrà

Capitale umano al centro

BENESSERE E RICONOSCIMENTO PROFESSIONALE

TRATTAMENTO ECONOMICO DIFFERENZIATO

Adeguamento specifico per la componente operativo e combat rispetto al pubblico impiego ordinario

CASA COME PILASTRO DELLA PRONTEZZA

Accesso agevolato agli alloggi per migliorare retention, morale e stabilità delle famiglie

VERSO IL "MONTANTE ORARIO"

Valutazione della previdenza basata sull'impiego effettivo prestato anzichè sulla sola anzianità



POTENZIAMENTO DELLA COMPONENTE CIVILE

PROCUREMENT E DIGITALE

Rafforzamento delle competenze tecniche e della continuità dei processi

SICUREZZA ENERGETICA

Gestione strategica delle risorse e delle infrastrutture critiche

AI Generate

2027-2029

INNOVAZIONE E SALUTE INTEGRATA





HUMAN READINESS LEVEL (HRL)

La maturità tecnologica è nulla senza personale addestrato a governarla efficacemente



SANITÀ MILITARE UNITARIA

Creazione di un sistema interforze con centri di alta specializzazione e medicina operativa



PROGETTO "DIFEASCOLTA"

Supporto logistico tempestivo per gestire disagio e situazioni familiari o sanitarie complesse

SUPPORTO OPERATIVO E ABILITANTE



LOGISTICA SPECIALISTICA

Supporto tecnico avanzato per il funzionamento globale dello Strumento Militare



INFRASTRUTTURE E SERVIZI

Modernizzazione delle basi, efficienza dei servizi e qualità della vita

Evoluzione professionale: dai talenti alle competenze strategiche

Reclutamento
Ringiovanire lo strumento militare e attrarre talenti specializzati nei domini tecnologici avanzati.

Formazione continua
Adattamento ai nuovi scenari. Percorsi professionali chiari, con formazione continua per acquisire nuove capacità.

Valutazione del merito
Oltre l'anzianità, valutazione basata su responsabilità, competenze e complessità dell'incarico.

L'integrazione della componente civile
Presenza crescente in funzioni dove la continuità professionale è critica. Focus sui settori: procurement, digitale, sicurezza energetica e logistica

La visione 2027-2029: il Personale come centro di gravità

"La modernizzazione della Difesa non passa solo dall'acquisizione di nuove tecnologie, ma dalla **creazione di condizioni professionali, sociali e previdenziali ottimali"**

Maturità tecnologica dei sistemi. L'acquisizione di nuove capacità non basta da sola

Technology Readiness Level

TRL + HRL =

Capacità reale del personale di utilizzare, adattare e governare la tecnologia in modo efficace e responsabile

Human Readiness Level

Sostenibilità, efficacia e reale impiegabilità dello strumento militare

1. Trattamento economico & Welfare
2. Ecosistema Alloggi/Sanità
3. Formazione & carriere
4. HRL ottimizzato

Ecosistema Vita: alloggi, mobilità e sanità militare



Sfida
Limitata disponibilità di alloggi nelle aree più popolate.

Intervento abitativo
Rinnovo patrimonio edile. Focus su efficienza energetica, sicurezza, salubrità. Tempi certi per manutenzioni

Supporto Mobilità
Supporto economico mirato per affrontare i costi della vita nei nuovi territori

Corpo di sanità unico

Direzione, unità, interfaccia e interoperabilità

Medicina operativa
Potenziamento delle strutture e mezzi d'urgenza per eventi ad alta intensità (con capacità di supporto alla popolazione)

Alta specializzazione
Centri di eccelenza per diagnostica, genomica e chirurgia d'urgenza. Accessibili a militari, veterani, famiglie e aperti al SSN

AI Generate

essere valutata. Lo stesso vale per il trattamento economico differenziato della componente operativa: l'Atto ne indica lo studio, non ne definisce ancora importi, modalità e decorrenza.
L'Atto poi comprende, nel perimetro del benessere, il trattamento economico e la previdenza, le tutele sociali, i servizi di sostegno, la copertura sanitaria integrativa per personale, famiglie e veterani, la qualità degli ambienti di lavoro, il supporto alla mobilità e un trattamento economico adeguato al costo della vita nelle diverse sedi di servizio, in Italia e all'estero.
La condizione abitativa assume un rilievo particolare perché ritenuta parte integrante del benessere e la collega a morale, retention e prontezza. L'obiettivo è agevolare l'accesso agli alloggi, soprattutto nelle aree più popolose dove la disponibilità limitata e i costi elevati incidono maggiormente sulla vita delle famiglie dei militari. Al riguardo, il patrimonio esistente dovrà essere rinnovato secondo criteri di qualità, sicurezza ed efficienza energetica, mentre la gestione dovrà garantire tempi certi per la manutenzione e standard di servizio chiari.
Altra problematica, alla quale si cerca di porre rimedio, è il trasferimento in una nuova sede di servizio che rappresenta una componente ordinaria della carriera militare e che può comportare costi differenti in funzione del territorio. Per questo l'Atto indica sia il supporto alla mobilità sia la necessità di un trattamento economico adeguato al costo della vita delle diverse sedi, comprese quelle all'estero.
La stessa impostazione viene applicata alla Sanità militare con l'attuazione della recente riforma verso un sistema sanitario militare unitario, interforze e interoperabile, fondato su un'unica Direzione della Sanità Militare e su un Corpo unico nel quale dovranno essere rivisitati i ruoli del personale sanitario.
La medicina operativa dovrà essere rafforzata, insieme alle strutture sanitarie di aderenza, cioè quelle più vicine alle unità impiegate, e ai mezzi medici d'urgenza. Il documento collega questo sviluppo alla capacità di operare in contesti multinazionali complessi e ad alta intensità, prevedendo anche capacità di protezione, cura ed eventuale evacuazione sanitaria a favore della popolazione civile.
Sul piano clinico, l'Atto indica, inoltre, la prosecuzione del progetto per creare centri di riferimento di alta specializzazione nei settori della diagnostica avanzata, della protesica e della chirurgia d'urgenza. Queste strutture dovranno servire innanzitutto veterani, militari in servizio e loro famiglie, ma potranno contribuire anche all'offerta del Servizio sanitario nazionale, mettendo a disposizione competenze specialistiche.
Sul benessere del personale spicca l'iniziativa "DifesAscolta", pensata per intercettare tempestivamente situazioni di disagio, in particolare quelle di natura psicologica e quelle legate a condizioni sanitarie e familiari complesse.
Sulla carriera e i sistemi di valutazione, l'obiettivo indicato è quello di costruire percorsi professionali più chiari, garantire formazione continua e introdurre sistemi di valutazione del merito, in grado di considerare responsabilità, competenze e complessità degli incarichi.
La trasformazione riguarda anche la composizione degli organici dove il Dicastero punta a intervenire sul reclutamento e sul dimensionamento dello Strumento militare, con l'esigenza di disporre di personale più giovane e di aumentare le competenze specialistiche, necessarie nei domini tecnologici avanzati.
Il rafforzamento delle competenze tecnologiche modifica anche il rapporto tra formazione e acquisizione delle capacità e non a caso il documento introduce il concetto di Human Readiness Level (HRL) accanto al Technology Readiness Level (TRL). Una tecnologia non è considerata realmente pronta soltanto perché il sistema ha raggiunto un determinato livello di maturità: occorre verificare anche che il personale sia in grado di utilizzarlo, adattarlo e governarlo in modo efficace e responsabile.
Anche la componente civile assume un ruolo crescente nel modello delineato dal documento con l'obiettivo di rafforzarne la presenza nelle funzioni nelle quali competenze specialistiche e continuità professionale risultano strategiche, tra cui "procurement", "digitale", "sicurezza energetica", "logistica" e altri settori tecnici specifici.
La modernizzazione della Difesa, nella prospettiva dell'Atto di indirizzo, non passa dunque soltanto dall'acquisizione di nuove capacità, ma anche dalla capacità di creare le condizioni professionali, formative, previdenziali e sociali necessarie alle donne e agli uomini chiamati a impiegarle.



Crosetto in Senato sulla riforma della Difesa

PLAY

Intervento del Ministro della Difesa Guido Crosetto alla IV Commissione Esteri e Difesa del Senato

Il Ministro della Difesa Guido Crosetto, agli inizi di ottobre, ha illustrato alla IV Commissione Esteri e Difesa del Senato il disegno di legge n. 2028 sul "rafforzamento e l'adeguamento della capacità di difesa nazionale". Il provvedimento nasce dall'esperienza operativa degli Stati maggiori, dei comandanti e del personale impegnato in Italia e all'estero e «non è la riforma del Ministro, non è la riforma di questa maggioranza, non è la riforma del Governo», ma «un punto di partenza» per adeguare lo Strumento militare, ha precisato il Ministro all'inizio del suo intervento. Il quadro di sicurezza è profondamente cambiato. Accanto ai domini tradizionali assumono un peso determinante, altri anbienti di competizione: cyber, spazio, spettro elettromagnetico, subacqueo, cognitivo informativo. Le minacce possono essere combinate e utilizzate simultaneamente, spesso «al di sotto della soglia tradizionale del conflitto». Per Crosetto la sfida è anche giuridica: occorre evitare il divario tra la velocità con cui cambiano minacce e tecnologie e quella con cui lo Stato adegua organizzazione, procedure e capacità di difesa. Una tecnologia può diventare obsoleta in mesi o settimane, mentre una professionalità richiede anni per essere formata. Sul fronte della minaccia ibrida il disegno di legge prevede il Centro Interforze per l'Addestramento e il Combattimento e il Contrasto della Minaccia Ibrida, alle dirette dipendenze del Capo di Stato Maggiore della Difesa, per l'analisi del rischio, lo sviluppo della dottrina e le esercitazioni multidominio. Nel cyber viene definito lo spazio cibernetico di interesse nazionale per la difesa e la sicurezza militare e introduce la figura dello «specialista cyber militare», con misure economiche, compreso l'incentivo anti-esodo, per trattenere competenze richieste dal mercato privato.

Un altro capitolo riguarda i sistemi senza equipaggio. Droni navali, subacquei e aerei sono già operativi, ma manca un quadro regolatorio adeguato. Il provvedimento interviene su classificazione, responsabilità di comando, abilitazione e regole d'impiego, dando «un fondamento giuridico flessibile a capacità che sono già operative».

> Al centro dell'audizione, la minaccia ibrida, il dominio cibernetico, i sistemi senza equipaggio, la dimensione interforze, l'innovazione tecnologica, la revisione delle procedure di acquisizione e il rapporto tra Difesa, industria, ricerca e università e la revisione delle procedure di acquisizione

La dimensione interforze attraversa la riforma. Le specificità delle singole Forze Armate devono essere preservate, ma i futuri vertici dovranno maturare esperienze trasversali e conoscere l'intero comparto. «L'interforze non può essere soltanto un principio organizzativo, deve diventare una cultura professionale» , precisa il Ministro.

Crosetto ha dedicato ampio spazio alla condizione del personale nei teatri operativi. «Un teatro operativo non può essere considerato sotto ogni profilo come un normale luogo di lavoro». La specificità della missione non significa ridurre le tutele: formazione, informazione,

addestramento, equipaggiamenti e norme tecnico-militari devono restare garantiti. Anche la responsabilità patrimoniale viene ridefinita: in caso di condotta colposa, l'azione risarcitoria del terzo viene indirizzata verso l'Amministrazione della Difesa, ferme le responsabilità del militare e l'eventuale rivalsa dello Stato. «Se non ha colpe, un comandante non può pagare personalmente per quello che ha fatto come comandante». La responsabilità penale resta distinta e ferma.

Il Ministro ha indicato, nelle procedure di acquisizione uno dei principali ostacoli all'efficienza. «Un processo di acquisizione adesso dura 4-5 anni» e può portare ad acquistare sistemi già superati. Sensoristica, guerra elettronica, sistemi senza equipaggio e intelligenza artificiale evolvono più rapidamente dei procedimenti amministrativi. «Il problema non è eliminare i controlli, ma costruire un sistema nel quale rapidità, sperimentazione, responsabilità e controlli possano convivere».

Il provvedimento rafforza il ruolo della Direzione Nazionale degli Armamenti, istituisce un Fondo per l'Efficientamento degli Investimenti della Ricerca Scientifica e Tecnologica Militare e sostiene la cooperazione Governo-Governo con gli Stati partner. Crosetto ha chiarito che «autonomia non deve essere confusa con autosufficienza»: significa poter scegliere con chi cooperare, evitando dipendenze da un'unica fonte e rafforzando la sicurezza delle catene di approvvigionamento.

Sul fronte della certificazione, oggi i tempi possono arrivare a due o tre anni. Il ricorso, quando previsto, a università, centri di ricerca ed enti certificatori esterni dovrebbe accelerare i processi e rafforzare il rapporto tra Difesa, ricerca e industria. In questa logica nasce il «Fast Prototyping», per sviluppare, sperimentare e validare rapidamente nuove soluzioni, coinvolgendo direttamente gli utilizzatori e riducendo la distanza tra innovazione e capacità operativa.

La riforma interviene inoltre sulle opere della Difesa e sulle procedure ambientali. La tutela dell'ambiente resta un interesse pubblico fondamentale, ma per infrastrutture esclusivamente destinate alla difesa potranno essere previste soluzioni specifiche quando le procedure ordinarie rischiano di compromettere l'obiettivo. «Io devo fare un bunker che non ho e non posso pensare ad avere gli stessi tempi di approvazione che ho per fare una casa privata».

Il tema degli organici non è stato abbandonato, ma sarà affrontato con un secondo disegno di legge, separato dalle norme tecniche e ordinamentali, perché gli incrementi strutturali richiedono coperture pluriennali. Restano nel percorso complessivo organici, riserva, specificità, infrastrutture e alloggi, compresa l'ipotesi di incremento fino a 40.000 unità.

Nelle conclusioni Crosetto ha ribadito che il testo non è definitivo e dovrà essere migliorato dal Parlamento. «Noi dobbiamo costruire un Paese che sappia adeguarsi a qualunque tipo di minaccia nei tempi più rapidi possibili». La minaccia è passata dal piano fisico al cyber e alla disinformazione e potrebbe arrivare, in futuro, ad agenti virtuali non più controllati dall'uomo.

«Sto proponendo una legge che non userò io come Ministro», ha sottolineato Crosetto. È una legge costruita «per il Paese», destinata a chi verrà dopo e pensata per garantire maggiore operatività, tutelare il personale e rafforzare la capacità della Repubblica di difendere «il Paese, le sue libere istituzioni, la democrazia».

«la Difesa deve correre alla velocità delle minacce»

Guido Crosetto - Ministro della Difesa

Intervento del
Gen. Portolano
Capo Stato
Maggiore della Difesa

Intervento del
Gen. C.A. Masiello
Capo Stato
Maggiore dell'Esercito

Intervento del
Amm. Sq. Berutti Bergotto
Capo Stato
Maggiore della Marina

Intervento del
Gen. S.A. Conserva
Capo Stato
Maggiore dell'Aeronautica

Intervento del
Gen. C.A. Luongo
Comandante Generale
dell'Arma dei Carabinieri

Le risorse per la Difesa Gli strumenti dell'Unione Europea



Le crisi internazionali, l'impegno assunto nella NATO e l'emergere di minacce militari, economiche e tecnologiche impongono all'Italia di ripensare il proprio modello di Difesa. La questione non è scegliere tra Difesa, Sanità o Scuola, ma trovare le risorse per garantire "insieme" difesa, sicurezza e prosperità

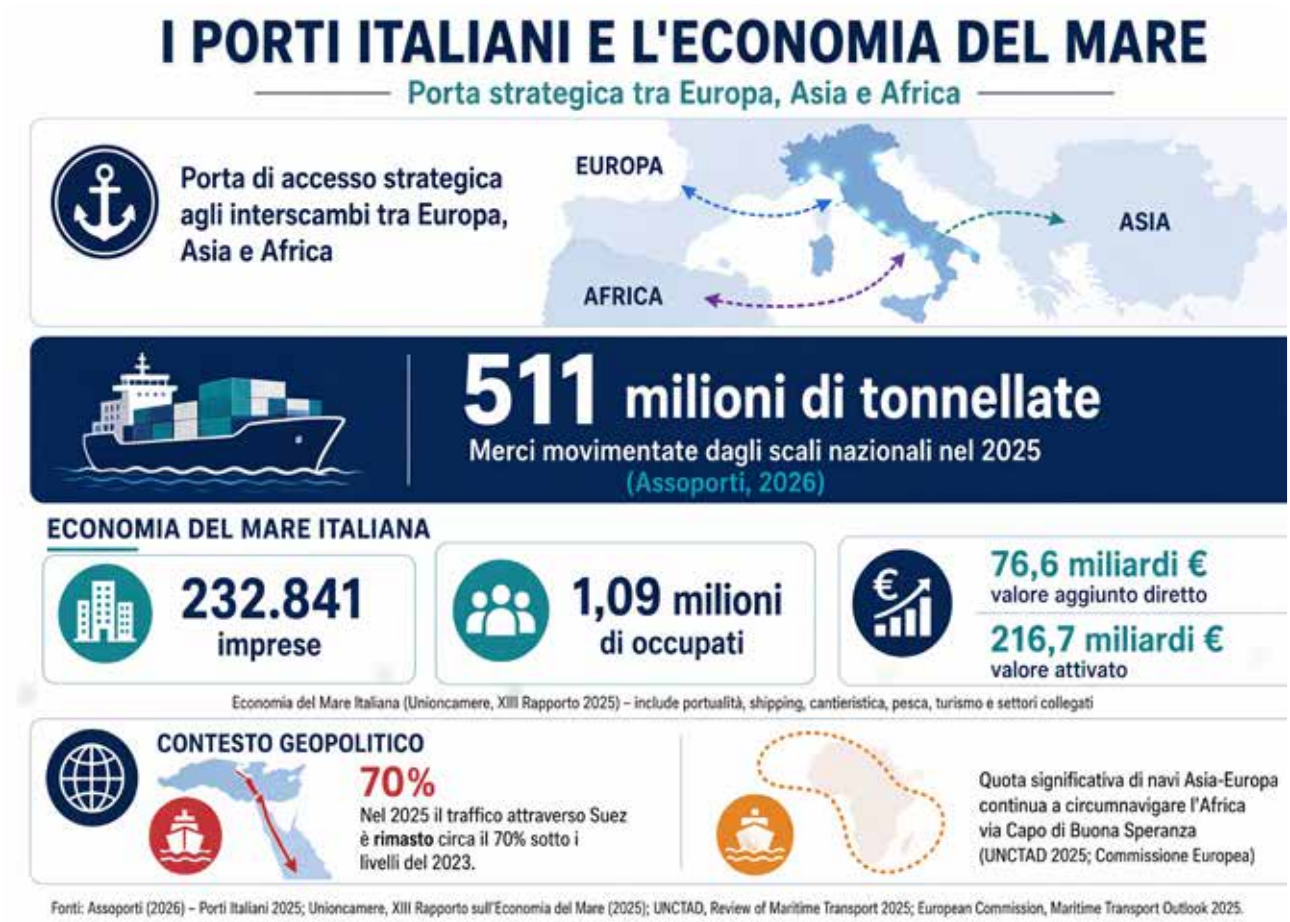
La Difesa italiana si trova oggi davanti a una doppia sfida, da una parte una situazione economica complessa, aggravata dalle crisi internazionali e dalla necessità di sostenere le diverse priorità dello Stato, dall'altra, uno scenario di sicurezza profondamente cambiato, che impone nuove capacità militari, maggiore prontezza operativa e strumenti adeguati per affrontare minacce sempre più diversificate e sofisticate.

Al vertice NATO dell'Aia di giugno 2025, gli Alleati hanno assunto l'impegno di portare, entro il 2035, gli investimenti complessivi per la Difesa e Sicurezza al 5% del Pil. Il 3,5%, destinato alle esigenze militari fondamentali ("spese core"), mentre l'1,5% ad attività più ampie, connesse alla sicurezza e protezione delle infrastrutture critiche del Paese, nonché all'innovazione e allo sviluppo della base industriale.

La Difesa deve, pertanto, garantire deterrenza, prontezza operativa e resilienza, contribuire alla difesa collettiva dell'Alleanza e dell'Unione Europea e, contemporaneamente, proteggere gli interessi nazionali, anche lontano dai propri confini.

Per un Paese manifatturiero e commerciale come l'Italia, la libertà di navigazione non è soltanto un principio di diritto internazionale, ma una condizione concreta per l'approvvigionamento energetico, l'arrivo delle materie prime, l'esportazione dei prodotti e il funzionamento delle catene logistiche.

Un prolungamento delle restrizioni a Bab el-Mandeb e Suez, insieme a ulteriori limitazioni nello Stretto di Hormuz, potrebbe rendere più frequente il ricorso a rotte alternative e modificare la geografia dei traffici. In questo scenario, potrebbero rafforzarsi i grandi hub del Nord Europa, in particolare Rotterdam, Anversa-Bruges e Amburgo, che nel 2024 erano rispettivamente i primi tre porti dell'Unione Europea per tonnellate movimentate (Eurostat), mentre i porti mediterranei rischierebbero di perdere parte del vantaggio, derivante dalla loro posizione nel Mediterraneo, sulle rotte Asia-Europa.



«Il programma SAFE, per come è stato impostato, è uno strumento di finanziamento della spesa militare, non aggiuntivo di quella prevista a bilancio»

**Ministro della Difesa Guido Crosetto,
alle Commissioni Esteri e Difesa di Camera e Senato,
Roma 28 luglio 2026**

Lo stesso vale per lo spazio, le telecomunicazioni, i cavi sottomarini, le reti energetiche, gli aeroporti e le infrastrutture digitali. Un attacco cyber contro un'infrastruttura critica, un'interferenza satellitare, un'interruzione delle comunicazioni o un'azione di sabotaggio possono produrre effetti economici e sociali ben prima che si manifesti una minaccia militare tradizionale. Parliamo, in tal senso, della cosiddetta guerra ibrida, caratterizzata da attacchi plurimi in diversi domini e ambienti di confronto, evitando per la loro caratteristica sottosoglia, l'imputabilità.

Considerate le minacce in corso e quelle emergenti, il concetto stesso di spesa per la Difesa non può essere relegato ad una funzione strettamente necessaria all'operatività delle Forze Armate. Ciò, poiché l'impegno finanziario coinvolge l'industria, l'intelligence, la ricerca scientifica, le università, il sistema energetico, le infrastrutture critiche, le telecomunicazioni, la cybersicurezza e la capacità complessiva del Paese di produrre tecnologie strategiche. Per questo motivo, l'obiettivo è quello di creare un sistema nel quale una parte della spesa pubblica destinata alla Difesa produca, contemporaneamente, capacità militari, innovazione tecnologica, competenze, occupazione qualificata e resilienza delle filiere produttive.

In una congiuntura internazionale "fluida e non prevedibile", la finanza pubblica italiana continua, comunque, ad essere sottoposta ai vincoli di bilancio europei, con la necessità di dover sostenere, comunque, spese incomprimibili come sanità, istruzione, previdenza, infrastrutture e sviluppo economico. In questo quadro, sarebbe riduttivo contrapporre le spese per la Difesa alle altre previste per altre funzioni essenziali dello Stato, come se fosse "necessario" scegliere tra difesa militare e altri servizi pubblici.

La soluzione più ragionevole è quella di stabilire una politica economica sostenibile, per riuscire a finanziarle tutte, senza compromettere le capacità militari per la difesa nazionale. Per questo motivo, per le spese in Difesa e Sicurezza energetica sono stati pensati strumenti di flessibilità che svincolano la finanza pubblica nazionale dalle rigide regole di bilancio comunitarie. L'Italia ha, di fatto, chiesto l'attivazione della "clausola nazionale di salvaguardia" (National Escape Clause) per il periodo 2026-2028. La clausola consente di non calcolare questi fondi nel computo del rapporto deficit/Pil che, per le regole UE (c.d. Fiscal Compact), non deve superare il 3% del Pil.

Ma come si possono finanziare le spese per la Difesa, senza incidere sul bilancio ordinario dello Stato, nel breve medio termine? Sempre l'UE, per favorire il raggiungimento degli obiettivi del piano "Readiness 2030", ha messo in campo una serie di strumenti finanziari, uno fra tutti il SAFE (Security Action for Europe), con 150 miliardi di euro, messi a disposizione ai Paesi richiedenti.

Nel caso italiano, l'utilizzo del SAFE è collegato a programmi di investimento per la Difesa, già inseriti nella programmazione approvata dal



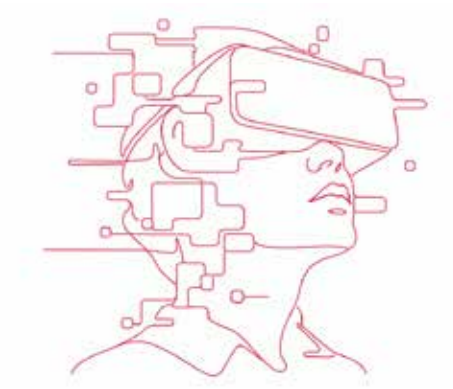
Il piano Readiness 2030 fa parte della strategia di difesa militare comunitaria proposta dalla presidente della Commissione europea Ursula von der Leyen a marzo 2025, per rafforzare le capacità di deterrenza e la prontezza strategica dell'Unione Europea entro il 2030

Parlamento. Il ricorso al SAFE non serve, quindi, per nuova spesa militare, c.d. spesa aggiuntiva, ma serve a rendere finanziariamente sostenibili gli investimenti già decisi. I finanziamenti del SAFE possono arrivare a una durata massima di 45 anni, con un periodo di "grazia" fino a dieci anni sul rimborso del capitale. Non si tratta, quindi, di un finanziamento a breve termine e i dieci anni non rappresentano la durata complessiva del prestito. Il tasso non è invece predeterminato in modo uniforme per tutti gli Stati, perché le condizioni finanziarie dipendono dal mercato finanziario del momento e dai singoli accordi di prestito con i diversi Stati membri.

SAFE e Clausola di Salvaguardia svolgono, pertanto, funzioni differenti, il primo modifica il canale attraverso cui possono essere finanziati determinati investimenti, mettendo a disposizione prestiti europei di lungo periodo, la seconda interviene, invece, sulle regole del percorso di aggiustamento della spesa pubblica, consentendo una flessibilità temporanea per le uscite destinate agli investimenti per il comparto Difesa.



MASSIMILIANO D'ELIA



È guerra ibrida

Una democrazia resiliente non è quella che non subisce attacchi ma è quella che riesce a riconoscere l'attacco, attribuirlo con sufficiente rapidità, comunicare informazioni attendibili e impedire che la paura produca decisioni irrazionali



Il 4 agosto 2026, il ritrovamento di un drone carico di esplosivo all'aeroporto di Lipsia/Halle, apparentemente destinato a colpire un aereo cargo ucraino, ha riportato al centro dell'attenzione la crescente minaccia della guerra ibrida russa in Europa. Il 1° settembre il governo tedesco ha attribuito alla Russia la responsabilità del tentato attacco, sulla base delle indagini di polizia, delle informazioni raccolte dai servizi di sicurezza e delle modalità operative individuate. Berlino ha inserito, l'episodio in un quadro più ampio di sabotaggi, cyberattacchi, interferenze elettromagnetiche e operazioni clandestine.

È proprio nella combinazione di queste azioni che si trova uno dei punti di forza della guerra ibrida: colpire senza esporsi, agire attraverso soggetti intermedi e rendere più complessa l'attribuzione dell'operazione. La cosiddetta "plausible deniability" che consente, infatti, all'autore di un'operazione ostile di rendere difficile l'attribuzione, mantenendo l'azione in quella zona di ambiguità strategica che viene definita "zona grigia", cioè al di sotto della soglia che prevede la "risposta armata".

Dietro questo modello di guerra "invisibile", opera un ecosistema composto da strutture dell'intelligence militare e civile, apparati di influenza e propaganda, gruppi cyber, contractor e intermediari esteri. All'interno del GRU, l'intelligence militare russa, esiste l'Unità 29155, che opera a stretto contatto con diversi gruppi hacker, uno fra tutti il Cadet Blizzard che risulta, tra l'altro, tra quelli sanzionati dall'Unione Europea per il coinvolgimento in attività cyber contro organizzazioni governative ucraine, e per aver preso di mira Stati membri dell'UE e Alleati NATO. L'UE ha, inoltre, sanzionato anche il "142nd

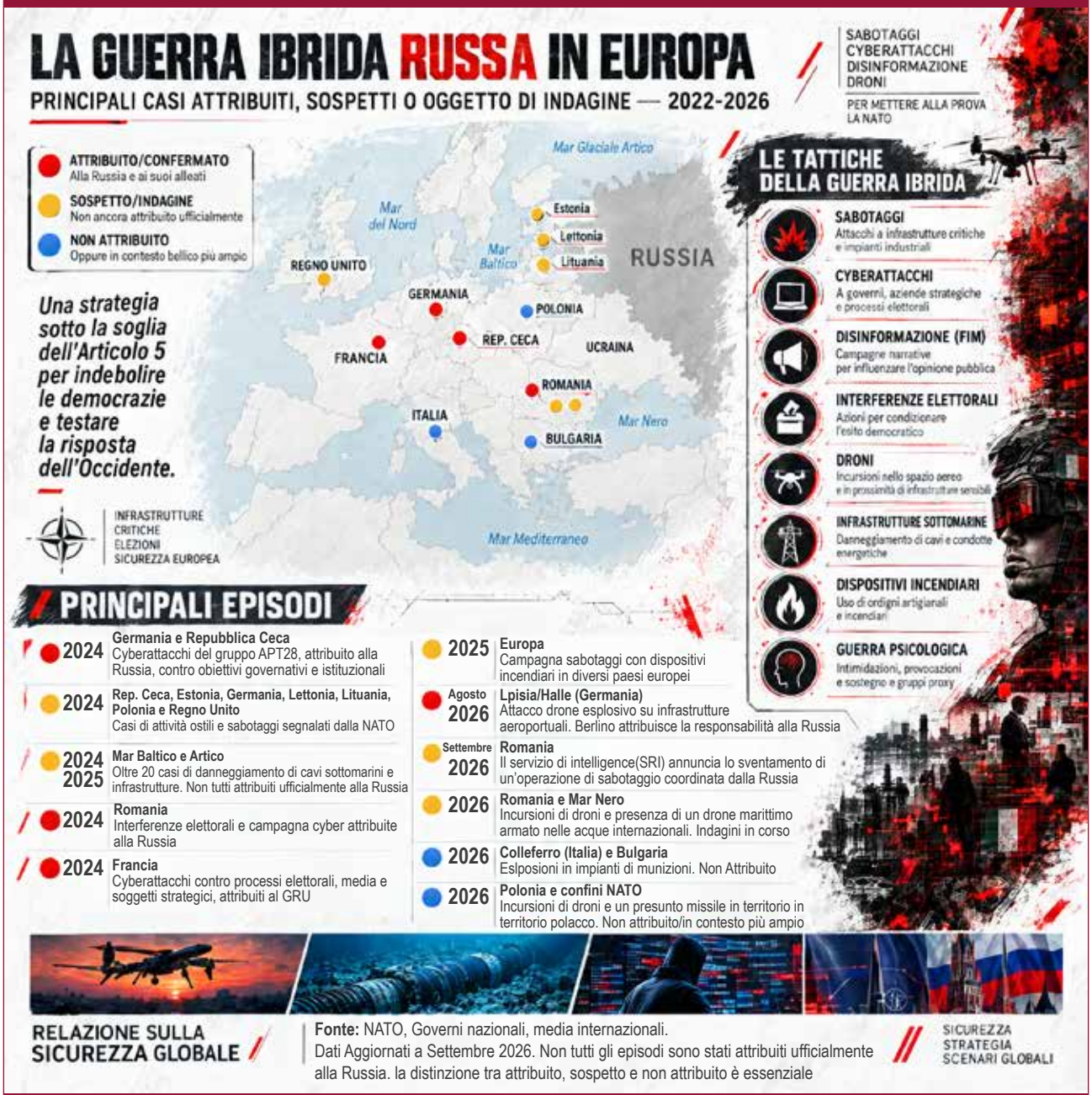
Separate Electronic Warfare Battalion", con sede nella regione di Kaliningrad, collegandolo ad attività di guerra elettronica (disturbing e spoofing dei segnali GPS), che hanno interessato soprattutto l'area degli Stati baltici.
Il 31 agosto 2025, l'aereo che trasportava la presidente della Commissione europea Ursula von der Leyen, in avvicinamento a Plovdiv, in Bulgaria, registrò un'interferenza del segnale GPS. L'episodio venne ricondotto dalle autorità bulgare a un possibile disturbo di origine russa, mentre la Commissione Europea ha poi confermato l'interferenza.

«La minaccia ibrida è una guerra continua che ci colpisce, giorno e notte, ogni giorno. Prende di mira le nostre infrastrutture critiche, i servizi essenziali, le industrie strategiche, le reti di comunicazione, le istituzioni democratiche, minando la fiducia dei cittadini e la stabilità stessa del Paese. Non siamo di fronte a un rischio potenziale, ma a un'aggressione costante che non conosce tregua e non conosce confini».

Camera dei deputati, 12 novembre 2025
Intervento del Ministro della Difesa Guido Crosetto

Secondo un'inchiesta di Reuters del 10 settembre 2026, Regno Unito, Norvegia e Stati Uniti hanno individuato nel Nord Atlantico un'attività del GUGI (Main Directorate of Deep-Sea Research), l'unità russa specializzata nelle operazioni subacquee, durante la quale sarebbero state testate nuove capacità per danneggiare o mettere fuori uso cavi sottomarini. Secondo la ricostruzione di Reuters, l'attività è stata intercettata e nessun cavo è stato danneggiato.
Una delle recenti evoluzioni più preoccupanti della metodologia russa, per compiere operazioni clandestine in Europa, riguarda il reclutamento attraverso social network, piattaforme di gioco e servizi di messaggistica, con la promessa di pagamento in denaro, in contanti o tramite criptovalute. Si tratta di comuni cittadini che possono essere coinvolti in attività apparentemente semplici, come la produzione di fotografie, video o la raccolta di informazioni, senza necessariamente conoscere il committente finale. Il servizio di sicurezza danese PET, nel settembre 2026, ha rilevato attività concrete di pianificazione e preparazione di sabotaggi russi in Danimarca, rivolte soprattutto ad aziende della difesa e ad imprese collegate al sostegno militare all'Ucraina. Il PET ha, inoltre, documentato tentativi di reclutamento attraverso social network, piattaforme di gaming e Telegram.
Tra i casi più documentati c'è quello statunitense di "Tenet Media", attraverso il quale, secondo il Dipartimento di Giustizia americano, due dipendenti di RT, l'emittente statale russa, hanno trasferito quasi 10 milioni di dollari attraverso società-schermo, per finanziare la produzione di migliaia di contenuti fake destinati al pubblico statunitense.
Altre campagne di disinformazione, come Doppelgänger e Storm-1516, attive dalla metà del 2022, mostrano l'evoluzione nel tempo delle tecniche russe di manipolazione dell'informazione. La prima campagna ha utilizzato soprattutto la clonazione di siti e testate occidentali per diffondere contenuti falsi o manipolati; la seconda, ha sviluppato una rete di siti, account e contenuti costruiti ad arte per alimentare e amplificare false narrazioni, anche attraverso video e materiali apparentemente giornalistici.
Il 21 aprile 2026, Bruxelles ha inserito nella lista delle entità sottoposte a sanzioni anche la piattaforma filorussa "Euromore" e la "Foundation for the Support and Protection of the Rights of Compatriots Living Abroad", Pravfond, accusate di svolgere un ruolo attivo nelle attività russe di

Non occorre far credere a tutti una stessa versione dei fatti, spesso è sufficiente produrre un numero sufficiente di versioni alternative per rendere difficile stabilire quale sia quella vera



Cosa può fare uno Stato per la sua resilienza democratica

Rafforzare i sistemi di early warning, proteggere infrastrutture e processi elettorali, contrastare disinformazione e interferenze straniere, garantire la continuità delle funzioni essenziali dello Stato. Decisivi sono il coordinamento tra Istituzioni, Difesa, Intelligence, industria e società civile, la formazione dei cittadini e una comunicazione pubblica tempestiva e credibile

manipolazione delle informazioni, propaganda e influenza.
Nell'agosto del 2026, OpenAI ha individuato e bloccato un gruppo di account ChatGPT, riconducibili alla Russia, utilizzati per promuovere l'International Burke Institute, una sedicente organizzazione con sede in Israele. Secondo OpenAI, gli operatori utilizzavano ChatGPT per generare contenuti destinati a social network e piattaforme online, cercando contemporaneamente di nascondere la propria origine.
Di fronte a una minaccia, quella della guerra ibrida, meno evidente e immediatamente letale rispetto a un conflitto tradizionale, NATO, Unione Europea e singoli Paesi hanno adottato misure diverse di prevenzione e resilienza. Le risposte sono state organizzate, in alcuni casi in modo centralizzato, in altri, come in Italia, attraverso un modello interministeriale e interagenzia che coinvolge più strutture e competenze.
Sul piano strategico, nel novembre 2025 il Ministro della Difesa Guido Crosetto ha presentato

Il Copasir ha acceso l'allerta sulle possibili interferenze straniere nel prossimo ciclo elettorale

Ansa , 09 settembre 2026

al Consiglio Supremo di Difesa il non-paper "Il contrasto alla guerra ibrida: una strategia attiva". A questo si aggiunge la "Strategia digitale della Difesa 2026-2030", orientata a rafforzare la capacità di operare in un ambiente digitale complesso e a sviluppare un approccio integrato con le altre amministrazioni dello Stato. La Strategia, emanata nel 2026, individua tra i propri pilastri la valorizzazione del dato, la connettività e la sicurezza nel dominio cibernetico.
La Difesa italiana, nel disegno di legge di riforma della Difesa, presentato al Consiglio dei Ministri il 7 agosto, prevede un "Centro interforze di addestramento per il combattimento e il contrasto alla minaccia ibrida". Tale Centro, posto alle dirette dipendenze del Capo di Stato Maggiore della Difesa, si pone l'obiettivo di sviluppare capacità comuni tra le Forze Armate per affrontare scenari nei quali cyberattacchi, guerra elettronica, campagne di disinformazione e operazioni militari tradizionali agiscono in maniera integrata.
L'Unione Europea, attraverso l'EU Hybrid



Crosetto sul deep fake:
«.....prima di credere a quello che vediamo sui social, chiediamoci sempre chi lo ha creato. Anche l'informazione va difesa.
Perché il falso non è mai sembrato così vero».

Così, in un video pubblicato sui canali social del Ministero della Difesa, appositamente rigenerato con l'intelligenza artificiale, in cui si vede la figura del Ministro che in un passaggio dice:

«Ciò che vediamo può sembrare assolutamente reale.
Per le informazioni ufficiali, affidiamoci ai canali ufficiali».

Link video fake Ministro della Difesa Guido Crosetto

I PRINCIPALI GRUPPI CYBER ATTRIBUITI ALLA RUSSIA
E I LORO LEGAMI CON L'APPARATO DI SICUREZZA RUSSO

CYBER
SPAZIO
INFORMAZIONE
POTERE

STRUMENTI DIGITALI
PER OBIETTIVI GEOPOLITICI



GRU
INTELLIGENCE MILITARE

Unità responsabile delle operazioni cyber offensive, del sabotaggio e delle attività di intelligence militare.

APT28
Alias: Fancy Bear, Forest Blizzard, Sofacy, Sednit, Strontium

Attività principale: spionaggio, operazioni di influenza

Principali bersagli: governi, NATO, processi elettorali, settore difesa

Attività globali

Sandworm
Alias: Voodoo Bear, Seashell Blizzard, APT44, Iridium

Attività principale: sabotaggio, attacchi distruttivi

Principali bersagli: infrastrutture critiche (energia, trasporti, telecomunicazioni), forze armate

Attività globali (in particolare Ucraina e Paesi NATO)

SVR
INTELLIGENCE ESTERA

Raccoglie informazioni all'estero e conduce operazioni di spionaggio globale.

APT29
Alias: Cozy Bear, Midnight Blizzard, Nobelium, Yttrium, UNC2452

Attività principale: spionaggio, furto di dati, accesso a lungo termine

Principali bersagli: governi, think tank, organizzazioni internazionali, settore tecnologico e sanitario

Attività globali

FSB
SICUREZZA INTERNA

Responsabile di controspionaggio, controllo interno e operazioni cyber.

Gamaredon
Alias: Actinium, Aqua Blizzard, Primitive Bear, UAC-0010

Attività principale: spionaggio, phishing, raccolta di informazioni

Principali bersagli: enti governativi, militari (soprattutto Ucraina)

Attività regionale (focalizzata su Ucraina)

Turla
Alias: Snake, Uroburos, Venomous Bear, Secret Blizzard, Krypton

Attività principale: spionaggio, ricognizione, accesso a lungo termine

Principali bersagli: governi, ambasciate, settore difesa, ricerca

Attività globale

Energetic Bear
Alias: Dragonfly, Berserk Bear, Crouching Yeti, Ghost Blizzard

Attività principale: spionaggio e preparazione di operazioni contro infrastrutture critiche

Principali bersagli: energia, manifattura, aviazione, difesa, settori industriali

Attività globale

Altri gruppi
ATTRIBUTI ALLA RUSSIA

Gruppi con forti attribuzioni russe, attivi in operazioni cyber e di influenza.

Callisto
Alias: Seaborgium, Star Blizzard, ColdRiver, BlueCharlie, TA446

Attività principale: spionaggio, phishing, operazioni di influenza

Principali bersagli: governi, settore difesa, organizzazioni internazionali

Attività globale

Cadet Blizzard
Alias: DEV-0568

Attività principale: operazioni distruttive

Principali bersagli: infrastrutture critiche

Attività regionale (Ucraina ed Europa)

Indrik Spider
Alias: Manatee Tempest, DEV-0243

Attività principale: operazioni cyber

Principali bersagli: governi, difesa

Attività globale

Storm-1516
Alias: CopyCop, New Flood

Attività principale: operazioni di influenza

Principali bersagli: opinione pubblica, processi elettorali

Attività globale

Storm-1679
Alias: Ruza Flood

Attività principale: operazioni di influenza

Principali bersagli: Paesi occidentali

Attività globale

PRINCIPALI TIPI DI ATTIVITÀ

- Spionaggio e furto di dati
- Sabotaggio e attacchi distruttivi
- Attacchi a infrastrutture critiche
- Operazioni di influenza (FIM)
- Phishing e accesso iniziale
- Ricognizione e preparazione operativa

PRINCIPALI SETTORI BERSAGLIO

- Governi e istituzioni
- Difesa e militare
- Energia
- Trasporti
- Telecomunicazioni
- Industria manifatturiera
- Settore tecnologico
- Sanità e ricerca

PRINCIPALI AREE GEOGRAFICHE DI ATTIVITÀ



- Russia (base operativa)
- Paesi principalmente colpiti
- Altre aree di attività



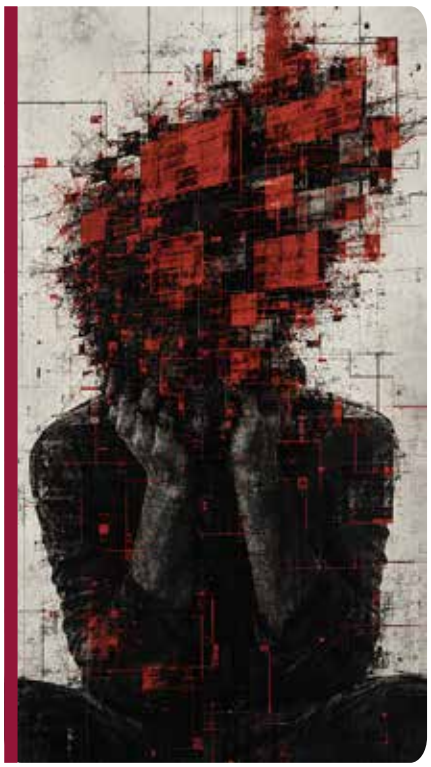


LA GUERRA IBRIDA RUSSA

SICUREZZA
STRATEGIA
SCENARI GLOBALI

AI Generate

Toolbox, coordina misure preventive, di resilienza, cooperazione, sostegno e sanzione. Al suo interno operano il FIMI Toolbox, contro la manipolazione delle informazioni e le ingerenze straniere, il Cyber Diplomacy Toolbox, per la risposta alle minacce e agli attacchi informatici, e gli Hybrid Rapid Response Teams, capaci di fornire rapidamente assistenza agli Stati colpiti.
A livello NATO, si parla di "Cognitive Warfare" e della possibilità di considerare il dominio umano/cognitivo nell'evoluzione futura del concetto multidominio, ma non esiste ancora attualmente il riconoscimento di un reale "sesto dominio operativo" dell'Alleanza. La stessa documentazione descrive il Cognitive Warfare come un ambito in fase di studio e sviluppo concettuale. Nel Vertice di Vilnius del luglio 2023, l'Alleanza ha precisato che le operazioni ibride contro un Paese membro possono raggiungere il livello di un attacco armato e, in determinate circostanze, condurre all'invocazione dell'Articolo 5 (un attacco armato contro un Paese membro della NATO è considerato un attacco contro tutti gli Alleati). Per quanto riguarda, invece, il dominio cyber, la NATO aveva già stabilito nella "Comprehensive Cyber Defence Policy del 2021", che anche l'effetto cumulativo di attività informatiche malevole significative può, in determinate circostanze, essere considerato alla stregua di un attacco armato.
Il nodo più delicato riguarda però il passaggio dalla difesa all'iniziativa perchè oggi, il contrasto alla guerra ibrida è ancora concentrato soprattutto sulla prevenzione, sulla protezione delle infrastrutture e sulla resilienza.
La sfida per i Paesi occidentali è quindi sviluppare anche la capacità di individuare, attribuire e contrastare le operazioni ostili, prima che producano i loro effetti, arrivando, quando necessario e nel rispetto del diritto internazionale, a colpire le capacità con cui l'avversario conduce la propria guerra ibrida.



«Sulla guerra ibrida noi, nei paesi occidentali, non stiamo facendo molto, la subiamo e basta, perché la guerra ibrida è una guerra strana in cui o reagisci e in qualche modo la porti dall'altra parte, cosa che non abbiamo mai voluto fare, oppure la subisci e cerchi di difenderti, noi lo facciamo di fronte a centinaia di attacchi quotidiani, ad esempio cyber, o lo facciamo nel tentativo di fermare una disinformazione che è sempre più forte e costante»

Guido Crosetto - Ministro della Difesa
Sky Tg24 , 21 settembre 2026

Fonti
- UK Government, Profile: GRU cyber and hybrid threat operations, 2025. UK Government – Profile: GRU cyber and hybrid threat operations
- FBI – CISA – NSA, Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure, 5 settembre 2024. CISA – Joint Cybersecurity Advisory
- U.S. Department of Justice, Five Russian GRU Officers and One Civilian Charged with Conspiring to Hack Ukrainian Government, 5 settembre 2024. U.S. Department of Justice
- European Union – EUR-Lex, Council Implementing Regulation (EU) 2025/2568, 12 dicembre 2025. EUR-Lex – EU sanctions concerning Unit 29155/Cadet Blizzard
- European Union – EUR-Lex, Council Decision (CFSP) 2024/2643, testo consolidato al 13 luglio 2026. EUR-Lex – EU restrictive measures

MASSIMILIANO D'ELIA



"A tu per tu con Maurizio Molinari"

Le notizie raccontano ciò che accade. "Oltre la Notizia" prova a spiegare perché accade. In questo spazio ID apre un confronto diretto con Maurizio Molinari per entrare nel cuore dei grandi dossier geopolitici e offrire chiavi di lettura utili a orientarsi, in uno scenario sempre più complesso.

La guerra ibrida è già in Europa





«Le minacce ibride che affronta l'Europa sono sempre meno ibride e sempre meno minacce». La presidente della Commissione europea ha citato «cyberattacchi, sabotaggi, incendi dolosi e incursioni di droni», sottolineando che «stanno aumentando ogni giorno». Sul caso Lipsia ha parlato di un «attacco con materiale di livello militare, condotto da operativi russi sul territorio europeo»

Ursula von der Leyen - Commissione europea discorso sullo Stato dell'Unione 2026.

La guerra ibrida è già dentro i confini europei con sabotaggi, cyberattacchi, sconfinamenti di droni e caccia militari, campagne di disinformazione e operazioni di influenza che, non sono più fenomeni episodici, ma strumenti di una competizione che si svolge sotto la soglia del conflitto dichiarato.
L'episodio del mancato attentato al velivolo cargo ucraino, all'aeroporto di Lipsia, rappresenta un "unicum" perché per la prima volta uno Stato, la Germania, ha attribuito la responsabilità di un attacco sotto soglia ad un altro, la Federazione russa che ne ha poi però smentito la paternità.
In vista di una stagione elettorale che nel 2027 coinvolgerà diversi Paesi europei, Italia compresa, la vulnerabilità non riguarda soltanto infrastrutture e sistemi informatici ma riguarda anche la capacità delle società democratiche di riconoscere e contrastare manipolazioni, interferenze e campagne costruite per alimentare paura, sfiducia e divisioni.
Di tutto ciò, ne parliamo con Maurizio Molinari, direttore editoriale del Gruppo SAE, per comprendere come sta evolvendo la minaccia russa e quali strumenti l'Europa può mettere in campo per difendere la propria sicurezza e, insieme, la qualità del dibattito pubblico.

La Germania ha fatto un salto di qualità accusando ufficialmente la Russia del tentativo di attacco con droni all'aeroporto di Lipsia, parlando apertamente di guerra ibrida. Che cosa ci dice questo episodio sull'evoluzione della minaccia russa verso l'Europa?

"Lipsia segna il passaggio dalla negazione alla consapevolezza. La sera del 4 agosto un drone con esplosivo è stato ritrovato nello scalo, vicino ad alcuni aerei cargo ucraini, in un aeroporto spesso utilizzato per trasferire aiuti destinati all'Ucraina. Il bersaglio non è casuale: colpire la logistica del sostegno a Kiev significa alzare il costo della solidarietà europea.
Il salto di qualità è doppio. Sul piano operativo, secondo Berlino la tecnologia impiegata era di livello professionale e l'operazione ha richiesto competenze tecniche elevate e un notevole sforzo organizzativo. Sul piano politico, il ministro Dobrindt ha detto che la Germania non è in guerra ma subisce ogni giorno attacchi ibridi, e che Lipsia non è un evento isolato ma parte di un quadro più ampio. Mosca respinge le accuse e Putin sostiene addirittura che Berlino abbia falsificato le prove ma la dinamica è chiara: la Russia sposta l'asticella dal sabotaggio di disturbo ad azioni potenzialmente letali, testando fino a dove l'Europa è disposta a tollerare senza reagire. L'obiettivo non è vincere una battaglia ma convincere le opinioni pubbliche che sostenere l'Ucraina rende insicure le loro città".

Dopo la denuncia tedesca sono emersi sospetti anche su altri episodi contro infrastrutture energetiche, depositi di armi e munizioni in Europa, seguiti da cyberattacchi, sconfinamenti di droni/velivoli e interferenze via social. È ancora corretto parlare di episodi separati, oppure dobbiamo considerarli come parti di un'unica strategia russa contro la sicurezza europea?

"Continuare a parlare di episodi isolati significa fare il gioco di Mosca. La forza della guerra ibrida sta proprio nella frammentazione: un incendio in un deposito, un cavo sottomarino tranciato, un drone su una base, un attacco informatico a un ospedale, una campagna social. Presi singolarmente sembrano incidenti, guasti o atti di criminalità comune; messi in fila disegnano una mappa coerente. Colpiscono energia, logistica militare, trasporti e fiducia nelle istituzioni, cioè i quattro pilastri su cui poggia la capacità europea di aiutare Kiev.
La logica è quella della "zona grigia": restare sotto la soglia che farebbe scattare l'articolo 5 della Nato, mantenere la negabilità attraverso intermediari reclutati online, piccoli criminali o proxy, e accumulare pressione. Il fine strategico è dividere: tra Stati più esposti e Stati più lontani dal fronte, tra governi e cittadini, tra chi chiede fermezza e chi invoca il "dialogo" pur di far cessare la paura. Un'Europa che litiga su come rispondere è già un'Europa più debole".

Il 2027 sarà un anno elettorale particolarmente importante per diversi Paesi europei, Italia compresa. Quanto dobbiamo preoccuparci di possibili operazioni di interferenza attraverso cyberattacchi, disinformazione, utilizzo di bot e manipolazioni con intelligenza artificiale? Quali sono le principali vulnerabilità per l'opinione pubblica italiana?

«Le minacce e gli attacchi ibridi che la Russia sta conducendo contro i nostri Paesi hanno l'obiettivo di intimidire gli Stati europei affinché smettano di sostenere l'Ucraina»

Kaja Kallas
intervista a Corriere della Sera
3 ottobre 2026

"Dobbiamo preoccuparci, e molto. Le elezioni sono il momento in cui una democrazia è più permeabile: l'attenzione è alta, i tempi sono stretti, le smentite arrivano sempre in ritardo rispetto al falso. L'intelligenza artificiale abbassa drasticamente i costi: video e audio contraffatti di leader politici, reti di bot capaci di simulare consenso, contenuti calibrati sulle paure di ogni singola nicchia.

L'Italia presenta vulnerabilità specifiche. Una quota rilevante di cittadini si informa soprattutto sui social e su app di messaggistica, dove la verifica è quasi assente. La fiducia nelle istituzioni e nei media tradizionali è bassa. Esiste un'area di opinione pubblica storicamente sensibile alle narrazioni "pacifiste" o antiamericane, che la propaganda russa sa sfruttare presentando ogni aiuto a Kiev come un costo sottratto a bollette, salari e sanità. E il caro energia resta un nervo scoperto. La strategia non punta necessariamente a far vincere qualcuno, ma a polarizzare, delegittimare il voto e spingere il futuro governo verso il disimpegno dall'Ucraina".

In diversi Paesi europei crescono le forze della destra radicale e nazionalista: è un fenomeno esclusivamente legato alle dinamiche interne delle società europee o può diventare un terreno fertile di influenza per potenze straniere non occidentali, con la Russia in cima alla lista?

"Le radici sono soprattutto interne: crisi del ceto medio, immigrazione, sfiducia verso le élite, paura del declassamento. Sarebbe un errore e un regalo alla propaganda, liquidare milioni di elettori come pedine di Mosca. Ma è proprio su queste fratture reali che si innesta l'influenza esterna. Il Cremlino non crea il malcontento: lo amplifica, lo orienta e lo usa.

Negli anni sono emersi rapporti, finanziamenti contestati e convergenze di linguaggio tra Mosca e diverse forze nazionaliste e sovraniste europee, accomunate dall'ostilità verso Bruxelles e verso la Nato. Per Putin ogni partito che chiede di ridurre le sanzioni, rinegoziare l'adesione all'Alleanza o "smettere di finanziare la guerra" è un alleato oggettivo nel progetto di svuotare l'Ue dall'interno. Che sia di estrema destra o di estrema sinistra per Putin poco importa. Va però sottolineato che non tutta la destra europea è filorussa: alcune forze conservatrici, anche al governo, sostengono con decisione Kiev, la Nato e l'Ue. Il punto non è l'ideologia ma la porosità di alcuni attori politici europei alle narrazioni russe".

La minaccia ibrida rende sempre più difficile distinguere la pace da un conflitto dichiarato. L'Italia e l'Europa sono oggi sufficientemente preparate a difendere infrastrutture, istituzioni e processi democratici da questa nuova forma di minaccia?

"Rispetto a qualche anno fa la consapevolezza è cresciuta ma la preparazione resta disomogenea. Le infrastrutture critiche sono spesso in mano a operatori privati con standard di sicurezza diversi; la cooperazione tra intelligence europee è ancora limitata dalle sovranità nazionali; mancano protocolli comuni e rapidi di attribuzione e risposta. L'Italia ha rafforzato l'Agenzia per la cybersicurezza nazionale ma la difesa dalla guerra ibrida non può essere solo tecnica: serve una resilienza della società intera, sul modello dei Paesi nordici e baltici, come anche di Israele, dove cittadini, imprese e istituzioni sono coinvolti nella "difesa totale".

Quale è il ruolo dell'informazione?

"L'editoria ha un ruolo decisivo. La disinformazione prospera nel vuoto lasciato dall'informazione

«Mentre noi stiamo parlando ci sono attacchi cyber, mentre noi parliamo c'è disinformazione, c'è il tentativo di manipolazione». E ha aggiunto: «La guerra cognitiva e la possibilità di manipolare le opinioni pubbliche fa parte del modo con cui si indebolisce l'avversario, senza fare una guerra vera e propria. Noi la stiamo subendo da anni»

Ministro Guido Crosetto
Sassari, 25 settembre 2026

di qualità. Giornali in carta e testate online possono fare tre cose: verificare con rigore e spiegare i fatti con tempestività senza inseguire la viralità; rendere riconoscibili le tecniche di manipolazione, educando i lettori a riconoscere deepfake e campagne coordinate; collaborare con istituzioni, università e piattaforme in reti di fact-checking condivise.
Un'informazione libera, autorevole e accessibile è la prima infrastruttura critica di una democrazia. Ed è esattamente ciò che la guerra ibrida di Putin cerca di demolire. Il primo obiettivo delle fake news è l'informazione di qualità perché se le bugie si impadroniscono della conoscenza ad essere demolita è la capacità di comprendere e decidere, su cui si basa la libertà di voto che in ultima istanza è il pilastro più cruciale della democrazia".

L'informazione di qualità è una difesa della democrazia

La disinformazione prospera nel vuoto lasciato dall'informazione di qualità. I giornali e le pubblicazioni online possono fare la differenza. Ecco tre cose che possono fare.

1

VERIFICARE E SPIEGARE I FATTI, SUBITO



Giornali e testate online devono verificare con rigore i fatti e spiegarli con chiarezza, senza inseguire la viralità.

2

RENDERE RICONOSCIBILI LE TECNICHE DI MANIPOLAZIONE



Bisogna far conoscere le tecniche di manipolazione, educando i lettori a riconoscere deepfake e campagne coordinate.

3

COLLABORARE CON ISTITUZIONI, UNIVERSITÀ E PIATTAFORME



È essenziale collaborare con isituzioni, università e piattaforme in reti condivise di fact-checking.



Un'informazione libera, autorevole e accessibile è la prima infrastruttura critica di una democrazia.

E proprio questo è ciò che la guerra ibrida di Putin vuole demolire.



IL BERSAGLIO PRINCIPALE DELLE NOTIZIE FALSE

La qualità dell'informazione è il primo obiettivo. Perché se le bugie prendono il sopravvento sulla conoscenza, ciò che viene davvero demolito è la capacità di capire e di decidere, su cui si basa la libertà di votare, che è il pilastro più cruciale della democrazia.





Neuroscienze e social network

L'attenzione dell'utente è diventata una risorsa strategica

La difesa del XXI secolo dovrà proteggere anche qualcosa che non può essere circondato da un muro, pattugliato da una nave o difeso da un sistema antimissile.
La capacità di una società di pensare, valutare e decidere autonomamente

La guerra dentro la mente





La guerra contemporanea ha progressivamente allargato il proprio campo di battaglia, ai tradizionali domini, si sono aggiunti il cyberspazio e l'ambiente informativo/cognitivo, un ambiente "ibrido" che coinvolge la capacità degli individui e delle società di interpretare ciò che accade intorno a loro.
In questo spazio le neuroscienze assumono una rilevanza strategica, perchè studiare il cervello significa comprendere come vengono selezionate le informazioni, come alcuni stimoli attirano l'attenzione più di altri, in che modo le emozioni condizionano il giudizio e come la memoria contribuisce alla costruzione delle nostre rappresentazioni della realtà.
I social network hanno poi dato un "booster" a questi meccanismi, perché ogni utente riceve un continuo flusso di contenuti, spesso determinato dalle proprie interazioni precedenti. La stessa notizia può, quindi, essere presentata a persone diverse, all'interno di contesti completamente differenti.
In tale ambiente virtuale, l'attenzione dell'utente è diventata una risorsa strategica, ed è per questo motivo che si tendono ad attuare delle



vere e proprie tattiche per "polarizzarla" con contenuti che interrompono il normale flusso delle informazioni. In questa sofisticata "manipolazione cognitiva" entrano in gioco immagini, video (deep fake), titoli sensazionali e notifiche "ricorrenti" che generano una reazione immediata, tra sorpresa, paura o indignazione.

Questa dinamica diventa poi particolarmente impattante, quando viene inserita all'interno di una campagna di influenza, dove da un fatto reale, vengono selezionati ad arte solo alcuni elementi, per costruire intorno a quel fatto una spiegazione capace di orientarne l'interpretazione. Una narrativa efficace tende, di fatto, a semplificare una realtà complessa, individua un responsabile, costruisce un antagonista, attribuisce un significato agli eventi e offre al pubblico una chiave interpretativa immediatamente comprensibile ed accettabile.

L'obiettivo di un attore ostile, infatti, non deve essere necessariamente quello di convincere una popolazione ad accettare una determinata posizione, può anche essere sufficiente modificare solo il modo nel quale viene interpretato un evento, aumentando così la sfiducia o la frattura già presente nella società. La differenza è sostanziale perchè una propaganda tradizionale cerca spesso di affermare una propria versione dei fatti, mentre una moderna operazione di influenza può, invece, puntare a produrre confusione.

L'emozione poi accelera questo processo, quando, paura, rabbia, indignazione e senso di appartenenza diventano potenti moltiplicatori della circolazione di un contenuto.

Una società resiliente deve, pertanto, essere capace e formata nel saper riconoscere, non soltanto una notizia falsa, ma anche il motivo che sta alla base della campagna d'influenza. Chi sta parlando? Quale pubblico sta cercando di raggiungere? Quali emozioni sta tentando di attivare? Quali account stanno amplificando il messaggio? Esistono collegamenti tra soggetti apparentemente indipendenti? La stessa narrativa compare contemporaneamente su piattaforme differenti? Queste domande spostano così l'attenzione dalla verifica del singolo contenuto all'analisi, vera e propria, dell'operazione.

La risposta, di conseguenza, non può essere affidata esclusivamente ai fact-checker, ma servono capacità di intelligence, analisi dei dati, monitoraggio dell'ambiente informativo/cognitivo, competenze tecnologiche e comunicazione strategica. Serve soprattutto una cooperazione stabile tra istituzioni, mondo accademico, piattaforme tecnologiche, editoria e società civile per una reale resilienza.

La sfida per le istituzioni è ancora più ampia, purché proteggere una società significa ormai considerare contemporaneamente infrastrutture fisiche, reti digitali, sistemi spaziali, comunicazioni e ambiente informativo. Una Nazione può disporre di capacità militari avanzate e infrastrutture tecnologiche resilienti, ma rimanere vulnerabile se perde la capacità di riconoscere una manipolazione o se la fiducia interna viene sistematicamente erosa.

La prossima frontiera della guerra ibrida, potrebbe, infatti, concentrarsi sulla capacità di modificare, prima ancora dell'azione, il modo nel quale una società percepisce una minaccia, interpreta gli eventi e decide come reagire. È qui che la dimensione neurocognitiva incontra quella della Foreign Information Manipulation and Interference, la FIMI.

MICHELE ZIZZA
Università degli Studi della Tuscia di Viterbo

Overload informativo e le minacce di natura antropica

Resilienza e sicurezza nell'era dell'iperinformazione



Le minacce antropiche e socio-tecnologiche impongono un nuovo modello di sicurezza, fondato su prevenzione, resilienza e partecipazione consapevole dei cittadini. Un approccio integrato in cui istituzioni, ricerca, industria e Difesa condividono conoscenze, tecnologie e responsabilità per anticipare crisi sempre più interconnesse

La volontà di promuovere la sinergia tra istituzioni e cittadini per far fronte agli eventi straordinari non è dettata da una facoltà esclusivamente politica, affatto; vi è, alla base, una ragione di carattere scientifico e, già nel secolo scorso, il tema era stato approfondito negli studi dell'antropologa britannica Mary Douglas: coinvolgere, informare e responsabilizzare il cittadino nella gestione dell'emergenza. Una questione centrale, nevralgica nel contesto attuale, che invita le politiche pubbliche, la ricerca scientifica e la partecipazione attiva delle comunità a convergere verso un unico paradigma di sostenibilità per far fronte allo scenario in continua evoluzione e che, a differenza del secolo scorso, manifesta mutamenti improvvisi e sempre più difficili da gestire. Ma cosa sono le minacce di origine antropica? Queste rappresentano, oggi, uno dei principali fattori di pressione sui sistemi naturali, economici e sociali. Incidenti industriali, compromissione delle infrastrutture critiche, cyber attacchi, contaminazioni e alterazioni degli habitat, crisi generate dall'impiego massivo delle tecnologie e iperinformazione mostrano come il rischio contemporaneo abbia assunto una forma sempre più complessa, interconnessa e difficilmente circoscrivibile a un singolo settore come lo era un tempo. È proprio questa interdipendenza a rendere necessario un cambio di prospettiva e ad optare per l'adozione di nuove metodologie di valutazione e controllo degli eventi.



Tant'è, ad esempio, che la gestione dei rischi antropogenici non può più essere ricondotta esclusivamente alla capacità di intervenire dopo il verificarsi di un evento. Oggi, vengono richiesti sistemi in grado di prevenire, anticipare, monitorare e assorbire gli effetti di crisi che possono propagarsi rapidamente tra

LA NUOVA NATURA DEL RISCHIO



Le Minacce Antropiche Complesse

Incidenti industriali, cyber attacchi e crisi iper-informative generano collassi sistemici tra ambiente, economia e società.



L'Interdipendenza dei Sistemi

Il rischio contemporaneo è difficilmente circoscrivibile a un singolo settore e richiede nuove metodologie di valutazione.



"L'attenzione è la risorsa scarsa"

Herbert Simon evidenzia come, in un mondo iper-informatizzato, l'attenzione umana sia la vulnerabilità critica da proteggere.

STRATEGIE DI RESILIENZA E DIFESA



Dalla Reazione all'Anticipazione

La resilienza non è solo resistere, ma adattarsi e trasformare le organizzazioni per preservare le funzioni essenziali dello Stato.



Il Ruolo del Sistema Difesa

Oltre alla difesa tradizionale, i militari offrono competenze logistiche, tecnologiche e di coordinamento per infrastrutture critiche.



Tecnologie Dual-Use

Innovazioni nate per la difesa applicate a protezione civile, monitoraggio ambientale e intelligenza artificiale.

PILASTRI DEL NUOVO PARADIGMA DI SICUREZZA NAZIONALE



SINERGIA ISTITUZIONALE

Coordinamento tra Difesa, Ricerca e Industria.



RESPONSABILIZZAZIONE

Coinvolgere il cittadino nella gestione dell'emergenza.



MONITORAGGIO SOCIO-TECNOLOGICO

Studiare l'attenzione umana per mitigare i rischi di percezione.

ambiente, economia, infrastrutture e società, generando veri e propri collassi di rilevanza primaria. Parlare di sicurezza significa, quindi, parlare anche di resilienza, continuità delle funzioni essenziali dello Stato, capacità tecnologica e coordinamento tra istituzioni ed è, esattamente in questo scenario, che assume particolare rilevanza il ruolo della Difesa italiana, la cui funzione si inserisce in un'architettura di sicurezza nazionale ed estera sempre più articolata e aggiornata. Accanto alla tradizionale missione di difesa dello Stato, che tutti conosciamo, le capacità militari concorrono alla gestione di scenari complessi attraverso competenze operative, logistiche, tecnologiche e informative, contribuendo alla protezione delle infrastrutture strategiche, alla sicurezza cibernetica, alla risposta alle emergenze e al mantenimento della continuità operativa nei contesti di crisi al fine di offrire una schermatura permanente sulla collettività. Una crescente convergenza tra dimensione civile e militare che trova, inoltre, uno dei suoi principali punti di contatto nello sviluppo di tecnologie dual-use: sistemi, conoscenze e innovazioni concepite o utilizzate in ambito difesa, ma applicabili nella protezione civile, nel monitoraggio ambientale, nelle telecomunicazioni, nella cybersecurity, nell'intelligenza artificiale, nell'osservazione della Terra, nella gestione delle infrastrutture critiche e nel monitoraggio delle operazioni informative finalizzate a influenzare e ad indirizzare i comportamenti.

La caratterizzazione dei rischi antropogenici diventa, quindi, parte di una riflessione più ampia sulla capacità del sistema-Paese di conoscere le proprie vulnerabilità, anticipare le minacce e costruire risposte coordinate e altamente efficaci. Una prospettiva nella quale governance, ricerca scientifica, industria, innovazione e Difesa sono chiamate a dialogare all'interno di un modello dinamico integrato e interdipendente. La questione centrale, dunque, non riguarda soltanto quali siano i principali rischi generati dall'attività umana, ma quanto un Paese sia realmente preparato ad affrontarne gli effetti sistemici. Ed è qui, su questo terreno, che il concetto di resilienza assume una valenza strategica: non semplicemente resistere a una crisi, ma preservare le funzioni essenziali, adattarsi al mutamento e trasformare capacità, organizzazioni e tecnologie per rispondere a scenari nuovi e sempre più complessi. In virtù di queste consapevolezze, dobbiamo porre l'attenzione su una delle più ingannevoli e pervasive minacce, quella socio - tecnologica e ricordare il pensiero di Herbert Simon, psicologo statunitense: "in un ambiente ricco di informazioni la risorsa veramente scarsa è l'attenzione umana". L'attenzione umana che diventa una risorsa preziosa che, in una società frenetica e iper-informatizzata, non bisogna più considerare come elemento scontato durante una lezione, in un dibattito, in un'azione di mediatizzazione che sia di natura politica, culturale o di intrattenimento.

L'individuo processa indubbiamente più dati rispetto a periodi antecedenti la telematizzazione della società e questo aspetto rappresenta un fattore da considerare nello studio della gestione delle crisi, una variabile da annoverare in fase di indagine sociologica al fine di mitigare i rischi di percezione della verità, di credibilità, di dispersione di energie intese come attenzione ed approfondimento. Le istituzioni, la ricerca, la Difesa come attore principale chiamato ad anticipare gli scenari di crisi, devono aprire un'ulteriore finestra di studio sull'attenzione, sulla necessità di catturare la concentrazione nell'evoluzione inarrestabile socio - tecnologica. L'approfondimento richiede una partecipazione trasversale di specializzazioni (psicologia sociale, ergonomia cognitiva, neuropsicologia, neuroscienze cognitive, scienze dell'informazione, psicofisiologia) e, come per altre sfide passate, interessa proprio una realtà centrale quale il "Sistema Difesa" di uno stato. La consapevolezza di operare su queste aree di interesse, la saggezza intellettuale di coinvolgere e responsabilizzare il cittadino, renderlo edotto della vulnerabilità che può rappresentare, se isolato nel sistema organizzativo, promuoverà una riduzione dell'esposizione ai rischi che, quotidianamente, si manifestano senza assetti fisici ed evidenti.

J LUIGI M. KUNZ SAPONARO

«Universidad Carlos III de Madrid - Departamento de Humanidades»

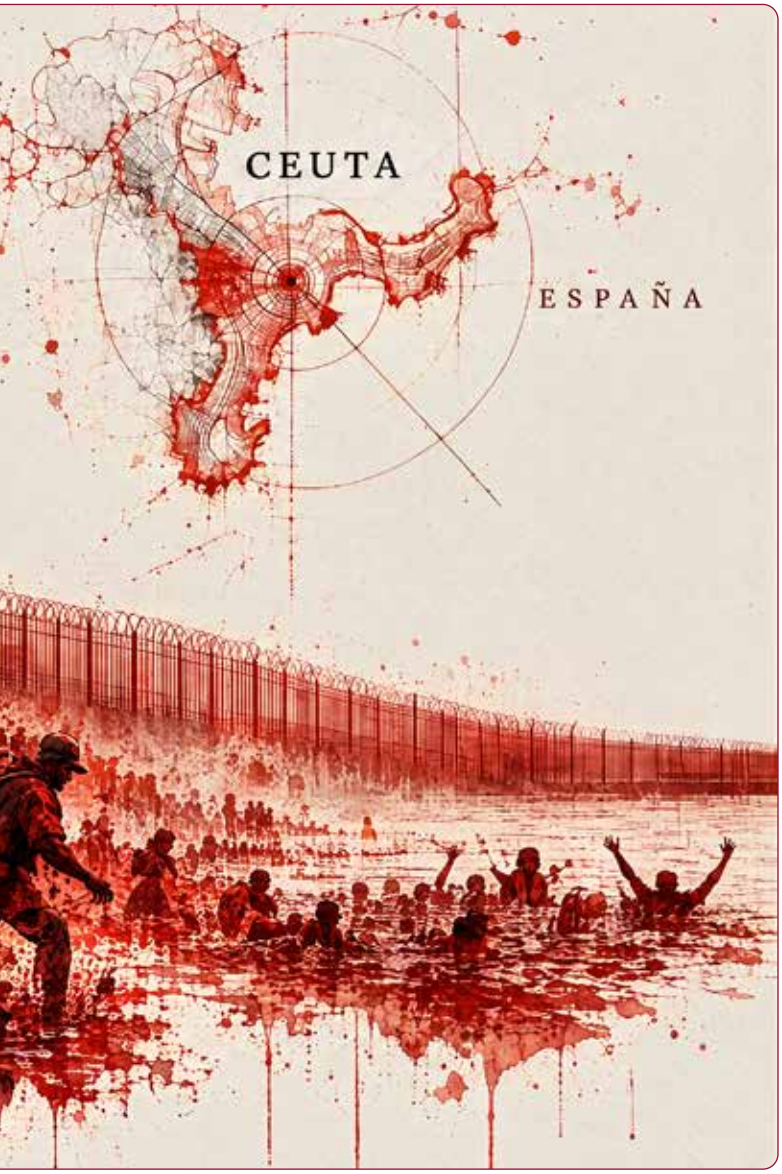
Ceuta e la strumentalizzazione politica delle migrazioni

Una leva di pressione politica sull'Unione Europea



La crisi di Ceuta mostra come la strumentalizzazione dei flussi migratori possa diventare uno strumento di pressione politica e strategica. Per Spagna e Unione Europea emerge la necessità di ridurre vulnerabilità e dipendenze dai Paesi terzi

Ceuta è una città autonoma spagnola situata sulla costa settentrionale del Marocco, le sue frontiere, assieme a quelle di Melilla, costituiscono gli unici confini terrestri dell'UE nel Continente africano. Il fenomeno migratorio ha profondamente segnato la storia recente e la vita politica delle due città, dove barriere e dispositivi di sorveglianza rendono questi confini tra i più fortificati al mondo.



La strumentalizzazione della migrazione per esercitare pressione sulla Spagna può rientrare tra le modalità di confronto strategico proprie della guerra ibrida. In questo contesto, i flussi migratori possono diventare uno strumento non militare di pressione politica, caratterizzato dall'ambiguità nell'attribuzione delle responsabilità e dallo sfruttamento delle vulnerabilità dell'avversario. Ne deriva una condizione di fragilità per la Spagna e per l'intera UE, la cui capacità di gestire il fenomeno dipende anche dalla cooperazione dei Paesi terzi, tra cui il Marocco.

A Ceuta, simili forme di pressione si sono manifestate in più occasioni. Nel maggio 2021, circa 9.000 persone entrarono irregolarmente nella città spagnola dopo che le autorità marocchine avevano temporaneamente allentato i controlli di frontiera, nel quadro di una forte tensione diplomatica fra Rabat e Madrid legata alla questione del Sahara Occidentale, ex colonia spagnola. Dieci mesi dopo, Pedro Sánchez definì, in una lettera indirizzata a Mohammed VI, il piano marocchino di autonomia per il Sahara Occidentale «la base più seria, realistica e credibile» per risolvere la controversia, modificando la posizione spagnola sulla questione della sovranità marocchina sul territorio dell'ex colonia.

La crisi iniziata il 30 luglio 2026 presenta alcuni elementi analoghi. Il 20 luglio, il governo spagnolo aveva annunciato una riunione di alto livello con l'Algeria, prevista per ottobre, allo scopo di rilanciare la cooperazione bilaterale,

La "Tempesta Perfetta": I 4 Pilastri della Crisi

CEUTA

30 Luglio 2026

MAROCCO

SPAGNA

1 Fattore Socio-Economico

Disperazione giovanile e crisi climatica in Marocco.

2 Fattore Legale

La regolarizzazione di massa in Spagna e la sentenza della Corte Suprema.

3 Fattore Diplomatico

Il disgelo Spagna-Algeria e la rappresaglia geopolitica.

4 Fattore Digitale

Disinformazione e reti di traffico sui social media.

La Guerra Ibrida: Il Fronte Digitale



1. Innesco Organico: Su TikTok e WhatsApp proliferano mappe dei punti ciechi di Ceuta e false interpretazioni della sentenza della Corte Suprema spagnola.



2. Amplificazione (Il Picco): Oltre 11 milioni di visualizzazioni generate da account localizzati in Algeria, Tunisia e Francia per incitare l'attraversamento.



3. Disinformazione di Stato: Il governo spagnolo accusa pubblicamente reti di bot russi e network israeliani di aver manipolato la crisi per promuovere teorie del complotto ("Great Replacement") e destabilizzare l'UE.

CEUTA

ESPAÑA

AI Generate

anche nel settore energetico, e di rafforzare la sicurezza degli approvvigionamenti della Spagna. Dieci giorni dopo, tra il 30 e il 31 luglio, si verificò un ingresso massiccio di migranti a Ceuta, inizialmente stimato dalle autorità spagnole in circa 50.000 persone e successivamente portato a 72.000.

In un primo momento, il governo spagnolo evitò di attribuire responsabilità dirette a Rabat e indicò nelle organizzazioni criminali una delle principali cause della crisi. In Spagna, l'ipotesi che la temporanea passività dei controlli marocchini costituisse un segnale di opposizione al riavvicinamento fra Madrid e Algeri, considerata la storica rivalità regionale tra Marocco e Algeria, ha tuttavia acquisito un seguito crescente.

La crisi ha avuto ripercussioni sul quadro politico spagnolo e sul dibattito europeo. A livello nazionale, la prudenza del governo nell'attribuire eventuali responsabilità ha suscitato dure critiche da parte dell'opposizione e un forte malcontento fra la popolazione di Ceuta e alcuni settori della società spagnola. Le critiche hanno investito lo Stato, accusato di aver ignorato gli avvertimenti dell'intelligence, e Bruxelles, per una risposta ritenuta lacunosa.

Il successivo disaccordo tra gli Stati membri sulla gestione delle frontiere dello spazio Schengen ha ulteriormente messo in luce la fragilità dell'Unione, indebolendone la posizione in un contesto geopolitico internazionale instabile. Parte del dibattito si è basata su una lettura imprecisa del regime Schengen di Ceuta, che prevede controlli sui collegamenti marittimi e aerei con la Spagna continentale. Gli effetti destabilizzanti di questa forma di pressione ibrida sono, pertanto, difficili da minimizzare perchè l'UE deve confrontarsi con attori in grado di strumentalizzare le persone migranti lungo le sue frontiere esterne. La cooperazione con gli Stati terzi è fondamentale per la gestione della migrazione irregolare, ma rimane un'arma a doppio taglio, poiché può generare dipendenze strategiche che rischiano di trasformarsi in vere e proprie vulnerabilità. La riduzione dell'eccessiva dipendenza strategica da singoli Paesi partner deve diventare una priorità, insieme al rafforzamento della collaborazione tra le istituzioni europee e nazionali. Occorre sviluppare la capacità di prevenire e gestire simili crisi attraverso interventi alle frontiere esterne e, soprattutto, mediante strumenti diplomatici e forme di cooperazione con i Paesi di origine e di transito.

La crisi di Ceuta è sintomatica di una vulnerabilità strategica che l'UE ha dimostrato di non saper ancora gestire con sufficiente determinazione. La grande attenzione prestata al numero delle persone entrate nella città spagnola ha prodotto una forte amplificazione mediatica, rischiando di oscurare il problema di fondo: la Spagna e, di conseguenza, l'UE possono essere esposte a forme di pressione politica esercitate da attori esterni attraverso la strumentalizzazione della migrazione. Per garantire la necessaria stabilità, occorre pertanto adottare una posizione risoluta e condivisa di fronte a criticità di questo genere.





immagine: © mod.gov.ua

CECILIA SALA

«CHORA NEWS»

LA GUERRA VISTA DALLA "KILL ZONE"

Il racconto dei soldati ucraini, dove il fronte non è più una linea continua, ma una profondità di circa 30 chilometri, dominata da droni e robot terrestri costruiti direttamente in Ucraina

In Ucraina il fronte non appare più come la linea continua che ha caratterizzato l'immaginario delle guerre del Novecento, è diventato un corridoio profondo circa 30 chilometri e lungo mille, una fascia di territorio che i militari ucraini chiamano "kill zone". È qui, sul terreno, insieme ai soldati, che il reportage ("La guerra dei droni" di Chora news) racconta una delle trasformazioni più radicali del conflitto: il campo di battaglia è diventato uno spazio nel quale il pericolo arriva soprattutto dall'alto e dove la presenza fisica dell'uomo viene progressivamente sostituita da macchine controllate a distanza.

A Druzhkivka, nel Donbas, il movimento lungo la "kill zone" avviene con modalità che fino a pochi anni fa sarebbero state difficili da immaginare. Dopo aver lasciato l'auto, il percorso prosegue per 12 chilometri a piedi, i soldati mantengono diversi metri di distanza l'uno dall'altro, per ridurre il rischio di diventare un unico bersaglio per i droni russi.

Occorreva un cambio radicale per non perdere la guerra e la risposta ucraina è stata quella di delegare alle macchine una parte crescente delle funzioni precedentemente affidate ai soldati. I robot vengono utilizzati per trasportare munizioni, recuperare feriti, effettuare operazioni di supporto e, in alcuni casi, combattere direttamente. La logica è innanzitutto quella della sopravvivenza: compensare la superiorità numerica russa e ridurre il numero di uomini esposti nella "kill zone".

Gli stessi militari sintetizzano questa filosofia con una frase: "**le macchine non sanguinano**".

L'obiettivo indicato per il 2027 è quello di arrivare a 100mila robot, una cifra significativa se rapportata ai circa 200 mila soldati complessivamente schierati al fronte. L'automazione non nasce però soltanto dalla necessità di proteggere il personale, è anche la risposta a un'altra vulnerabilità strategica: la dipendenza dalle forniture occidentali di munizioni e armamenti. Il conflitto è entrato in una fase nella quale Kyiv deve produrre internamente una quota crescente di strumenti necessari alla guerra, arrivando al 75% delle armi utilizzate sul campo costituite da droni progettati e prodotti in Ucraina.



I numeri sono eloquenti: i veicoli autonomi ucraini hanno effettuato più di 50 mila missioni dall'inizio del 2026. Un sistema armato di mitragliatrice ha difeso autonomamente una posizione avanzata per 45 giorni consecutivi e, in un altro episodio, tre soldati russi si sono dovuti arrendere ad una macchina.

Il comandante del "Terzo corpo d'armata" sostiene che i robot potrebbero sostituire immediatamente un terzo delle proprie truppe e, nel lungo periodo, arrivare a svolgere funzioni oggi affidate all'80 per cento del personale impiegato al fronte.

La funzione nella quale la sostituzione dell'uomo appare già più evidente è nella logistica dove i robot effettuano, ormai, tre movimenti logistici su quattro. Il caso più semplice è quello delle munizioni: trasportare 400 chilogrammi per alcuni chilometri all'interno della "kill zone" richiedeva in precedenza cinque soldati impegnati per tutta la notte, oggi la stessa operazione può essere affidata ad un veicolo autonomo, dove se la macchina viene colpita, la perdita è quella di un mezzo e non di cinque uomini.

La stessa logica emerge dalla scritta "**I robot salvano vite**", riportata sulla schiena di un soldato che controlla con un joypad una macchina destinata alla posa delle mine.

Un tenente colonnello, conosciuto con il nome di battaglia "Pinkman", quando un drone russo gli ha amputato entrambe le gambe dal ginocchio in giù, è rimasto lucido e ha utilizzato il proprio kit di primo soccorso. Ha applicato due tourniquet, utilizzando un righello per posizionarli alla stessa altezza. Una procedura che aveva una ragione precisa: "Pinkman" sapeva che avrebbe probabilmente subito l'amputazione e che avere due monconi della stessa lunghezza avrebbe facilitato la successiva riabilitazione. Nel kit aveva anche un pennarello per registrare l'orario di applicazione dei tourniquet. Da quel momento, il tempo diventa determinante perché occorre raggiungere l'ospedale entro circa due ore, per evitare conseguenze ulteriori all'arto.

Il problema è che nella "kill zone", l'evacuazione di un ferito è diventata una delle operazioni più pericolose. Gli elicotteri rimangono il mezzo più efficace per una evacuazione sanitaria, ma la presenza dei droni rende impossibile utilizzarli liberamente, in una zona nella quale decine di migliaia di piccoli velivoli possono essere presenti contemporaneamente. Si perde così quella che, nella medicina militare d'urgenza, viene definita la "golden hour", il periodo immediatamente successivo al ferimento nel quale un intervento rapido può determinare la sopravvivenza del soldato e ridurre il rischio di amputazioni.

Anche il rapporto tra morti e feriti raccontano quanto la natura del combattimento sia cambiata. L'Ucraina presenta, secondo i dati riportati dal ministero della Difesa, un rapporto più vicino a quello della Prima guerra mondiale che a quello osservato nella guerra in Afghanistan che contava un morto ogni tre/quattro feriti.

Durante la Seconda guerra mondiale, nella stessa area combattevano eserciti composti da milioni di uomini dove per ogni chilometro di fronte potevano essere schierati quasi mille soldati. Oggi, gli ucraini dispongono di appena 15 soldati per chilometro. La trasformazione non riguarda però soltanto la difesa delle posizioni perché, grazie ai sistemi senza pilota, l'Ucraina può colpire a corto, medio e lungo raggio, fino a raggiungere obiettivi in profondità nel territorio russo.

L'evoluzione tecnologica del ministero della Difesa ucraino, è stata affidata, in parte, anche Serghii Sternenko, un attivista e youtuber che ha rivoluzionato la gestione della guerra con la produzione massiva di droni: +441% (ricognizione), +312% (medio raggio) e +179% (corto raggio), la maggior parte guidati attraverso fibra ottica, una soluzione pensata per renderli meno vulnerabili alle interferenze elettromagnetiche.



Al centro della trasformazione, vi è però anche e soprattutto Mykhailo Fedorov, già ministro del Digitale e successivamente entrato nella gestione della Difesa (nominato ministro a gennaio 2026, ha perso l'incarico, a seguito del rimpasto governativo del 15 luglio 2026).

La digitalizzazione tattica, quella sul campo, è arrivata anche alla gestione delle operazioni perché oggi l'esercito ucraino, tra le varie soluzioni di comando e controllo, dispone anche di una "piattaforma a punti" sulla quale i militari caricano le immagini registrate dai droni. Le distruzioni documentate vengono associate a un punteggio che può essere utilizzato per ottenere nuovi equipaggiamenti, attraverso una piattaforma digitale dedicata.

Prima della diffusione capillare dei droni era più difficile verificare in tempo reale la situazione lungo il fronte, oggi decine di migliaia di sistemi raccolgono immagini organizzate per settore e il Comando dispone, così, di una enorme quantità di informazioni che vengono utilizzate per verificare le perdite, seguire i movimenti dei soldati ed assumere decisioni operative.

Il sistema incentiva, inoltre, i militari a condividere le immagini delle operazioni; nel solo mese di giugno, la piattaforma aveva raggiunto centomila video verificati, relativi a militari russi uccisi dai droni.

La stessa piattaforma conferisce poi un punteggio all'obiettivo: un soldato russo vivo vale più di uno morto, perché la cattura produce un punteggio superiore.

Sternenko racconta che, attraverso la raccolta di fondi ottenuta grazie a milioni di follower su YouTube e Telegram, è stato possibile procedere alla fornitura di circa 200 mila droni a corto raggio e di decine di migliaia di altri sistemi.

In questa serrata rivoluzione digitale, le grandi industrie pubbliche hanno, però, perso parte delle risorse, reindirizzate a favore di startup specializzate nei droni. Gli ingegneri delle aziende produttrici vengono così messi direttamente a confronto con i militari che utilizzano i sistemi sul campo. I soldati spiegano agli ingeneri dove il drone non funziona, quali modifiche sono necessarie e quali caratteristiche devono essere cambiate. Il risultato è un ciclo di sviluppo molto più rapido con aggiornamenti software mensili e modifiche hardware semestrali.

La trasformazione tecnologica ha, però, un prezzo umano perché la guerra condotta attraverso macchine pilotate a distanza può ridurre l'esposizione diretta dei soldati, ma non rende il conflitto meno letale; al contrario, amplia lo spazio nel quale un uomo può essere individuato, seguito e colpito senza che riesca necessariamente a comprendere da dove provenga la minaccia.





LA DIGITALIZZAZIONE DELLA GUERRA

La trincea nel conflitto russo-ucraino non è scomparsa, ma ha perso il ruolo centrale che aveva mantenuto per oltre un secolo, mentre la separazione tra linea del fronte e retrovia è diventata sempre più difficile da individuare

La linea del fronte e la retrovia ci sono ancora, ma ancor prima si è sviluppata una vasta "kill zone", una fascia di territorio nella quale ogni movimento può essere osservato attraverso droni, sensori, satelliti e sistemi di guerra elettronica. Nel Donbass questa zona può estendersi per decine di chilometri oltre la linea di contatto, rendendo vulnerabili non soltanto le unità impegnate direttamente nei combattimenti, ma anche depositi, centri di comando, ambulanze e colonne logistiche.
Il dato più significativo riguarda proprio il ruolo assunto dai sistemi senza pilota. Secondo il Ministero della Difesa ucraino, dall'inizio del 2026 le unità di sistemi senza pilota hanno registrato oltre 800 mila bersagli nemici colpiti e verificati e i droni rappresentano oggi più del 90% degli obiettivi colpiti. Non si tratta soltanto dei piccoli FPV diventati l'immagine più riconoscibile della guerra, ma di un ecosistema che comprende piattaforme di ricognizione, velivoli d'attacco, sistemi per l'individuazione dei bersagli, correttori di tiro e apparati capaci di trasmettere rapidamente informazioni alle unità di combattimento. La conseguenza è una riduzione drastica dei tempi tra individuazione e ingaggio, con la possibilità di trasformare, quasi immediatamente, un movimento sul terreno in un bersaglio.
La concentrazione di uomini e mezzi di un tempo è diventata una vulnerabilità perché convogli, mezzi corazzati e reparti numerosi possono essere individuati e colpiti dall'alto. Le unità sono quindi costrette a muoversi in gruppi sempre più piccoli, spesso di pochi uomini, sfruttando vegetazione, macerie e terreno per ridurre la possibilità di essere scoperti. Come ha spiegato un operatore del 4° Reggimento Ranger ucraino a Reuters, identificato con il nominativo "Gur": "la guerra crea le sue condizioni, sono comparsi i droni FPV e noi abbiamo dovuto adattarci e se non ci adattiamo, non sopravviviamo".
Anche la vita quotidiana dei soldati è stata trasformata da questa nuova geografia del combattimento. Nelle aree più esposte non esistono necessariamente linee continue di trincee, ma una successione di piccole postazioni isolate, chiamate "burrows", tane, nelle quali i militari possono rimanere immobili per giorni per evitare di essere individuati dai sensori.
Nel paesaggio del Donbass questa trasformazione è visibile anche nei resti materiali della guerra. Blindati, autocarri e motociclette



> ***"la guerra crea le sue condizioni, sono comparsi i droni FPV e noi abbiamo dovuto adattarci e se non ci adattiamo, non sopravviviamo"***
>
> **Operatore del 4° Reggimento Ranger ucraino a Reuters**

distrutti vengono spesso abbandonati perché recuperarli significa esporre altri mezzi al fuoco dei droni, mentre i nuovi velivoli guidati attraverso fibra ottica lasciano sul terreno e tra i boschi chilometri di sottilissimi cavi. Questa tecnologia nasce dalla necessità di superare le interferenze della guerra elettronica.

Un drone tradizionale comunica con il proprio operatore, attraverso collegamenti radio che possono essere disturbati, mentre un sistema a fibra ottica trasmette attraverso un cavo che viene progressivamente srotolato durante il volo, riducendo drasticamente l'efficacia dei sistemi di jamming (sitemi di disturbo eletromagnetici).

Alla crescente difficoltà di muovere uomini e mezzi, risponde anche l'impiego degli "Unmanned Ground Vehicles", robot terrestri utilizzati per trasportare munizioni, acqua, batterie e viveri oppure per evacuare i feriti dalle aree nelle quali l'impiego di un'ambulanza tradizionale sarebbe troppo rischioso. Il Ministero della Difesa ucraino sta ampliando rapidamente l'impiego di questi sistemi e, più in generale, dei mezzi senza pilota, mentre il settore industriale nazionale ha aumentato la produzione di tecnologie destinate al campo di battaglia.

La trasformazione non riguarda però soltanto le piattaforme che volano o si muovono sul terreno, ma soprattutto il modo nel quale le informazioni vengono raccolte e utilizzate. È qui che entra in gioco il software, perché la superiorità operativa dipende sempre più dalla capacità di collegare dati provenienti da droni, sensori, radar e altre fonti e trasformarli rapidamente in una rappresentazione coerente del campo di battaglia. Il sistema ucraino DELTA rappresenta uno degli esempi più avanzati di questa evoluzione. Secondo Allied Command Transformation della NATO, l'ecosistema digitale è già utilizzato da oltre 200mila membri delle Forze di Difesa ucraine e sta integrando anche modelli di intelligenza artificiale destinati a migliorare l'analisi dei movimenti e delle attività sul campo.

La guerra dell'informazione procede così accanto a quella combattuta sul terreno, dove contenuti manipolati, attraverso l'intelligenza artificiale, hanno cercato di rappresentare come già conquistate aree ancora contese, mostrando come il controllo della percezione possa diventare parte della stessa operazione militare. Il campo di battaglia si estende quindi dalla posizione del soldato alla rete digitale che raccoglie dati, dalla fibra ottica che collega un drone al suo operatore fino agli algoritmi che aiutano a individuare schemi e movimenti.



IL SOFTWARE COME ARMA PRIMARIA

Sintesi
La superiorità operativa risiede nella capacità di aggregare più dati in una singola rappresentazione coerente in tempo reale del campo di battaglia

Evoluzione AI
Integrazione di modelli AI per l'analisi avanzata di schemi operativi, automatizzando il riconoscimento dei movimenti sul campo

DELTA SYSTEM

+200.000
Membri delle Forze di Difesa ucraine utilizzano attivamente l'ecosistema digitale come rete neurale tattica (dati NATO ACT)



LA GAMIFICATION DELLA GUERRA

La digitalizzazione tattica e la struttura degli incentivi centralizzata.



La Piattaforma:
I soldati caricano video registrati dai droni. Le distruzioni verificate generano un punteggio, convertibile in nuovi equipaggiamenti.

Volume Dati:
Nel solo mese di giugno, registrati 100.000 video verificati di soldati nemici colpiti.

Incentivi di Cattura: Un soldato nemico vivo genera un punteggio superiore rispetto a un'uccisione, per incentivare la resa e lo scambio di prigionieri.

11:59:07:87


DATA CENTER HALLS A-D
SMR-1
AI Generate

GIUSEPPE CALABRÒ

UNIVERSITÀ TUSCIA VITERBO

DALL'INTELLIGENZA ARTIFICIALE AL NUCLEARE

La nuova corsa ai mini reattori passa dai data center

Con l'IA il ruolo dell'energia è ora una risorsa chiave. I data center usano molta più elettricità e hanno bisogno di una rete stabile, sicura e sempre attiva. Per questo, i piccoli reattori e i microreattori entrano nei piani delle grandi aziende tech e, con scopi diversi, nei piani per la tenuta delle reti della Difesa

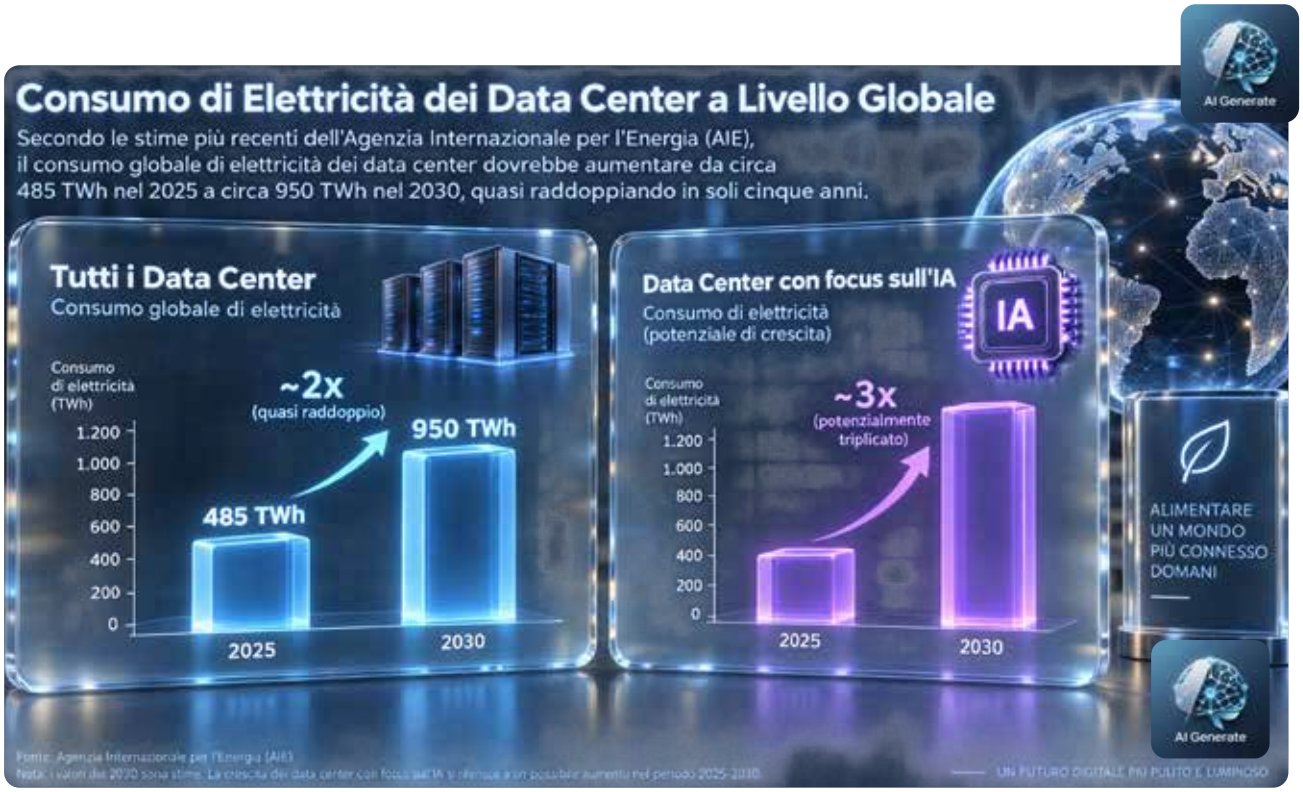


La rivoluzione dell'intelligenza artificiale ha un problema che fino a pochi anni fa sembrava appartenere a un altro settore: l'energia. I modelli di AI, i servizi cloud, i sistemi di calcolo ad alte prestazioni e i data center che li ospitano richiedono quantità crescenti di elettricità. Secondo le più recenti stime dell'Agenzia Internazionale dell'Energia (AIE), il consumo elettrico globale dei data center dovrebbe passare da circa 485 TWh nel 2025 a circa 950 TWh nel 2030, quasi raddoppiando in cinque anni. Nello stesso periodo il consumo dei data center maggiormente orientati all'intelligenza artificiale potrebbe crescere ancora più rapidamente, fino a triplicare.

Ma il problema non riguarda soltanto la quantità di energia richiesta perchè, un grande data center dedicato all'AI, presenta altri requisiti indispensabili, riferiti alla continuità, qualità e affidabilità dell'alimentazione. Per questo motivo, l'energia nucleare non è più soltanto considerata una fonte destinata al sistema elettrico nel suo complesso, ma anche come possibile fonte di energia stabile e a basse emissioni associata ai grandi poli digitali.

L'AIE prevede che le fonti rinnovabili soddisfino circa la metà della crescita della domanda elettrica mondiale dei data center nei prossimi anni, mentre il nucleare è destinato ad assumere un ruolo crescente verso la fine del decennio e soprattutto dopo il 2030. In Europa, rinnovabili e nucleare potrebbero arrivare insieme a rappresentare circa l'85 per cento dell'elettricità destinata ai data center entro il 2030.

Solare ed eolico costituiscono, di fatto, componenti fondamentali del processo di decarbonizzazione, insieme alle reti e ai sistemi di accumulo, il nucleare presenta, invece, la caratteristica di poter fornire grandi quantità di energia a basse emissioni con



elevata disponibilità e continuità: una proprietà particolarmente interessante per infrastrutture progettate per funzionare ventiquattr'ore su ventiquattro.

Da qui nasce anche l'interesse per gli "Small Modular Reactor", gli SMR, reattori di potenza inferiore rispetto alle grandi centrali convenzionali e concepiti per sfruttare maggiormente modularità, standardizzazione e fabbricazione industriale.

L'obiettivo è trasferire una parte crescente della realizzazione dell'impianto dal cantiere alla fabbrica: componenti standardizzati, processi replicabili e assemblaggio modulare dovrebbero, nelle aspettative dei progettisti, contribuire a ridurre complessità, tempi di costruzione e rischi finanziari.

Questo non significa, tuttavia, che gli SMR rappresentino già una soluzione commerciale consolidata su larga scala. Molti progetti occidentali devono ancora dimostrare pienamente competitività economica, ripetibilità industriale e capacità di rispettare tempi e costi; parallelamente devono evolvere i processi regolatori, le catene di fornitura e, per alcuni progetti avanzati, anche la disponibilità del combustibile.

È proprio questa una delle sfide della nuova fase del nucleare: passare dal prototipo e dal first-of-a-kind alla produzione seriale.

Nel frattempo, il mercato si sta muovendo perchè le grandi aziende tecnologiche hanno iniziato a considerare direttamente il nucleare nelle proprie strategie energetiche.

Il cambiamento è significativo: per i grandi hyperscaler l'elettricità non è più soltanto una voce dei costi operativi, sta diventando uno dei fattori che determinano dove, quanto rapidamente e con quale scala possa crescere la capacità di calcolo.

Dai data center alla Difesa

Il fenomeno assume una dimensione ancora diversa quando si osserva ciò che sta accadendo nel settore della Difesa. Negli Stati Uniti, l'U.S. Army sta sviluppando attraverso il Janus Program microreattori destinati alle installazioni militari con l'obiettivo di assicurare energia sicura, resiliente e affidabile alle missioni critiche.

Nell'agosto 2026 l'Esercito americano ha selezionato cinque aziende e cinque prime installazioni, mettendo a disposizione fino a 2,2 miliardi di dollari nell'ambito di un modello nel quale i reattori saranno posseduti, costruiti e gestiti dagli operatori industriali. I sistemi previsti avranno potenze inferiori a 20 MWe e l'obiettivo indicato è arrivare all'operatività del primo reattore entro settembre 2028. Con il contributo del capitale privato, l'US Army prevede che il programma possa portare nel



tempo oltre venti microreattori nelle installazioni della Difesa statunitense.

La scala è profondamente diversa rispetto a quella di una grande centrale o anche di molti SMR destinati alla rete. Un microreattore può essere concepito per alimentare un'installazione, una porzione di essa o una microrete, garantendo localmente una capacità di generazione indipendente o complementare alla rete esterna.

Per le Forze armate questo significa qualcosa di più della semplice disponibilità di energia: significa resilienza e continuità della missione.

Una moderna installazione militare dipende

sempre più da radar e sensori, segmenti terrestri dei sistemi satellitari, comunicazioni, sistemi di comando e controllo, capacità cyber, guerra elettronica, piattaforme autonome e infrastrutture di calcolo dedicate all'intelligenza artificiale.

La catena diventa quindi sempre più stretta:
energia → calcolo → informazione → decisione → capacità operativa.

Se viene compromesso il primo anello, anche gli altri possono essere progressivamente degradati. In uno scenario di crisi o conflitto, inoltre, la vulnerabilità non riguarda soltanto gli impianti di generazione. Reti, sottostazioni, sistemi di controllo e infrastrutture di comunicazione possono essere interessati da attacchi fisici, cyber o ibridi, generando effetti a cascata sulle funzioni essenziali.

Non sorprende quindi che la NATO consideri ormai la disponibilità di energia resiliente una componente della capacità di difesa e richieda agli Alleati di rafforzare la protezione delle infrastrutture critiche e la capacità di assicurare le forniture energetiche alle forze militari anche in condizioni di crisi. I nuovi "Baseline Requirements for Resilience", pubblicati nel settembre 2026, dedicano uno specifico requisito proprio alla continuità delle forniture energetiche e alla capacità di reagire e recuperare dopo un'interruzione.

Il punto, quindi, non è stabilire che ogni infrastruttura strategica debba dotarsi di un reattore nucleare, ma è quello di adottare un approccio requirements-driven e resilience-by-design: individuare innanzitutto quali funzioni devono continuare a operare durante una crisi, per quanto tempo, con quale livello di autonomia e con quali ridondanze; successivamente dimensionare il fabbisogno energetico e, solo alla fine, individuare la combinazione tecnologica più appropriata.

Rete elettrica, generazione distribuita, rinnovabili, accumuli, microgrid, sistemi di emergenza e fonti programmabili possono così concorrere, con pesi differenti, alla costruzione di un'architettura resiliente. In alcune applicazioni future anche SMR e microreattori potrebbero diventare una delle opzioni disponibili.

Energia e potenza di calcolo

È qui che il rapporto tra intelligenza artificiale, data center ed energia nucleare assume una dimensione strategica più ampia.

La capacità di sviluppare sistemi avanzati di AI dipenderà sempre più non soltanto dalla disponibilità di algoritmi e semiconduttori, ma anche dalla possibilità di alimentare grandi infrastrutture di calcolo con energia sufficiente, affidabile, sostenibile e competitiva.

Energia, capacità computazionale, semiconduttori, cloud, comunicazioni e infrastrutture spaziali stanno progressivamente entrando nello stesso ecosistema strategico.

La competizione tecnologica dei prossimi anni potrebbe quindi essere determinata non soltanto da chi saprà sviluppare i processori o gli algoritmi più avanzati, ma anche da chi saprà costruire e proteggere l'infrastruttura energetica e digitale necessaria a farli funzionare in modo continuo e resiliente.



leonardo.com

Eurofighter Typhoon: tecnologia, prestazioni e sicurezza.



L'Eurofighter Typhoon, il più importante programma aeronautico della storia industriale europea, è un avanzato caccia multiruolo ordinato da nove forze aeree per un totale di 769 esemplari. Leonardo svolge un ruolo chiave nella produzione di componenti aeronautici ed elettronici del velivolo ed è responsabile dell'assemblaggio finale dei caccia ordinati da Italia e Kuwait Protezione dei cieli h24, 365 giorni all'anno, oltre 400 fornitori e 100.000 posti di lavoro in tutta Europa, di cui oltre 24.000 in Italia.

LEONARDO
TECHNOLOGY FOR A SAFER FUTURE


AI Generate

IL MARE, NUOVA FRONTIERA STRATEGICA DELL'INTELLIGENZA ARTIFICIALE

La competizione per la supremazia digitale spinge le potenze tecnologiche a ripensare l'architettura dei data center. Cina e Stati Uniti sperimentano infrastrutture offshore e sottomarine dove energia, raffreddamento e capacità di calcolo sono integrati in un unico sistema



La competizione tecnologica per l'intelligenza artificiale sta producendo una conseguenza che va ben oltre l'evoluzione dei processori: la capacità di calcolo dipende sempre più dalla disponibilità di energia, dall'acqua e dai sistemi di raffreddamento, ma anche dallo spazio fisico necessario per ospitare infrastrutture sempre più grandi. L'espansione degli "hyperscale data center" sta infatti trasformando il territorio in una risorsa strategica, con campus che richiedono vaste superfici, nuove reti elettriche e infrastrutture di supporto. Secondo un rapporto del 2026 dell'Università delle Nazioni Unite, il land footprint globale, associato ai data center che alimentano l'IA, potrebbe superare entro il 2030 i 14.500 km², mentre i consumi elettrici potrebbero raggiungere 945 TWh. È anche per questo che l'industria tecnologica guarda oltre la terraferma, verso il mare e, in prospettiva, verso lo spazio. Lo spazio rappresenta, oggi, ancora una frontiera pionieristica: Starcloud, startup sostenuta dal programma NVIDIA Inception, sta sviluppando l'idea di data center orbitali alimentati dall'energia solare e ha indicato come obiettivo futuro un'infrastruttura da 5 GW in orbita.

La Cina sta sperimentando la soluzione del mare nella zona speciale di Lin-gang, a una decina di chilometri dalla costa di Shanghai, dove moduli contenenti server vengono immersi nel Mar Cinese Orientale. L'acqua marina viene utilizzata come sistema naturale di dissipazione del calore, mentre l'infrastruttura energetica offshore punta a integrare la produzione eolica con il funzionamento dei sistemi informatici. Il progetto dovrebbe raggiungere 24 megawatt di capacità, con un investimento indicato in circa 1,6 miliardi di yuan. Secondo le stime diffuse per il progetto, il sistema potrebbe ridurre del 22,8 per cento il consumo energetico rispetto a un data center convenzionale, limitare quasi completamente l'impiego di acqua dolce per il raffreddamento

e ridurre di oltre il 90 per cento il terreno necessario. Più del 95 per cento dell'elettricità dovrebbe inoltre provenire da fonti rinnovabili. Se questi risultati saranno confermati su scala industriale, il modello potrebbe offrire alla Cina una nuova modalità per espandere la capacità di calcolo, senza concentrare ulteriormente infrastrutture e consumi sulla terraferma. Pechino dispone già di un'esperienza significativa, dal 2022 HiCloud ha sperimentato a Hainan moduli installati a oltre 30 metri di profondità, verificando il comportamento delle apparecchiature e dei sistemi di alimentazione in condizioni sottomarine. La questione assume, comunque, una dimensione strategica perché l'intelligenza artificiale sta trasformando il rapporto tra energia e potere tecnologico. Un Paese capace di disporre di grandi quantità di elettricità a costi sostenibili e di trasformarle rapidamente in capacità computazionale acquisisce un vantaggio nella ricerca, nell'industria, nella difesa e nell'elaborazione delle informazioni.

Il mare può contribuire a questa equazione offrendo contemporaneamente spazio, raffreddamento e accesso a nuove fonti energetiche anche se non rappresenta una soluzione priva di vulnerabilità. Il calore prodotto dai server, infatti, non viene eliminato ma trasferito all'ambiente marino, con eventuale aumento della temperatura dell'acqua che potrebbe modificare la quantità di ossigeno disciolto e incidere sugli ecosistemi locali. Per il precedente progetto di Hainan, HiCloud ha indicato un aumento inferiore a un grado Celsius, nei pressi dell'infrastruttura e la presenza di fauna marina invariata nelle immediate vicinanze.

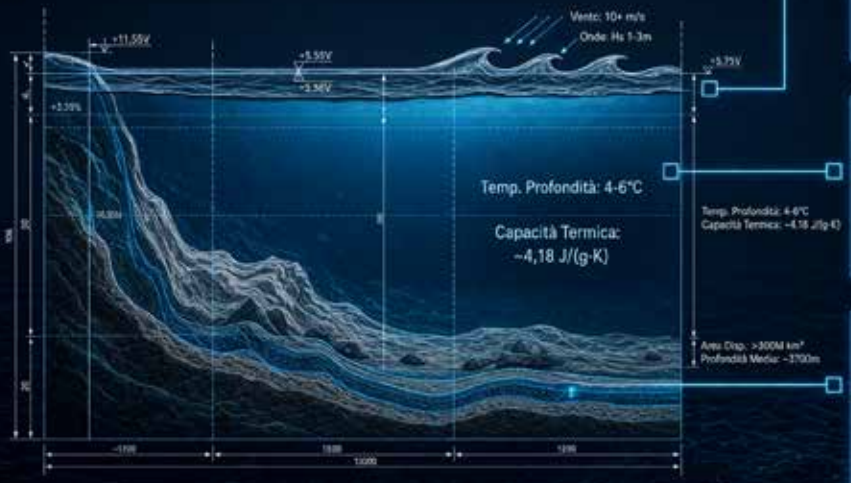
Il problema potrebbe diventare ancora più rilevante però con l'aumento delle dimensioni perchè HiCloud, insieme a Shenergy, China Telecom e altri partner, hanno previsto un progetto offshore da 500 megawatt, oltre venti volte la capacità prevista per Lin-gang.

Sul versante statunitense, Microsoft ha sperimentato con Project Natick data center sottomarini alimentati anche attraverso infrastrutture energetiche offshore. Panthalassa, società tecnologica con sede a Portland, sta sviluppando, invece, infrastrutture oceaniche nelle quali la produzione di energia e il calcolo vengono concentrati nella stessa struttura. Nel maggio 2026 l'azienda ha raccolto 140 milioni di dollari in un finanziamento guidato da Peter Thiel (Palantir), portando la propria valutazione vicino al miliardo di dollari. Il principio dei suoi "nodes" è diverso da quello cinese. Le strutture, lunghe circa 85 metri, sono progettate per utilizzare il movimento delle onde per produrre energia.

Il moto verticale dell'oceano viene trasformato attraverso un sistema meccanico in elettricità destinata direttamente ai sistemi informatici installati a bordo, mentre l'acqua marina contribuisce al raffreddamento dei server. Panthalassa prevede, inoltre, l'utilizzo di comunicazioni satellitari, compresa Starlink, per collegare le infrastrutture oceaniche con gli utenti a terra. I primi deployment sono previsti nel Pacifico settentrionale, con applicazioni commerciali indicate dalla società a partire dal 2027.

In chiave di sicurezza nazionale, i data center in mare non rappresentano soltanto una soluzione energetica, ma l'emergere di una possibile nuova componente dell'infrastruttura strategica di uno Stato, capace di integrare energia, capacità computazionale e connettività. Il modello offre opportunità per sostenere la crescente domanda di calcolo legata all'intelligenza artificiale, anche nel settore della Difesa, ma introduce nuove vulnerabilità legate a condizioni ambientali estreme, manutenzione, sicurezza fisica e resilienza delle comunicazioni. La convergenza tra infrastrutture oceaniche, reti sottomarine, sistemi energetici, dominio spaziale e cyberspazio potrebbe quindi trasformare il mare in un nuovo ambiente strategico della potenza computazionale, in una competizione nella quale energia e capacità di calcolo diventano elementi sempre più rilevanti della sicurezza nazionale.

Il Paradigma Oceanico: Una Soluzione Tripartita



1. Superficie (Energia Diretta)

Integrazione nativa con fonti offshore (eolico, moto ondoso). Bypass delle reti elettriche terrestri sature.

2. Colonna d'Acqua (Raffreddamento Passivo)

Dissipazione termica naturale e infinita. Eliminazione totale dell'uso di acqua dolce potabile, criticità dei sistemi terrestri.

3. Fondale / Orizzonte (Spazio Illimitato)

Zero competizione con aree urbane, industriali oigre cole. Scalabilità geografica senza precedenti.

Il Modello Cinese: Immersione Profonda



Profile

Progetto Attivo:	Lin-gang (Shanghai)
Capacità:	24 MW (Obiettivo: 500 MW)
Investimento:	~1,6 miliardi di Yuan

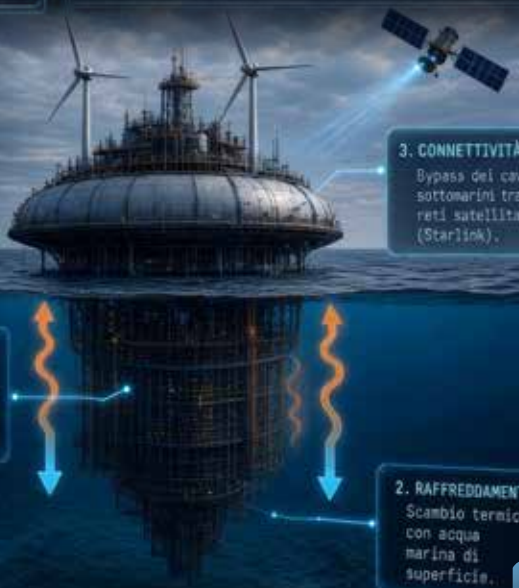
-22,8%	-90%	>95%
Consumo energetico	Consumo di suolo	Alimentazione rinnovabile

Dashboard

Background: Sperimentato dal 2022 a Hainan (HiCloud) a >30m di profondità.

Filosofia Strategica: Usare l'oceano come un gigantesco dissipatore di calore passivo per estendere la capacità di calcolo nazionale senza gravare sulla rete terrestre.

Il Modello Statunitense: Nodi di Superficie Attivi



Infrastruttura: Panthalassa
Deployment: 2027, Pacifico settentrionale
Precedente: Microsoft Project Natick

Dimensioni Nodo: Strutture pelagiche (85m)
Valutazione: ~$1 Miliardo

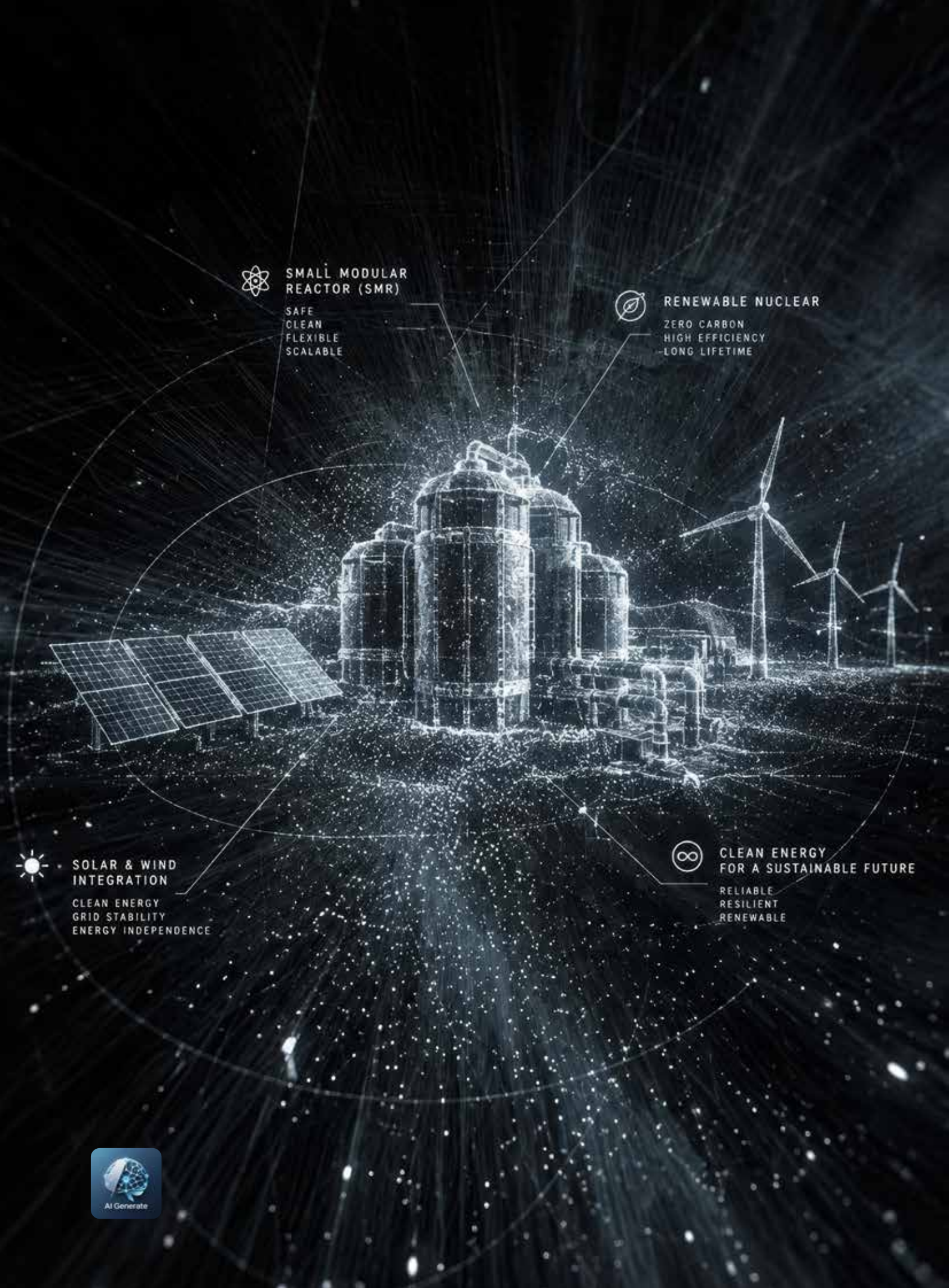
Finanziamento: 140M$ (Maggio 2026)
Valutazione: ~$1 Miliardo

1. GENERAZIONE: Conversione meccanica diretta del moto ondoso in elettricità.

2. RAFFREDDAMENTO: Scambio termico con acqua marina di superficie.

3. CONNETTIVITÀ: Bypass dei cavi sottomarini tramite reti satellitari (Starlink).

AI Generated


SMALL MODULAR REACTOR (SMR)
SAFE
CLEAN
FLEXIBLE
SCALABLE
RENEWABLE NUCLEAR
ZERO CARBON
HIGH EFFICIENCY
LONG LIFETIME
SOLAR & WIND INTEGRATION
CLEAN ENERGY
GRID STABILITY
ENERGY INDEPENDENCE
CLEAN ENERGY FOR A SUSTAINABLE FUTURE
RELIABLE
RESILIENT
RENEWABLE
AI Generate

ANDREA CELESTI

«CORRIERE DELLA SERA»

RINNOVABILI E NUCLEARE
La sfida per l'Europa del futuro

Nel 2024 le rinnovabili hanno raggiunto il 47,4% della produzione elettrica europea, superando nettamente il nucleare. L'Europa punta ora a integrare fonti rinnovabili e atomo di nuova generazione per rafforzare sicurezza, autonomia e sovranità energetica



I dati ufficiali Eurostat relativi al 2024 delineano in modo inequivocabile la nuova geografia energetica del Vecchio Continente: oggi le fonti rinnovabili sono il vero motore d'Europa, con una produzione di 1.326 TWh pari al 47,4% del totale. Si tratta di una cifra che supera di oltre il doppio il contributo dell'energia nucleare, attestatasi a 649 TWh (il 23,3%). A completare il quadro figurano il gas naturale con 602 TWh (21,5%) e il carbone al 7,6% (212 TWh). Il dato da cui partire è proprio questo: ad oggi le rinnovabili in Europa producono ben più energia rispetto al nucleare, guidando una transizione che nell'ultimo decennio ha visto le fonti pulite crescere, con l'atomo che si è mantenuto stabile attorno alla sua soglia storica, con la produzione concentrata in soli 12 Paesi membri su 27.

Questa trasformazione ha già portato benefici tangibili sia sul fronte ambientale sia su quello degli scambi commerciali: nel settore elettrico dell'Ue si è registrato un crollo del 57% delle emissioni di gas serra rispetto al 1990, accompagnato da un taglio del 18% delle importazioni di gas nel 2024 rispetto al 2023. La rotta verso la decarbonizzazione evidenzia come sole, vento e acqua siano diventati pilastri fondamentali dell'indipendenza energetica comunitaria.

Un'Europa divisa

Dietro la media europea si nasconde, tuttavia, un continente profondamente divisa nelle sue strategie nazionali, dove i principali attori si muovono in direzioni opposte. A guidare i due blocchi sono Parigi e Berlino. La Francia si conferma il gigante atomico d'Europa con 380,5 TWh prodotti da fonte nucleare (il 67,3% del proprio fabbisogno) e rinnovabili al 27,4% (154,7 TWh). Al contrario, la Germania ha completato il suo progressivo addio all'atomo – sceso all'11,6% (22,8 TWh) prima dello spegnimento definitivo delle ultime centrali – scommettendo sul green che oggi copre il 59,4% della produzione tedesca (233,4 TWh). La spaccatura attraversa l'intero continente: la Polonia, ad esempio, ha deciso di azzerare la dipendenza dal carbone programmando sei reattori entro il 2043 con il primo cantiere a Lubiatowo-Kopalino dal 2028; la Spagna,

di contro, ha confermato la dismissione dei suoi sette reattori attivi entro il 2035. In questo scenario si inserisce l'Italia con un mix di 309 TWh, dove le rinnovabili coprono quasi la metà della domanda (149,1 TWh), ma il gas mantiene un ruolo ancora centrale al 42,7% (132,3 TWh). Priva di produzione nucleare interna, l'Italia ha avviato una svolta con l'approvazione del ddl delega per il ritorno dell'atomo a fine settembre di quest'anno: l'obiettivo del Governo è installare i primi impianti tra il 2033 e il 2034, puntando sulla tecnologia di nuova generazione dei Reattori Modulari Piccoli (SMR) e di quarta generazione (AMR), valorizzando la ricerca di startup come Newcleo, il progetto Nuward del colosso transalpino EDF e la neonata Nuclitalia.

Un nuovo Polo Nucleare Europeo

Di fronte alle vulnerabilità mostrate dalle recenti crisi internazionali – dal conflitto in Ucraina alle minacce di blocco nello stretto di Hormuz – la ricerca della stabilità energetica è diventata una priorità. Al Nuclear Energy Summit di Parigi del 10 marzo, la Presidente della Commissione Europea, Ursula von der Leyen, ha definito l'uscita affrettata dal nucleare un vero e proprio "errore strategico", facendosi promotrice della nascita di un Polo Europeo per l'energia nucleare di nuova generazione.

L'obiettivo dell'Ue è chiaro: spezzare la dipendenza dal gas russo e dai fornitori del Nord Africa per creare un sistema energetico flessibile, sicuro e sovrano. Il perno di questa strategia





risiede come detto negli SMR, mini-reattori modulari compatti, più economici e rapidi da costruire rispetto alle centrali tradizionali, pensati per entrare in funzione all'inizio degli anni '30. Nella visione europea, l'atomo di nuova generazione non nasce per frenare la corsa delle rinnovabili, ma per sostenerla. Se il solare e l'eolico generano l'elettrone più economico e pulito, soffrono inevitabilmente delle condizioni atmosferiche; il nucleare, al contrario, garantisce quella stabilità capace di erogare elettricità continua 24 ore su 24, 365 giorni all'anno.

Verso il futuro: alla ricerca di un sistema perfetto

La grande partita energetica dell'Europa non si giocherà dunque su uno scontro ideologico tra rinnovabili e nucleare, ma sulla capacità di fondere queste due tecnologie in un unico mix. Le prime hanno conquistato la maggioranza della produzione elettrica europea e tracciato la strada dei prossimi anni.

Se l'Unione saprà superare le differenze a livello nazionale, l'alleanza tra le rinnovabili e il nucleare non sarà solo una scelta politica, ma l'atto di nascita della vera sovranità energetica: il momento in cui l'Europa smetterà finalmente di subire le crisi degli altri per tornare a scrivere il proprio futuro.

PUBBLIREDAZIONALE

ETS
ENGINEERING & TECHNICAL SERVICES

Da oltre trent'anni ETS S.p.A. - Engineering and Technical Services opera nel settore dell'ingegneria, accompagnando enti pubblici e operatori privati nella progettazione e nella realizzazione di infrastrutture e impianti caratterizzati da elevata complessità tecnica. Quotata su Euronext Growth Milan, la società ha costruito nel tempo un posizionamento fondato su competenze multidisciplinari, capacità progettuale e diversificazione dei mercati di riferimento. Fondata nel 1992 dagli ingegneri *Donato Romano* e *Giambattista Parietti*, ETS S.p.A. offre un modello integrato di servizi che comprende studi di fattibilità tecnico-economica, progettazione definitiva ed esecutiva, direzione lavori, coordinamento della sicurezza e project management. A queste attività si affiancano competenze specialistiche nei collaudi, nella prevenzione incendi, nell'ottimizzazione energetica, nell'acustica, nel facility management e nei rilievi topografici. Il know-how maturato consente alla società di operare in settori diversificati: infrastrutture, edilizia sanitaria e residenziale e, soprattutto, comparti ad alta intensità tecnologica definiti *mission critical*, tra cui data center, aeroporti e impianti nucleari. Sono ambiti nei quali affidabilità, continuità operativa, sicurezza e precisione progettuale assumono un ruolo centrale. In questa prospettiva si inserisce il consolidamento delle competenze nel settore nucleare. ETS S.p.A. ha già un contratto quadro per servizi di ingegneria con SOGIN ed è membro dell'Associazione Italiana Nucleare, oltre che dell'Italian Data Center Association e di ANIMP. Nel 2025 la società ha inoltre costituito ETS NH, con sede a Bergamo, dedicata alla progettazione, direzione lavori e servizi tecnici per impianti nucleari e per le infrastrutture legate alla produzione, allo stoccaggio e al trasporto dell'idrogeno. Nell'ambito dell'operazione l'acquisizione di BAQ (SUISSE) SA di Ginevra, spin off del CERN, specializzata nei servizi di ingegneria e consulenza per il nucleare e la sicurezza ambientale. La strategia di ETS S.p.A. guarda quindi ai settori destinati a caratterizzare l'evoluzione dell'ingegneria energetica e infrastrutturale europea, con l'obiettivo di consolidare la presenza nei comparti dell'energia, delle infrastrutture innovative e delle tecnologie di nuova generazione. A completare il profilo aziendale è l'investimento nella trasformazione digitale: ETS S.p.A. dispone della certificazione BIM secondo la UNI/PdR 74:2019 e di un team di professionisti certificati. Un patrimonio di competenze che sostiene la crescita della società e ne rafforza la capacità di operare su progetti complessi, in Italia e sui mercati internazionali.

ETS NH
NUCLEAR & HYDROGEN



GIANCLAUDIO TORLIZZI

FONDATORE DI T-COMMODITY

TERRE RARE, LA VERA BATTAGLIA È SUL MAGNETE

La vera sfida sulle terre rare non è soltanto estrarle, ma trasformarle in magneti. L'Europa dipende dalla Cina per quasi tutta la filiera, per Difesa e industria serve una strategia che unisca produzione, riciclo, investimenti e domanda

Per anni l'Europa ha affrontato il tema delle materie prime critiche partendo da un presupposto sbagliato: che il problema fosse essenzialmente minerario. Se dipendiamo dalla Cina, si è detto, dobbiamo aprire nuove miniere, diversificare le forniture, costruire raffinerie e accumulare scorte. Tutto corretto, ma non sufficiente, perché mentre l'Occidente cercava nuovi giacimenti, Pechino spostava il campo di battaglia molto più avanti lungo la catena del valore.

La vera partita oggi non si gioca sulla terra rara estratta, ma sul componente industriale nel quale quella terra rara viene incorporata. E nel caso di neodimio, praseodimio, disprosio e terbio il componente decisivo è il magnete permanente. Senza magneti ad alte prestazioni non ci sono F-35, missili, droni, radar e satelliti. Ma non ci sono neppure motori elettrici, robot industriali e turbine eoliche. È qui che la dipendenza occidentale dalla Cina diventa realmente strategica.

I numeri aiutano a capire. Nel 2024 la Cina ha esportato 5.229 tonnellate di neodimio-praseodimio sotto forma di minerali e concentrati. Ma ne ha esportate 17.394 tonnellate incorporate nei magneti. È un rapporto di oltre tre a uno. Lo stesso fenomeno riguarda il gallio: 101 tonnellate esportate come materiale contro 190 incorporate nei wafer. In altre parole, una quota crescente della dipendenza occidentale non compare più nelle statistiche sulle materie prime, perché viaggia nascosta dentro i prodotti industriali. Ed è esattamente questa la strategia perseguita dalla Cina negli ultimi dieci anni. Controllare il monte della filiera, utilizzare sussidi e pressione sui prezzi per indebolire i concorrenti e conquistare progressivamente le lavorazioni a maggiore valore aggiunto. Il risultato è che possiamo anche trovare una miniera alternativa in Australia, Canada o Africa, ma se poi quel materiale deve entrare nella capacità industriale cinese per diventare lega, magnete e componente, non abbiamo eliminato la dipendenza: l'abbiamo semplicemente spostata.

Non è un dettaglio, perché Pechino sta adattando proprio a questa realtà la propria politica commerciale. I controlli all'esportazione non si fermano più alle materie prime. La Cina ha già limitato l'accesso



ad alcune tecnologie e attrezzature necessarie all'estrazione, alla raffinazione e alla produzione di batterie. Il salto strategico è evidente: colpire non soltanto ciò che l'Occidente compra dalla Cina, ma potenzialmente anche gli strumenti che gli servono per emanciparsi dalla Cina.

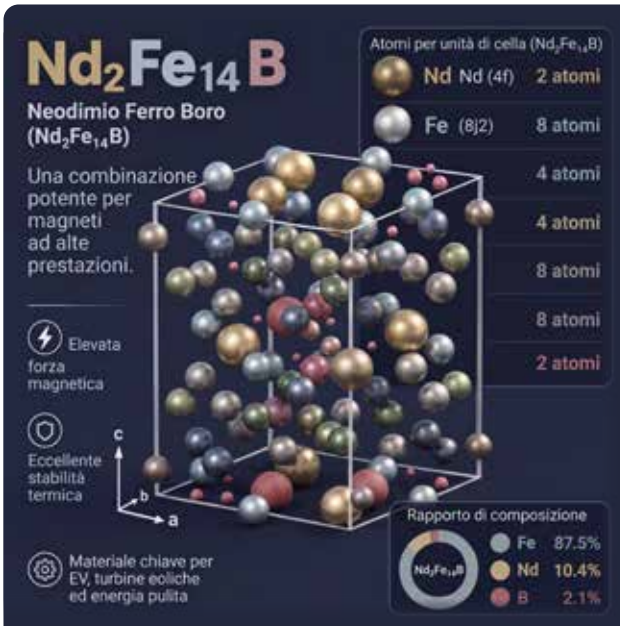
Ecco perché la sicurezza delle materie prime non può più essere considerata una politica mineraria, ma deve diventare una politica industriale. Prendiamo ad esempio i magneti permanenti. Il mercato europeo vale nell'ordine dei 5-8 miliardi di dollari, mentre il solo segmento NdFeB vale circa 4,5 miliardi. Ma il dato veramente importante è un altro: l'Europa consuma circa 16.000 tonnellate l'anno di magneti NdFeB e circa il 98% del fabbisogno viene coperto dalle importazioni, prevalentemente cinesi. La produzione interna si ferma al 2-3%. Con una domanda spinta da decarbonizzazione, robotica e riarmo, il consumo europeo potrebbe arrivare a 30.000-35.000 tonnellate entro il 2035.

Significa che stiamo costruendo contemporaneamente elettrificazione e riarmo europeo sopra una filiera industriale che quasi non controlliamo.

Per la Difesa il problema è ancora più evidente. Il fabbisogno militare è relativamente piccolo in termini quantitativi, ma è praticamente non sostituibile dal punto di vista tecnologico. I magneti NdFeB e SmCo entrano nei sistemi più sofisticati. Le stime citate nel documento indicano per un F-35 circa 40-70 chilogrammi di materiali contenenti terre rare. Negli Stati Uniti il fabbisogno di magneti specializzati per la Difesa potrebbe raggiungere le 10.000 tonnellate l'anno entro il 2030, rispetto alle 3.000-4.000 attuali. In Europa, invece, non esiste ancora una stima ufficiale consolidata del fabbisogno militare complessivo.

La parola chiave non deve essere "sussidio", deve essere "sincronizzazione". Non finanziare singoli progetti, ma costruire una filiera nella quale estrazione, separazione, produzione delle leghe, magneti e domanda industriale procedano secondo una tempistica coerente. Una campagna industriale di cinque-dieci anni, alimentata da flussi finanziari certi e progressivi. Perché la certezza del capitale conta spesso più della sua quantità.

L'Italia, inoltre, non deve necessariamente possedere la miniera per controllare la filiera perché può investire in progetti estrattivi e di



MAGNETI NdFeB PICCOLI E STRATEGICI

I magneti NdFeB (neodimio-ferro-boro) sono magneti permanenti realizzati principalmente con neodimio, ferro e boro. Sono tra i magneti più potenti oggi disponibili e proprio per questo sono fondamentali in numerose tecnologie avanzate. Il loro principale vantaggio è l'elevata densità di energia magnetica, che permette di ottenere grandi prestazioni utilizzando componenti molto più piccoli e leggeri rispetto ai magneti tradizionali. Sono quindi impiegati nei motori elettrici delle automobili, in particolare nei veicoli elettrici, nei generatori delle turbine eoliche, nei droni e nella robotica, oltre che in numerosi dispositivi elettronici. Si trovano anche in hard disk, altoparlanti, sensori, apparecchiature medicali e sistemi industriali. In ambito militare e aerospaziale entrano in diversi sistemi che richiedono motori, attuatori, sensori e componenti elettrici compatti e ad alte prestazioni. La loro importanza strategica deriva soprattutto dal fatto che la produzione dei magneti NdFeB richiede terre rare, in particolare il neodimio e, per alcune applicazioni ad alte temperature, il disprosio e il terbio. Per questo il controllo della filiera non riguarda soltanto l'estrazione delle materie prime, ma anche la loro separazione, raffinazione, trasformazione in leghe e produzione dei magneti. È proprio in quest'ultimo passaggio industriale che si concentra una parte decisiva della dipendenza europea dalla Cina.

Timeline di attuazione

Fase 0
Fondazioni

01

0-12 mesi

Cabina di regia a Palazzo Chigi; mappatura asset e PMI; primi contratti di offtake e lettere d'intenti; sportello unico per l'accesso ai programmi pubblici

Fase 1
Circolarità e servizi

02

16-36 mesi

Avvio impianti di riciclo magneti (urban mining); flussi pluriennali alle PMI di servizi; partenza percorsi ITS e universitari

Fase 2
Capacità industriale

03

3-6 anni

Polo nazionale dei magneti (NdFeB/SmCo) operativo; impianti modulari su aree demaniali e ZES; fondo di co-investimento a regime

Fase 3
Consolidamento

04

6-10 anni

Quota crescente di magnete finito prodotto in Italia/UE; candidatura a stockpile europeo; esportazione verso alleati

Fabbisogno finanziario indicativo

Contratti di offtake e price floor: impegni pluriennali della Difesa e dei gruppi pubblici, a costo di bilancio contenuto ma ad alto effetto leva

Polo nazionale dei magneti: investimento pubblico-privato iniziale nell'ordine delle centinaia di milioni di euro, con quota pubblica di minoranza

PMI: programma da 5-10 milioni di euro l'anno per beneficiario, per cinque anni, in luogo di grandi contributi una tantum

Circolarità: leva sui fondi europei (RESourceEU, programmi CRMA) per gli impianti di riciclo e urban mining

Formazione: finanziamento ordinario di ITS e corsi universitari dedicati, con borse legate a impegni occupazionali nella filiera

Fonte: © Ministero della Difesa - Strategia nazionale per le terre rare - luglio 2026

AI Generate

raffinazione nei Paesi alleati e concentrare sul territorio nazionale l'ultimo miglio industriale: il magnete. Il modello dovrebbe partire dalla domanda. Prima si mappano i fabbisogni delle imprese della Difesa; poi, attraverso le partecipate, si individuano gli asset minerari esteri; quindi si utilizzano contratti pluriennali di acquisto e prezzi minimi garantiti per dare bancabilità agli investimenti e alimentare un polo nazionale dei magneti NdFeB e SmCo.

C'è poi un vantaggio italiano che viene spesso sottovalutato: il riciclo. Se non abbiamo grandi giacimenti di terre rare, abbiamo uno dei sistemi industriali di riciclo più sviluppati d'Europa. Motori elettrici, dischi rigidi, apparecchiature industriali e turbine dismesse possono trasformarsi nella nostra miniera. L'urban mining deve diventare parte integrante della sicurezza nazionale delle materie prime.

Ma serve soprattutto capitale e qui bisogna abbandonare l'idea secondo cui interesse nazionale e rendimento finanziario siano necessariamente in conflitto. Un fondo di coinvestimento tra CDP e capitale privato potrebbe acquisire, ricapitalizzare e consolidare impianti metallurgici, aziende della chimica di processo e fornitori specializzati. Lo Stato dovrebbe stabilire le priorità, assorbire parte del rischio politico e garantire domanda stabile. Il capitale privato dovrebbe fare quello che sa fare meglio: selezionare gli asset, finanziare la crescita e imporre disciplina industriale.

Il punto è anche evitare l'errore americano: concentrare miliardi su pochi grandi campioni lasciando senza ossigeno finanziario società junior, laboratori, ingegneria, impianti pilota e PMI specializzate. Sono questi gli anelli invisibili senza i quali la grande fabbrica finanziata dallo Stato rischia di rimanere un capannone senza filiera. Il documento propone per questo flussi relativamente piccoli ma continuativi, nell'ordine di 5-10 milioni di euro l'anno per cinque anni, accompagnati dalla formazione di tecnici specializzati in metallurgia delle terre rare e chimica di separazione.

La collaborazione con altri Paesi è d'obbligo. Stati Uniti, Europa e alleati devono costruire un mercato sufficientemente grande da consentire alle nuove filiere di raggiungere economie di scala. Una guerra di sussidi, requisiti nazionali e barriere commerciali fra Paesi occidentali finirebbe paradossalmente per rafforzare il vantaggio cinese.

L'obiettivo deve quindi essere misurabile. Non quante miniere abbiamo finanziato, non quanti memorandum abbiamo firmato, non quanti impianti abbiamo inaugurato, ma quante tonnellate di magnete finito siamo realmente in grado di consegnare.

Con una domanda europea prevista a 30.000-35.000 tonnellate nel 2035, un obiettivo del 30% richiederebbe una capacità europea di circa 9.000-10.500 tonnellate annue. Un'autonomia del 50% nel 2045 significherebbe superare le 17.000-20.000 tonnellate. Questo è il KPI che dovrebbe finire sul tavolo di Palazzo Chigi.





Il tuo futuro, il nostro impegno.

Costruiamo un futuro migliore per le prossime generazioni attraverso **soluzioni energetiche innovative e responsabili**, per ridurre al minimo l'impatto ambientale.

ENEL.IT

enel

STEFANO PIAZZA
«Panorama/La Verità»

Xi Jinping e il ritorno dell'uomo forte per una Cina destinata a dominare il XXI secolo



Con Xi Jinping la Cina concentra il potere nelle mani di un solo leader. Epurazioni, controllo del Partito e pianificazione strategica fino al 2049 sostengono l'ambizione di fare di Pechino la principale potenza del XXI secolo, ma aumentano anche i rischi legati all'assenza di contrappesi e successioni

Tappeto rosso, sorvoli militari e una cena di Stato hanno accompagnato l'ultimo incontro alla Casa Bianca tra Donald Trump e Xi Jinping. Alla ricchezza del cerimoniale non ha però corrisposto una svolta nei rapporti tra Washington e Pechino. Il risultato più concreto è una proroga di due mesi della distensione commerciale, mentre restano aperte le divergenze sulla tecnologia, su Taiwan e sul sostegno cinese all'Iran. I due presidenti hanno esibito cordialità, evitando di approfondire pubblicamente le questioni più controverse. La visita, destinata a proseguire venerdì, ha inoltre provocato malumori tra i repubblicani, alcuni dei quali contestano l'accoglienza concessa al principale rivale strategico degli Stati Uniti. Sul commercio, le delegazioni hanno concordato di spostare al 10 gennaio la scadenza dell'intesa esistente. L'obiettivo è concedere ai negoziatori altro tempo per costruire un accordo più ampio, senza interrompere la tregua in corso. La soluzione resta tuttavia lontana dalle aspettative cinesi: Pechino avrebbe preferito un prolungamento di due anni, capace di assicurare maggiore stabilità ai rapporti economici. Il compromesso raggiunto rinvia dunque il confronto, ma non scioglie i nodi che continuano a dividere le due economie. Non sono stati annunciati altri progressi sostanziali in grado di modificare il quadro delle controversie commerciali. Una parte importante della trattativa riguarda gli acquisti agricoli, tema particolarmente sensibile per gli Stati americani produttori e per gli elettori repubblicani. La Cina ha accettato di comprare 25 milioni di tonnellate di soia statunitense. Il segretario al Tesoro Scott Bessent ha spiegato che Pechino sta rispettando con particolare impegno questa parte dell'accordo, mentre procede più lentamente su altre obbligazioni agricole, per un valore complessivo di circa 17 miliardi di dollari. Washington continua a sollecitarne l'attuazione. Bessent ha inoltre collegato ulteriori acquisti a un meccanismo da lui descritto come un «consiglio commerciale», senza che dal vertice



emergessero dettagli sufficienti a chiarirne il funzionamento. Dietro il negoziato economico rimane la questione di Taiwan. Secondo il resoconto dell'agenzia ufficiale Xinhua, durante il colloquio riservato Xi ha chiesto agli Stati Uniti di assumere una posizione esplicitamente contraria all'indipendenza dell'isola, democratica e autogovernata, sulla quale Pechino rivendica la sovranità. Il presidente cinese ha quindi riportato al centro dell'incontro una delle controversie più delicate nei rapporti bilaterali. La richiesta rivolta a Trump riguarda direttamente l'atteggiamento politico di Washington verso Taipei, mentre la Cina continua a perseguire l'obiettivo dell'unificazione e gli Stati Uniti mantengono i propri legami con l'isola.

Washington segue la linea dell'«ambiguità strategica»: contribuisce alla difesa di Taiwan attraverso la vendita di armamenti, senza precisare se interverrebbe militarmente in caso di attacco cinese. A maggio, dopo avere discusso dell'isola con Xi a Pechino, Trump aveva evitato di dire se avrebbe inviato soldati americani in uno scenario del genere. Rimane inoltre in attesa della sua approvazione un pacchetto di armi da 14 miliardi di dollari destinato a Taipei. Diversi parlamentari, anche repubblicani, premono affinché le forniture siano autorizzate. Il dossier resta così sospeso mentre il presidente americano cerca di migliorare il rapporto con il suo interlocutore cinese. Nel suo intervento pubblico, Xi ha invitato le due potenze a evitare una competizione concepita come una «sfida gladiatoria a somma zero». Ha richiamato anche la «trappola di Tucidide», espressione utilizzata per descrivere il rischio che la rivalità tra una potenza dominante e una emergente conduca alla guerra. Il messaggio riprende un tema già affrontato nel precedente vertice di Pechino. Sullo sfondo restano le valutazioni formulate negli anni scorsi da funzionari americani sui preparativi militari cinesi per un possibile conflitto. Alle dichiarazioni sulla necessità di scongiurare lo scontro non si sono accompagnati annunci di intese capaci di ridurre le divergenze su Taiwan.

Anche l'intelligenza artificiale ha trovato spazio nei colloqui, in una fase di forte competizione tecnologica e di crescente preoccupazione per la possibilità che sistemi sempre più avanzati sfuggano al controllo umano. Xi ha sostenuto che Cina e Stati Uniti possiedono sia gli strumenti sia la responsabilità necessari per governarne lo sviluppo nell'interesse collettivo. Ha insistito sulla necessità che la tecnologia rimanga sotto la supervisione delle persone e contribuisca al loro benessere. Trump ha invece lasciato intendere di voler mantenere l'attuale impostazione, con entrambi i Paesi impegnati nella corsa alla supremazia nel settore.

Prima del vertice, Bessent aveva prospettato un sistema di comunicazione reciproca per gli incidenti legati all'intelligenza artificiale che assumano rilevanza per la sicurezza nazionale. L'idea era quella di una linea diretta che permettesse alle due capitali di avvertirsi tempestivamente. Giovedì sera non risultava però chiaro se Trump e Xi avessero effettivamente discusso la proposta. Alla cena di Stato erano presenti alcuni protagonisti americani del settore. Tra le assenze figurava Dario Amodei, amministratore delegato di Anthropic, intervenuto più volte sulla necessità di prendere sul serio i rischi associati allo sviluppo dell'IA. Quanto alla rappresentazione pubblica della visita, Xi ha ottenuto un'accoglienza all'altezza delle richieste cinesi, e per alcuni aspetti superiore. Pechino aveva insistito sul riconoscimento di una piena parità tra i due leader. Trump si è recato personalmente sulla pista d'atterraggio per ricevere l'ospite, un gesto descritto come assai inconsueto per un presidente americano. Sono seguiti gli omaggi militari e il ricevimento ufficiale. Il leader cinese ha annunciato che il suo Paese donerà agli Stati Uniti due panda giganti, aggiungendo un gesto simbolico alla visita.

Trump ha dedicato attenzione anche ai lavori della Casa Bianca, mostrando a Xi il nuovo eliporto sul prato meridionale e soffermandosi sui materiali utilizzati. «Ama il buon granito», ha commentato a proposito dell'ospite. Davanti ai ritratti presidenziali ha inoltre ironizzato su Joe Biden, rappresentato da una firma automatica. La nuova sala da ballo, invece, non era pronta per l'occasione. Durante la cena il presidente americano è rimasto sui convenevoli, senza illustrare il contenuto delle discussioni. Xi ha parlato di una visione condivisa su diverse questioni, ma non ha specificato quali. Le domande sull'Iran e sull'IA non hanno ottenuto chiarimenti sostanziali. L'accoglienza ha alimentato critiche nel Partito repubblicano a sei settimane dalle elezioni di metà mandato.



Il senatore della Louisiana John Kennedy ha definito Xi «un rettile», pur augurando a Trump di riuscire a raggiungere un accordo. Joni Ernst, senatrice dell'Iowa, ha espresso disagio per lo sfarzo del cerimoniale, accompagnandolo alla speranza che la visita produca benefici per gli agricoltori colpiti dalle politiche tariffarie. Thom Tillis, della Carolina del Nord, ha sottolineato la distanza tra gli onori concessi al leader cinese e i messaggi pronunciati nei comizi del movimento MAGA. Mentre Trump accusa i democratici di comunismo, ha osservato Tillis, il tappeto rosso per Xi complica la comunicazione elettorale repubblicana. Il vertice lascia quindi una proroga commerciale limitata, molte immagini di cordialità e i principali dossier ancora aperti.

VITTORIO EMANUELE PARSI

Università Cattolica del Sacro Cuore,
Accademia dei Lincei

Il momento dell'Europa (e del Canada)



L'ordine liberale occidentale affronta una crisi senza precedenti, alimentata da tre minacce intrecciate: l'aggressione russa, la competizione economica cinese e il progressivo disimpegno degli Stati Uniti. Per l'Europa diventa urgente rafforzare autonomia, difesa e coesione democratica

L'ordine internazionale liberale sta affrontando la sua crisi più grave dai tempi della Guerra Fredda, la minaccia a cui è sottoposto, in solido con le istituzioni e le singole democrazie europee, non ha avuto un eguale neppure con gli attacchi terroristici dell'11 settembre 2001 e con la successiva "War on Terror".

Per essere chiari, sostengo da anni che, in termini di minaccia esistenziale per l'ordine liberale e per le democrazie occidentali, il terrorismo jihadista è stato ampiamente sopravvalutato. Per quanto riguarda gli Stati Uniti, paradossalmente, le conseguenze più deleterie per la società americana sono arrivate, dalla legislazione emergenziale adottata sulla spinta dello shock postraumatico dell'11 settembre, che hanno indebolito i meccanismi di checks and balance e consentito l'assalto alle garanzie costituzionali, a cominciare dalla separazione dei poteri e dalla centralità del Congresso.

La mia riflessione riguarderà soprattutto il destino delle democrazie europee e della stessa Unione Europea, perché ritengo che oggi sia essenzialmente l'Europa, con l'aggiunta del Canada e delle democrazie consolidate del Pacifico, a rappresentare quel che rimane dell'Occidente postbellico, fondato sulla triade costituita dalla democrazia rappresentativa, dall'economia di libero mercato e dalla società aperta.



Oggi, la minaccia che le democrazie occidentali si ritrovano a dover fronteggiare è triplice e completamente inedita nella sua composizione e morfologia, perché intreccia una dimensione politico-militare, una economico-sociale e una

politico-istituzionale: ognuna delle quali vede un protagonista principale diverso, ha conseguenze peculiari e richiede contromisure differenti proprio per la natura differenziata che esse presentano.

La minaccia russa e la guerra in Ucraina

Dal punto di vista politico-militare, è difficile non constatare che la guerra di aggressione, priva di qualunque fondamento giuridico e di qualsiasi seria motivazione di sicurezza, scatenata dalla Federazione russa nei confronti dell'Ucraina costituisca una vera e propria minaccia esistenziale per l'Europa libera.

Illudersi che un'eventuale resa dell'Ucraina sazierebbe gli appetiti di Putin può essere frutto solo di deliberata malafede o di una colossale ignoranza della storia. Esattamente come accadde nel 1938 coi Sudeti rivendicati dalla Germania di Hitler per la tutela dei Volksdeutschen, quello della difesa dei "russi etnici" residenti fuori dai confini postsovietici è un mero pretesto, utile nel disegno della propaganda russa che ha scelto il revanscismo, la nostalgia imperiale e la restaurazione della "grandezza russa" come prima leva della legittimazione del potere di Putin.

Sempre di più, da quando ha imboccato questa via, nel 2006, il regime russo ha bisogno di una mobilitazione permanente della società contro un nemico esterno, cui addebitare tutte le ragioni dello stato miserabile in cui versano la gran parte dei russi a causa principalmente delle scelte corrotte della loro leadership.

Al di là delle fondamentali ragioni di principio per cui occorre sostenere la resistenza del popolo ucraino da chi cerca di riportarlo con la violenza a un passato da cui vuole voglino allontanarsi con tutte le loro forze, è la scelta di impiegare la guerra per ampliare la propria pretesa sfera di influenza a costituire una minaccia esistenziale per la sopravvivenza delle democrazie europee e della loro Unione.

La nostra idea delle procedure legittime con le quali si può garantire l'ordine e la sicurezza del continente europeo – e non solo dello spazio giuridico interno alla UE – è semplicemente incompatibile con i principi e le prassi della Russia putiniana.

Se non mostreremo coraggio e fermezza nel sostenere l'Ucraina e se non incrementeremo le nostre capacità di difesa, e quindi la credibilità della nostra deterrenza a livello di singoli Stati-membri e di Unione Europea, le nostre democrazie nazionali semplicemente non sopravviveranno. L'importanza di far comprendere la gravità della minaccia, da un lato, e la possibilità concreta di contrastarla, dall'altro, credo sia uno dei lavori più ingrati, decisivi e meritori a cui si è dedicato con determinazione il Capo di SME, generale Carmine Masiello, ed è doveroso riconoscerglielo.

La pressione economica della Cina

La minaccia di carattere economico-sociale è quella che la Repubblica popolare cinese porta da anni nei confronti del nostro tessuto imprenditoriale, attuando politiche mercantilistiche, con il ricorso sistematico ad aiuti di Stato, dumping e violazioni del copyright con lo scopo non semplicemente di alterare la concorrenza, ma di eliminare i soggetti concorrenti.

Nonostante ami presentarsi come principale tutrice delle istituzioni che presiedono al libero commercio, Pechino sfrutta le istituzioni libero-scambiste per veicolare politiche mercantilistiche.

Ben prima delle sciagurate decisioni trumpiane in materia di dazi, Xi Jinping ha imboccato con forza la strada della weaponizzazione (o "arsenalizzazione", per impiegare un neologismo italiano) dell'economia, e per la militarizzazione della competizione economica, piegandone le logiche proprie al servizio della potenza nazionale.

Le modalità più dissimulate e meno arroganti con le quali Pechino si è mossa dipendono principalmente da due fattori. La logica più debitrice verso Sun Tzu che verso Clausewitz della cultura strategica cinese e il minor livello in termini di potenza e status che la Cina ancora occupa a livello globale in confronto agli Stati Uniti.

Per gli effetti devastanti in termini di deindustrializzazione e di alterazione dell'equilibrio tra forza lavoro disponibile e domanda di lavoro effettiva e per le ricadute pesantissime sulle dinamiche salariali, l'attacco cinese non va affatto sottovalutato.

Ricordo, oltretutto, che mentre la Cina ama presentarsi come campione del multilateralismo e delle istituzioni che lo incarnano, da cinque anni a questa parte è il principale sostegno finanziario, tecnologico e militare sul quale la Russia di Putin può contare per continuare la propria aggressione all'Ucraina.

L'ordine internazionale liberale sta affrontando la sua crisi più grave dalla Guerra Fredda

La minaccia che affronta, in congiunzione con le istituzioni e le democrazie europee individuali, non è stata eguagliata nemmeno dagli attacchi terroristici dell'11 settembre 2001, e dalla successiva "Guerra al Terrore".

CINA
Espansione economica e influenza globale
RIVALITÀ STRATEGICA

UNIONE EUROPEA
Difesa delle istituzioni democratiche e della stabilità
RESILIENZA DEMOCRATICA

2. ECONOMICO-SOCIALE

LA PRESSIONE ECONOMICA DALLA CINA

- Politiche mercantilistiche
- Aiuti da stato, dumping, violazioni della PI
- Amterarizzazione dell'economia competzione militare
- Deindustrializzazione, distorsioni del mercato del lavoro
- Impatto a lungo termine sulla competitività europea e sulla sicurezza economica

3. POLITICO-ISTITUZIONALE

L'EROSIONE DELLE ISTITUZIONI DEMOCRATICHE

- Interferenze ibride
- Disinformazione e cyberattacchi
- Minare lo stato di diritto
- Pressione sui processi democratici

UNA MINACCIA TRIPLA SENZA PRECEDENTI

Dimensioni politico-militari, economico-sociali e politico-istituzionali, con diversi protagonisti, conseguenze e contromisure.

COSA RIMANE DELL'OCCIDENTE POST-BELLICO

Europa, insieme a Canada e le democrazie consolidate del Pacifico, rappresenta ancora ciò che rimane dell'Occidente post-bellico, forgiato dalla fine del

DEMOCRAZIA RAPPRESENTATIVA
ECONOMIA DI MERCATO LIBERO
SOCIETÀ APERTA

Simulazione Politica

L'ordine internazionale liberale sta affrontando la sua crisi più grave dalla Guerra Fredda

Analisi completata 05.03.2025 14:37

Sintesi principale

La crisi dell'ordine liberale è il risultato di una combinazione di pressioni economiche, politiche e militari, con la Cina come principale sfidante geopolitico.

Esplora dettagli →

Livello di minaccia

ALTO

+12% rispetto all'anno precedente

2 Organizzazioni multilaterali chiave sotto pressione	3 Aree di crisi principali
11 Attori statali coinvolti	5 Contromisure raccomandate

Analisi AI

Le tre dimensioni della minaccia si rafforzano a vicenda, creando una sfida sistemica per la stabilità globale.

Visualizza simulazione completa →

AI Generate

La crisi politico-istituzionale

Vengo infine alla minaccia maggiormente inedita, più sottile e più complicata da contrastare: ovvero quella di carattere politico-istituzionale che, malauguratamente e incredibilmente, è attuata agli Stati Uniti della seconda amministrazione Trump.

Il danno principale e più tangibile apportato dall'amministrazione Trump consiste nella perdita di credibilità politica della garanzia di sicurezza nei confronti degli alleati europei inscritta nell'articolo 5 del Trattato dell'Atlantico del Nord.

Tutti i segnali che arrivano dall'amministrazione Trump vanno nella direzione di mettere in dubbio che gli Stati Uniti interverrebbero effettivamente a sostegno degli altri Stati membri dell'Alleanza nel caso di azioni offensive da parte della Russia.

Ciò non significa che la Nato sia morta, ma, per riprendere una dura e preveggente dichiarazione del presidente Macron, è in uno stato di "coma cerebrale", se gli Stati Uniti rappresentano la "testa" dell'Alleanza.

I segnali concreti del disimpegno americano sono tangibili e vanno ben oltre la riduzione (in parte annunciata e in parte attuata) del personale militare statunitense permanentemente stanziato in Europa, o la sufficienza, per non dire il disprezzo con cui il presidente Trump tratta i suoi omologhi dell'Alleanza.

La rottura dell'effettività della "comunità di sicurezza transatlantica" (per riprendere una antica ed efficace, allora, immagine di Karl Deutsch) è scritta nero su bianco sull'ultimo documento della National Security Strategy rilasciato dall'amministrazione Trump, oltre che dalle indiscrezioni del più accurato documento riservato fatto filtrare all'esterno.

L'Europa è descritta come un teatro marginale, minacciato dal wokismo e dai fenomeni migratori e non dalla persistente guerra di aggressione russa ai suoi confini.

L'Unione Europea è delineata con i tratti di una rivale ideologica oltre che un competitor economico, il cui declino è rappresentato come un interesse degli Stati Uniti.

L'attacco all'Occidente politico

L'attacco frontale portato dall'amministrazione Trump alle istituzioni internazionali e alle norme del diritto internazionale, ovvero alla principale intelaiatura che aveva consentito la realizzazione dell'egemonia di Washington su un sistema internazionale modellato da un ordine liberale di fattura e ispirazione statunitense, è un attacco alla concezione di Occidente politico post-bellico: quello fondato su democrazia liberale, mercato globale e società aperta.

Il punto è che è solo quella comune appartenenza all'Occidente politico (e non identitario, religioso o etnico) che aveva sancito il riavvicinamento transatlantico e la chiusura della plurisecolare separazione volontaria inaugurata con la stessa Rivoluzione americana del 1776 e ribadita nel celeberrimo "Washington Farewell" alla fine del secondo mandato presidenziale del generale-presidente.

Che cosa resta dell'identità occidentale?

Se l'America di Trump annacqua – per usare un eufemismo fin troppo garbato – i tratti liberali e democratici del suo ordinamento, se impiega forze di polizia di confine come milizie private presidenziali con licenza di uccidere i propri stessi cittadini, se bullizza gli alleati e i partner democratici e ricerca invece l'intesa con gli avversari autocratici e i rivali strategici, se la separazione dei poteri viene aggirata sistematicamente persino sul tema fondante dell'identità statunitense espressa nel principio "no taxation without representation" attraverso l'imposizione di dazi da parte del presidente, se la Corte Suprema consente una simile pratica e obietta solo sul tipo di strumento maldestramente adottato e addirittura stabilisce un'inedita e inqualificabile immunità preventiva per qualunque atto compiuto dal presidente nel corso del suo mandato (e il diritto costituzionalmente previsto di richiederne l'impeachment come sta insieme con tutto questo?), se, infine, il presidente, la sua famiglia e i suoi famigli – da Jared Kushner a Steve Witkoff – si rendono responsabili dei casi più eclatanti di insider trading, conflitto di interessi e arricchimento illecito della storia degli Stati Uniti, che cosa resta della comune identità occidentale?

Una relazione transatlantica da ripensare

È questo che rende non più credibile in maniera assoluta la garanzia di sicurezza americana verso gli europei prevista dall'articolo 5.

Da qui discende l'incredibile ottimo legame tra il presidente Trump e l'autocrate russo

Putin, le minacce agli europei e ai canadesi sulla loro stessa integrità territoriale, la volontà di sanzionare gli alleati per non aver voluto partecipare alla illegale (e quindi criminale) guerra di aggressione scatenata da Trump e Netanyahu nei confronti dell'orribile regime iraniano.

Si tratta di qualcosa di inedito, imprevedibile e impensabile che ristruttura la nostra relazione con gli USA potenzialmente in maniera permanente.

Il momento dell'Europa

Per noi, la sola strategia possibile in un simile scenario è quella di cercare di ottenere dall'alleanza tutto quello che è ancora possibile, sperando che una nuova amministrazione americana possa almeno parzialmente ritonificarla, ma senza farci più illusioni sulla sua "eternità".

Il genio del "Transataltic divide" è uscito dalla lampada a causa di un apprendista stregone malaccorto e malintenzionato e non credo sarà più possibile farlo interamente rientrare.

La responsabilità delle "middle powers"

Nel frattempo, è cruciale che gli altri membri dell'Alleanza, da quelli europei al Canada, insieme agli Stati membri dell'Unione Europea e all'Unione stessa, si adoperino molto rapidamente per ricoprire un ruolo da protagonisti nella difesa del proprio territorio, delle proprie istituzioni e della propria libertà, contro tutte le minacce, "da qualunque parte provengano", tanto esterne quanto interne.

L'Occidente non è morto solo perché l'America di Trump ne tradisce le premesse e le promesse. Sta a noi, alle "middle powers" che ancora credono nei suoi valori, nelle sue istituzioni e nelle sue prassi - per citare il premier canadese Mark Carney - mantenerne in vita non il ricordo del passato ma la speranza del futuro.



Il Ministro Crosetto incontra Kallas a Roma: difesa europea, Mar Rosso e Libano

Roma, 2 ottobre 2026

Il ministro della Difesa Guido Crosetto ha incontrato a Roma l'Alto Rappresentante Ue Kaja Kallas per discutere di sicurezza europea, operazione ASPIDES, rotte commerciali nel Mar Rosso e Mediterraneo e situazione in Libano. Crosetto ha sottolineato la necessità per l'Europa di trasformare gli impegni politici in capacità operative e risorse concrete.

Nel confronto è stata accolta positivamente la disponibilità di alcuni Paesi europei a fornire nuovi assetti ad ASPIDES, considerata essenziale per la sicurezza della navigazione e la continuità dei commerci. Crosetto e Kallas hanno inoltre discusso della possibilità di rafforzare il coordinamento europeo contro le minacce ibride, attraverso una maggiore condivisione delle informazioni e una risposta più rapida.

Ampio spazio è stato dedicato al Libano, con l'obiettivo di evitare vuoti di sicurezza dopo la conclusione della missione UNIFIL e valorizzare l'esperienza dei Paesi già impegnati sul terreno. Al centro anche il rafforzamento delle capacità europee nella difesa, nel cyber e nelle tecnologie avanzate, attraverso una maggiore integrazione delle risorse disponibili.











ESERCITAZIONE “AEGIS 26” AL POLIGONO DI MONTE ROMANO

Monte Romano (VT), 17 settembre 2026

”Signor Presidente della Repubblica, la Sua presenza testimonia, ancora una volta, la costante attenzione che Lei riserva alle Forze Armate e la Sua preziosa vicinanza alle donne e agli uomini in uniforme che ogni giorno servono il Paese con professionalità, dedizione, lealtà e senso del dovere. Il riconoscimento dell’Esercito e delle Forze Armate quali riferimenti per l’intera Nazione, insieme al richiamo alla fedeltà verso la Repubblica, costituiscono per noi un monito e, al tempo stesso, uno sprone a fare sempre meglio al servizio dell’Italia. Ogni esercitazione rappresenta la fase conclusiva di un percorso e il banco di prova dell’impegno quotidiano che rende le Forze Armate efficaci, moderne e pronte. Prepararsi significa non soltanto saper reagire, ma anche prevedere e, quando possibile, anticipare sfide e insidie. Significa mettere alla prova capacità, acquisire procedure e tecnologie, perfezionare l’interoperabilità con gli alleati, individuando ciò che può essere migliorato. In questa continua evoluzione rimane, però, un punto fermo: il vero capitale della Difesa sono le donne e gli uomini, con la loro professionalità e la capacità di conoscere, governare e utilizzare le tecnologie. Come Ministro della Difesa, ho il dovere di pensare anche allo scenario peggiore, con la speranza che non si realizzi mai. In un contesto come quello attuale, nel quale in troppe parti del mondo la forza pretende di prevalere sul diritto, dobbiamo ricordare che la sicurezza è il presupposto concreto della libertà e della democrazia. La pace non è mai acquisita una volta per tutte: va costruita e difesa ogni giorno, anche attraverso Forze Armate preparate, moderne e credibili, capaci di proteggere l’Italia, le sue Istituzioni e i suoi cittadini”.

Il Ministro Crosetto incontra l'omologo greco Dendias

Roma, 8 settembre 2026



"Cordiale e particolarmente costruttivo incontro con il collega greco Nikos Dendias, nel corso del quale abbiamo concordato di avviare un dialogo strutturato tra i rispettivi Ministeri, per approfondire la visione comune sui temi della difesa e della sicurezza europea e individuare risposte condivise alle sfide attuali. Abbiamo anche riconosciuto l'importanza della nostra collaborazione per assicurare la libertà di navigazione delle nostre flotte, anche commerciali, e più in generale per la sicurezza attraverso il Mediterraneo. Approfondito, inoltre, come rafforzare la cooperazione tra le industrie della difesa dei nostri Paesi, promuovendo sinergie tecnologiche e lo sviluppo congiunto di prodotti e capacità innovative". Così il Ministro Guido Crosetto.

Crosetto sul fianco orientale della NATO tra deterrenza e difesa europea

Bulgaria, 14 settembre 2026



Dalla Bulgaria alla Lettonia, dalla Lituania alla Polonia, il Ministro della Difesa Guido Crosetto ribadisce l'impegno italiano sul fianco orientale della NATO e rilancia la necessità di una difesa europea più integrata, capace di rafforzare deterrenza, interoperabilità e sicurezza del continente.

La visita di Guido Crosetto sul fianco orientale dell'Alleanza ha toccato Bulgaria, Lettonia, Lituania e Polonia, con incontri dedicati alla sicurezza europea, al sostegno all'Ucraina e al rafforzamento delle capacità militari. In Bulgaria, rivolgendosi al personale impegnato nel Multinational Battle Group, il Ministro ha sottolineato la responsabilità italiana nella tutela del fianco sud-orientale della NATO, evidenziando come la credibilità della deterrenza dipenda da preparazione, efficienza operativa e interoperabilità con gli Alleati. L'esperienza dei conflitti contemporanei, ha osservato Crosetto, impone inoltre di aggiornare costantemente

Il Sottosegretario Perego ha incontrato il Vice Ministro della Difesa del Giappone

Roma, 15 settembre 2025



Il Sottosegretario di Stato alla Difesa, On. Matteo Perego di Cremnago, ha incontrato oggi, a Palazzo Marina, il Vice Ministro della Difesa del Giappone, On. Wakabayashi Yohei.

Al centro del colloquio diversi dossier su difesa e sicurezza: dall'attuale situazione geopolitica alla cooperazione tra Italia e Giappone, sino a un approfondimento delle dinamiche che stanno interessando l'Indo-Pacifico.

"A fronte di minacce sempre più pervasive e ibride, in un contesto globale segnato dall'instabilità, dove la tecnologia si evolve con estrema velocità, la vera sfida sarà mantenere la competitività nei prossimi anni. Una visione condivisa contribuirà alla tutela di un ordine internazionale basato su regole e responsabilità. In questo contesto, la partnership creata con il programma GCAP tra Italia, Regno Unito e Giappone - prosegue Perego - genererà notevoli ricadute positive in termini di occupazione, ricerca e know-how, interessando in modo virtuoso il tessuto industriale delle nostre nazioni, ben oltre l'ambito della Difesa. L'Indo-Pacifico rappresenta uno dei quadranti più rilevanti per gli equilibri globali futuri. Ciò rende ancora più significativo il dialogo tra partner che condividono i medesimi valori di libertà, sicurezza e democrazia". L'On. Wakabayashi ha sottolineato il prezioso contributo dell'Italia alla pace e alla stabilità internazionale, evidenziando l'eccellenza dell'industria della difesa italiana, riconosciuta in tutto il mondo.

addestramento e capacità.

In Lettonia, presso la base di Adazi, il Ministro ha incontrato i militari dell'Esercito impegnati nell'operazione Baltic Guardian, richiamando il valore della presenza italiana e della professionalità costruita nelle missioni internazionali. Crosetto ha collegato questa credibilità alla capacità di unire efficacia militare e attenzione alle persone, sostenendo la necessità di prepararsi a scenari in continua evoluzione e di contribuire contemporaneamente alla sicurezza nazionale e alla stabilità internazionale.

In Lituania, il Ministro ha ricevuto il ringraziamento per l'intervento dei due caccia italiani che hanno abbattuto un drone dopo una violazione dello spazio aereo lituano. La vicenda ha rafforzato, nelle parole di Crosetto, la necessità di sviluppare una difesa europea integrata, con priorità per difesa aerea e missilistica, protezione delle infrastrutture critiche, cyber e sorveglianza delle frontiere. La presenza della Task Force Air Baltic Thunder III rappresenta in questo quadro un contributo concreto alla sicurezza del fianco orientale. A Varsavia, infine, Crosetto ha incontrato il Ministro polacco Kosiniak-Kamysz, ribadendo il sostegno all'Ucraina e sottolineando il legame tra la sicurezza polacca, italiana ed europea. Italia e Polonia condividono l'obiettivo di costruire una difesa europea nella sua dimensione continentale, oltre i 27 Stati dell'Unione e complementare alla NATO. Al centro della cooperazione anche difesa aerea, spazio, intelligenza artificiale, sistemi unmanned e robotici, contrasto alle minacce ibride, mobilità militare e industria della difesa, con progetti che comprendono elicotteri, F-35 e infrastrutture strategiche. La Polonia, ha sottolineato Crosetto, rappresenta un riferimento per la rapidità con cui ha adeguato la propria postura al nuovo scenario di sicurezza, mentre l'Italia continuerà a garantire il proprio contributo alla NATO con oltre 2.000 militari impegnati nell'area.



Rauti alla Prima Conferenza Nazionale della Difesa sull'Artico

Roma, 29 settembre 2026

Il Sottosegretario alla Difesa Isabella Rauti, con delega all'ambiente artico, subartico e antartico, ha partecipato a Roma alla presentazione degli Atti della Prima Conferenza Nazionale della Difesa sull'Artico, svoltasi nell'ottobre 2025. Rauti ha sottolineato come il rapido cambiamento climatico abbia trasformato l'Artico in uno spazio centrale della competizione globale, dove si intrecciano sicurezza, rotte commerciali, infrastrutture strategiche, ricerca, tecnologia e risorse. «Ciò che accade nell'Artico non rimane nell'Artico», ha affermato, evidenziando le ricadute sulla sicurezza europea e sugli equilibri geopolitici. La nuova Politica Artica Italiana, presentata dal Governo nel gennaio 2026, rafforza la dimensione della sicurezza rispetto alle linee guida del 2015. Rauti ha inoltre annunciato la prossima Conferenza, prevista a Roma il 29 ottobre, con un respiro più internazionale e un focus anche sull'Antartide. L'obiettivo è mettere in rete istituzioni, ricerca e industria e costruire una vera architettura nazionale per le regioni polari, consolidando il ruolo dell'Italia nella cooperazione scientifica, nella sostenibilità e nella stabilità internazionale.

XV Trans-Regional Seapower Symposium

Venezia, 6 ottobre 2026



"Il mare non ci separa dal mondo. Ci rende parte del mondo. Non è soltanto uno spazio geografico o operativo: è un complesso sistema di connessioni da cui dipendono sicurezza, economia e tecnologia globale.
Così il Ministro della Difesa al XV Trans-Regional Seapower Symposium a Vernezia, insieme ai rappresentanti di oltre 70 Marine. Viviamo in un tempo nel quale ciò che accade a migliaia di chilometri da noi può produrre conseguenze immediate sulla nostra sicurezza, sulla nostra economia, sulla vita quotidiana dei nostri cittadini.
Lo vediamo a Hormuz e a Bab el-Mandeb. Lo vediamo nel Mar Rosso. Me esiste un fronte che non vediamo: è sotto la superficie del mare, dove passano cavi, energia, dati e infrastrutture essenziali che spesso non vediamo, ma dalle quali dipendiamo ogni giorno.
E lo vediamo nella velocità con cui tecnologia, droni, sistemi autonomi, cyber e intelligenza artificiale stanno cambiando il modo stesso di concepire la Difesa. Per questo nessun Paese può pensare di affrontare da solo le sfide che abbiamo davanti. Servono cooperazione, interoperabilità, capacità industriale, innovazione e, soprattutto, la capacità di trasformare rapidamente la tecnologia in strumenti concreti di sicurezza. Proteggere il mare significa proteggere ciò che attraverso il mare ci rende forti: la nostra sicurezza, la nostra economia, la nostra libertà.
Venezia lo aveva capito secoli fa.

SAATI

MAKING A MATERIAL DIFFERENCE

L'ECCELLENZA ITALIANA NELLA PROTEZIONE BALISTICA

Da oltre 90 anni SAATI sviluppa materiali avanzati ad alte prestazioni per applicazioni industriali e tecnologiche, trasformando la ricerca e il know-how in soluzioni capaci di fare la differenza. Con oltre quarant'anni di esperienza nel settore della difesa, SAATI sviluppa e produce sistemi innovativi per la protezione individuale e la blindatura di veicoli civili e militari, adottati da forze di polizia ed eserciti in tutto il mondo: Italia, USA, UK, Francia, Spagna, Belgio, Germania, Nord ed Est Europa, Turchia, Australia, Emirati Arabi e Arabia Saudita.

SOLUZIONI

- Tessuti aramidici ad alte prestazioni
- Trattamenti con finissaggi idrorepellenti PFAS free
- Laminati e pre-preg termoplastici, fenolici, epossidici e gommati
- Sistemi anti-taglio, anti-perforazione e antitrauma
- Backing e Spall Liner
- CoreMatrix™
- ArmourFit™

APPLICAZIONI

- **Giubbotti tattici e sottocamicia (antiproiettile e antisommossa)**
- Elmetti per forze dell'ordine e militari
- Veicoli civili e militari
- Tute antiesplosione e protettive (EOD)



www.saati.com | info.it@saati.com | Via Milano 14, 22070, Appiano Gentile (CO)

CHOD/NAD Conference

a Roma l'incontro dei vertici europei della Difesa

Roma, 23 settembre 2026









“Difesa europea, la sfida è decidere in tempo”

Si è conclusa a Roma la seconda CHOD/NAD Conference, che ha riunito Capi di Stato Maggiore della Difesa e Direttori Nazionali degli Armamenti europei e dei Paesi partner. Aprendo i lavori, il ministro della Difesa Guido Crosetto ha sottolineato che «L’Europa non ha bisogno di nuova burocrazia, ma di velocità decisionale e operatività» e che «Non basta spendere: servono requisiti comuni, interoperabilità, sviluppo industriale e uno “Scudo della Difesa Europeo”».

Il Capo di Stato Maggiore della Difesa, Generale Luciano Portolano, ha indicato nella rapidità delle decisioni una priorità: «nessun avversario adatterà i propri piani ai nostri tempi procedurali». La deterrenza, ha spiegato, dipende anche dalla capacità industriale di sostenere uno sforzo prolungato: «Un’eccellenza tecnologica priva di profondità industriale, di scorte adeguate, di capacità di rigenerazione non produce deterrenza. Produce una promessa. E le promesse non si schierano sul terreno». Al centro del confronto cooperazione, approvvigionamenti, prontezza operativa, UAS e contrasto ai droni. EDIP e SAFE offrono nuovi strumenti, ma «la disponibilità di risorse non garantisce, di per sé, un cambiamento». La sfida resta trasformare le iniziative emergenziali in una strategia europea strutturata e integrata.

CARLO ALBERTO CARNEVALE MAFFÈ
SDA Bocconi School of Management

La deterrenza non è un arsenale ma una filiera

La filiera resiliente come prima linea della difesa



immagine: © Antonio Morlupi

La guerra in Ucraina ha cambiato la misura della potenza militare: non conta solo ciò che un Paese possiede oggi, ma ciò che è in grado di produrre, rigenerare e sostituire domani. Per l'Italia la sfida è trasformare la sua industria in una riserva strategica

Una frase meriterebbe di stare appesa in ogni ufficio di programmazione della difesa: un avversario non si lascia impressionare da quanti sistemi d'arma possiedi oggi, ma dalla tua capacità di averne altrettanti fra sei mesi. La deterrenza, in altre parole, non è la fotografia di un magazzino ma la capacità di riempirlo. La guerra in Ucraina ha trasformato quella che sembrava una massima da manuale in un vincolo di bilancio.

La spesa militare si misura quasi sempre in percentuale del PIL, indicatore di volontà politica più che di forza. Nel libro «Il costo della pace. L'economia della deterrenza», scritto con Andrea Bignami e di prossima uscita per l'editore Piemme, proponiamo una misura diversa, il tasso di conversione strategico: la quota di ogni euro stanziato che, entro un orizzonte dato, diventa capacità pronta, disponibile e rigenerabile. Tra il bilancio e il sistema operativo corre una catena di sette anelli, dal requisito alla rigenerazione, e a ogni anello si perde qualcosa. Il fondo speciale tedesco da cento miliardi lo mostra: vincolato quasi per intero in contratti entro il 2024, a metà 2026 risultava pagato, cioè consegnato, per circa la metà.

Nel 2022 l'Europa produceva circa trecentomila proiettili da 155 millimetri l'anno, mentre l'Ucraina ne sparava fino a ottomila al giorno: in dodici mesi il continente produceva ciò che Kiev consumava in cinque settimane. Per arrivare a circa due milioni di colpi l'anno ci sono voluti tre anni. Nel 2026 la lezione si è ripetuta su scala più grande: poche settimane di conflitto ad alta intensità con l'Iran sono bastate a consumare circa due terzi degli intercettori Patriot americani, a fronte di una produzione di circa 650 l'anno, e il Pentagono ha contattato Ford e General Motors chiedendo di riconvertire parte della produzione



automobilistica. Quando le linee sono sature, la moneta diventa quasi irrilevante, e la vera merce di scambio, più che il prezzo, è la data di consegna.
L'Ucraina ha costruito quasi da zero una filiera di droni FPV (First Person View, pilotati in soggettiva) passata in meno di tre anni da poche migliaia a milioni di unità, con costi tra mille e cinquemila dollari e un progetto riscritto ogni due o tre settimane sulla base del ritorno dal campo. I componenti sono commerciali, le schede di volo a codice aperto, la produzione è distribuita in centinaia di officine: la perdita di un fornitore si compensa in ore, non in anni, e una fabbrica dispersa è un bersaglio difficile. Anche l'acquisto è stato rovesciato: con il catalogo digitale "Brave1 Market" i reparti ordinano direttamente ai produttori certificati, fra oltre ottocento prodotti, e ricevono il materiale in prima linea in dieci giorni in media.
Qui il ciclo di aggiornamento diventa esso stesso un'arma, perché costringe l'avversario a un contro-adattamento continuo che ne assorbe le risorse. Vale il principio delle "Liberty Ships": la fabbrica della deterrenza non vince con il prodotto perfetto, ma con il prodotto buono che arriva in tempo. Kiev non è più brava di Berlino; opera in un altro regime, quello dell'emergenza. La sfida europea è costruirne uno intermedio, di transizione, che comprima i tempi senza rinunciare ai controlli democratici.
La seconda idea del libro è la dipendenza per attrito: chi compra un sistema complesso non compra un oggetto, ma un rapporto trentennale fatto di software, manutenzione, ricambi e autorizzazioni. Non serve un atto ostile perché quel rapporto diventi una leva: basta il controllo del ciclo di vita, o anche una decisione di bilancio presa altrove, come quando nel 2025 Washington ha cancellato il successore dell'aereo radar E-3. La misuriamo con un indice di attrito da zero a uno, sempre accompagnato da un orologio, il tempo di degrado: minuti od ore per un servizio satellitare come Starlink, mesi per un caccia che vive di aggiornamenti come l'F-35, anni per un obice con le munizioni in deposito. Il caso limite è la Svizzera, che nel 2021 ha ordinato cinque batterie Patriot, ne ha pagato un terzo e non ne ha ancora vista arrivare nessuna: conversione lentissima e attrito altissimo, saldati in anticipo.
È qui che le due misure convergono perchè una filiera reattiva e distribuita alza il tasso di conversione e, insieme, abbassa l'indice di attrito, perché incorpora per progetto la sostituibilità dei fornitori. Autonomia strategica non significa autarchia, ma controllo delle interfacce critiche: il criterio fondamentale, prima del passaporto del fornitore, è quanto a lungo la capacità sopravvive se quel fornitore smette di collaborare. Con un'avvertenza: anche il componente commerciale porta con sé il suo attrito. Quando nell'aprile 2025 Pechino ha sottoposto a licenza l'export di sette terre rare, le sue esportazioni di magneti sono crollate di circa tre quarti in due mesi, con un tempo di degrado misurato in settimane. Non a caso la fabbrica sotterranea di droni annunciata da Ucraina e Croazia nel 2026 nasce con l'obiettivo dichiarato di affrancarsi dalla componentistica cinese.

Che cosa significa per l'Italia

Non si tratta di rinunciare alle grandi piattaforme, ma di affiancare loro un secondo binario. Primo, valutare i programmi sul tasso di conversione, rigenerazione compresa, e non sul solo impegno contabile. Secondo, negoziare l'attrito prima di firmare, perché dopo il potere passa al venditore: Cameri per l'F-35 e la produzione su licenza in Polonia dei sistemi coreani, consegnati in meno di due anni, dimostrano che l'attrito è una clausola che va negoziata, più che un vincolo assoluto. Terzo, contratti quadro pluriennali per i consumabili, munizioni, intercettori e droni, che diano all'industria la visibilità necessaria ad allargare le linee, con una corsia rapida per le piccole imprese. Quarto, una funzione pubblica di visibilità della filiera, capace di mappare e monitorare costantemente i fornitori di secondo e terzo livello e i punti unici di rottura, ordinaria in pace e operativa in crisi, imponendo tra i requisiti militari specifici parametri di resilienza operativa e continuità di fornitura. I materiali di maggiore diffusione devono essere producibili in modo decentrato e semplificato, utilizzando il massimo di componenti commerciali e prevedendo anche l'auto-produzione distribuita tramite sistemi di stampa 3D, come più volte raccomandato dal generale Masiello.
L'Italia ha qui un vantaggio che raramente si



riconosce: un tessuto di distretti manifatturieri che è, per sua natura, produzione distribuita, modulare e rapida nell'adattarsi. Trasformarlo in riserva di capacità della difesa sarebbe forse l'investimento a più alto tasso di conversione disponibile. Un arsenale è una fotografia; una filiera è una promessa che va mantenuta ogni settimana.

ANIELLO FASANO

Tessuti intelligenti, innovazione italiana

La ricerca per l'abbigliamento spaziale trasforma tessuti e tute in tecnologie intelligenti, rafforzando al tempo stesso innovazione, manifattura e competenze italiane



Intervista a Corinna Sperandini

Amministratore Delegato di Spacewear



Dallo spazio alla vita quotidiana, passando per la Difesa e per una manifattura italiana chiamata a reinventarsi, è questa la traiettoria lungo la quale si muove l'esperienza di Spacewear, azienda che ha trasformato la ricerca sui tessuti e sull'abbigliamento per ambienti estremi in un laboratorio di innovazione applicabile anche sulla Terra. Tute ultraleggere, materiali termoregolanti, proprietà antibatteriche e sistemi capaci di monitorare parametri fisiologici raccontano un'evoluzione che supera il concetto tradizionale di abbigliamento e avvicina sempre più il tessuto alla tecnologia. La Smart Flight Suit 1 (SFS1) è stata testata durante la missione suborbitale Virtute-1, il 29 giugno 2023, mentre la Smart Flight Suit 2 (SFS2) è stata utilizzata a bordo della Stazione Spaziale Internazionale durante la missione Axiom-3 (Ax-3), dal 18 gennaio al 9 febbraio 2024, per monitorare i parametri biomedici degli astronauti.



Una frontiera che riguarda anche il futuro dell'aerospazio e dei sistemi di protezione individuale, ma che pone al tempo stesso una questione più ampia: come trasferire le tecnologie sviluppate per condizioni estreme nei prodotti destinati alla vita di ogni giorno e come trasformare la ricerca in nuova capacità industriale. È su questo terreno che Spacewear ha scelto di investire, destinando una parte significativa delle proprie risorse alla ricerca e coinvolgendo una filiera italiana fatta di piccole e medie imprese, università e competenze specialistiche.
Per Corinna Sperandini, Amministratrice Delegata di Spacewear, innovazione tecnologica e manifattura non sono percorsi alternativi, ma parti della stessa strategia. Una strategia che punta alla reindustrializzazione tecnologica del Paese, alla valorizzazione del know-how italiano e alla capacità di trasformare la ricerca in prodotti, occupazione e competitività internazionale. Una sfida che coinvolge anche il ruolo delle donne nell'impresa e la necessità di costruire condizioni più favorevoli perché competenze e idee possano diventare aziende capaci di crescere sui mercati globali. Per approfondire questi temi, ne abbiamo direttamente con l'A.D. di Spacewear.

Spacewear è nata nel 2021 con l'obiettivo di portare il tessile e l'abbigliamento verso livelli di innovazione propri degli ambienti estremi. Quali sono state le principali difficoltà nel trasformare questa visione in tute spaziali effettivamente autorizzate dalla NASA e utilizzate sulla Stazione Spaziale Internazionale durante la missione Ax-3?

In primis, la visione: rendere credibile e realizzabile un progetto visionario. In questo percorso è stato fondamentale incontrare, nell'Aeronautica Militare, quella lungimiranza che, forse, altre istituzioni dovrebbero avere maggiormente.

Le difficoltà si sono poi presentate lungo tutta la catena progettuale. Ma affrontare lo spazio, il contesto più estremo e rigoroso nel quale si possa operare, ci ha permesso di compiere un vero salto quantico. Un percorso che ha dato vita non solo a una nuova realtà e a nuovi stimoli per un sistema industriale come quello tessile-abbigliamento, ancora in larga parte ancorato a logiche pre-digitali, ma che ha anche dato visibilità a innovazioni che, prima delle nostre tute, sembravano difficilmente realizzabili.

Per affrontare una sfida di questo livello sono necessarie competenze, esperienza e una conoscenza estremamente precisa dei tessuti e del loro comportamento. La criticità maggiore consiste nell'innovare aumentando le performance e, allo stesso tempo, rispettare gli stringenti requisiti di sicurezza e le certificazioni richieste da Axiom e NASA.

Superare la fase di revisione ha significato dimostrare, tecnicamente e scientificamente, come fosse costruita la tuta, come interagissero i diversi componenti tessili e i device per conferirle tutte le performance innovative, come funzionasse senza consumare energia e quale fosse il livello di sicurezza raggiunto.

Il fatto che fosse totalmente Made in Italy è stato particolarmente apprezzato, così come la nostra disponibilità a rispondere sempre, e tempestivamente, alle domande dei diversi referenti di progetto.

Il nostro impegno è stato totale. Abbiamo sentito fortemente la responsabilità di raggiungere un risultato italiano di portata internazionale, destinato a essere utile alla vita nello spazio e proveniente da un settore che, fino a quel momento, non si era mai realmente aperto a un processo di innovazione di questa portata.

Le vostre tute combinano leggerezza, termoregolazione, proprietà antibatteriche, design ergonomico e monitoraggio dei



parametri medici, con un peso inferiore al chilogrammo. Quali tecnologie sviluppate per gli astronauti possono essere trasferite concretamente nell'abbigliamento di tutti i giorni e come potrebbe cambiare, grazie alla ricerca spaziale, il modo in cui concepiamo i vestiti?

Le nostre tecnologie e le nostre tute intelligenti sono potenzialmente applicabili, in forme più o meno estreme, a tutto il settore aerospaziale e anche ai piloti delle future generazioni di caccia. Ma il cambiamento riguarderà anche il mondo dell'abbigliamento e, soprattutto, la mentalità del consumatore. Pensiamo, ad esempio, al concetto di antibattericità: una tecnologia che permette a un capo utilizzato persino durante l'attività di training, grazie alla riduzione della proliferazione batterica, di mantenere un livello di igiene superiore a quello di un capo semplicemente lavato, che per essere mantenuto pulito richiede acqua e detergenti.

Pensiamo ai tessuti ultraleggeri e termoregolanti, capaci di contribuire al mantenimento della temperatura corporea. Sono il risultato di innovativi processi produttivi che permettono di utilizzare materie prime naturali insieme a nuovi materiali ad alte prestazioni.

Innovare i tessuti significa inevitabilmente innovare anche il design. E in Italia il design è cultura. Si genererà così un abbigliamento sempre più integrato con gli stili di vita del presente e del futuro: capi pensati per un'umanità che vivrà in contesti destinati a modificarsi radicalmente e che richiederanno un rapporto completamente nuovo tra il corpo, ciò che indossiamo e l'ambiente che ci circonda.

Spacewear destina circa il 25% del fatturato alla ricerca e sviluppo e coinvolge una filiera italiana composta da piccole e medie imprese e università. Quanto è importante questo modello per riportare innovazione e competenze nel sistema manifatturiero italiano e contrastare la perdita di marchi e know-how che ha accompagnato la delocalizzazione del settore tessile?

È fondamentale coinvolgere le filiere tradizionali e saper riconvertire le produzioni alle nuove necessità: è questo il fattore primo che può salvaguardare la manifattura.

Noi abbiamo perseguito questa strada fin dall'inizio. Investire il più possibile in ricerca per portare a terra il maggior numero di soluzioni e innovazioni, trasformandole in motore di nuove produzioni, è per noi la via maestra per recuperare il primato delle nostre



SMART FLIGHT SUIT 2

Tuta interattiva certificata

Creata per aumentare il comfort psico-fisico dell'astronauta e per monitorare i dati medici

SFS2, progettata e prodotta da Spacewear, costruita per fornire il massimo comfort di movimento, dotata di paracolpi di sicurezza nelle parti fisiche più esposte, ignifuga ma traspirante, e in grado di rilevare dati biomedici. SFS2 viene utilizzata sulla Stazione Spaziale Internazionale durante la Missione Ax-3 organizzata da Axiom Space. I dispositivi tutti certificati, integrati sulla SFS2, sono stati approvati dalla NASA e dal board internazionale per la ISS e sono gli unici device abilitati on board a rilevare dati medici nella Missione Ax-3, oltre quelli di default di NASA. Qualunque ricerca medica di rilevazione dati on board dovrà utilizzare i dati rilevati da SFS2.

Tessuti e dispositivi sono certificati pertanto SFS2 rappresenta un esempio unico nel panorama attuale che verrà testato per un minimo di 8 ore durante la Missione Ax-3. La tuta è in grado di mantenere la temperatura corporea a livelli normali sia sotto sforzo fisico che in contesti di raffreddamento ed è in grado di monitorare dati biomedici tramite dispositivi integrati e trasmetterli in tempo reale o memorizzarli.

Oltre a fornire una forma di sicurezza attiva e passiva, è il preludio a ulteriori sviluppi nell'implementazione del comfort e della sicurezza operativa nello spazio, con implicazioni utilizzabili anche sul pianeta Terra.

manifatture e, con esso, i posti di lavoro. Serve una vera reindustrializzazione tecnologica del manifatturiero italiano.
Produrre in Italia costa più che produrre nei Paesi terzi, ma rende molto più di quanto costa: crea PIL, produce manufatti durevoli, genera sostenibilità industriale, sostiene le famiglie attraverso un reddito dignitoso e rafforza la struttura stessa del Paese. Senza manifattura si diventa ininfluenti, non solo sullo scacchiere economico mondiale, ma in tutto ciò che da questo deriva. Occorre un cambio di mentalità da parte di tutti gli attori. A partire dalla burocrazia, che troppo spesso blocca lo sviluppo e rallenta i processi, al punto tale che aziende virtuose si trovano costrette a scegliere tra la vendita a gruppi esteri e il rischio di scomparire. Passando per le aziende che spesso temono l'innovazione e che, anno dopo anno, vedono diminuire la propria capacità competitiva a causa del proprio immobilismo produttivo. E arrivando alle banche e ai fondi di investimento, che spesso premiano quasi esclusivamente la scalabilità: il falso mito del "tutto e subito", che troppe volte finisce per trasformarsi in carta straccia. La manifattura non è tutto e subito, è un'impresa lenta perché costruisce lavoro, non finanza. Costruisce prodotti tangibili, utili e belli; crea brand riconoscibili, ambasciatori del DNA di un Paese; forma cultura d'impresa e costruisce, giorno dopo giorno, la spina dorsale di una nazione. E su questo che bisogna investire.
Nessun corpo può sostenersi senza una spina dorsale.

Lei ha sostenuto che per rafforzare l'imprenditoria femminile servano sia una maggiore fiducia nelle proprie capacità sia un cambiamento nella percezione culturale dell'impresa guidata da una donna.

Dopo il riconoscimento ricevuto con il premio "Le donne di ora" di Invitalia, quale cambiamento ritiene ancora necessario per permettere a più donne di trasformare competenze e idee innovative in imprese capaci di competere nei mercati tecnologici internazionali?

Perché le donne possano investire tempo, competenze e capacità in se stesse e in imprese proprie, occorre un sistema-Paese che le sostenga. È evidente che il carico dei compiti sociali e familiari continua a gravare in misura significativa sulle donne.
Se vogliamo che possano avere più tempo da dedicare al lavoro quando scelgono di fare impresa, dobbiamo mettere a disposizione servizi capaci di liberare quel tempo. Ma occorre anche creare le condizioni perché possano acquisire gli strumenti necessari a diventare competitive, sviluppando una vera cultura d'impresa e avendo accesso alle risorse finanziarie necessarie alla crescita.



In questo senso, Invitalia rappresenta un esempio concreto di come un sistema pubblico possa contribuire a creare queste condizioni, attraverso strumenti finanziari e percorsi capaci di avvicinare le persone alla cultura d'impresa e accompagnarle nello sviluppo.
Investire nelle donne significa investire nella capacità produttiva del Paese. Reindustrializzazione tecnologica, innovazione e crescita dell'imprenditoria femminile fanno parte della stessa sfida: costruire un sistema produttivo capace di innovare, creare valore e lavoro, mantenendo in Italia le competenze e la capacità manifatturiera che rappresentano una parte essenziale della nostra identità.

TECNOLOGIA CHE ISPIRA PERSONE CHE INNOVANO

Ogni giorno costruiamo
un **ecosistema inclusivo**
dove l'**innovazione crea valore**
e la **sostenibilità guida**
il cambiamento



LOTTOMatica

ITALIAN SPACE ACTIVITIES

AIR LAUNCH
ALPHAJET + HAX25

INNOVAZIONE
TECNOLOGIA
SOVRANITÀ SPAZIALE



GIOVANNI CAPRARA

GIORNALISTA SCIENTIFICO

AVIOLANCIO ITALIANO

Il crescente fabbisogno di accesso allo spazio impone nuovi lanciatori e infrastrutture. L'Italia punta anche sull'aviolancio con HAX25, programma Cnr che mira a sviluppare un sistema autonomo, flessibile e rapido per mettere satelliti in orbita

Il trasporto in orbita sta diventando sempre di più un collo di bottiglia per lo sviluppo delle attività spaziali sia civili che per la difesa a livello internazionale. Ora l'Europa, dopo anni di sottovalutazione del problema, dispone di due vettori: il grande Ariane-6 e il vettore Vega-C costruito in Italia da Avio. Entrambi, hanno prenotazioni garantite per almeno un paio d'anni di attività, dato il ritmo contenuto dei lanci possibili dalla Guyana francese. In agosto, l'agenzia spaziale europea ESA ha finanziato con 543,6 milioni di euro il sostegno di tre progetti nell'ambito dell'European Launcher Challenger e realizzati da due società tedesche e una spagnola. In cantiere, ci sono poi altri piani con l'intento di arrivare al recupero del primo stadio come oggi già effettuano le società americane Space X e Blue Origin e le cinesi Landspace (privata) e Casc (pubblica). Le società impegnate in questa direzione nel Vecchio Continente sono Maiaspace di Airbus e Avio che sta costruendo un dimostratore finanziato con risorse del PNRR. In Italia è però in corso un altro programma completamente diverso che guarda ad un sistema di aviolancio, per rispondere al variegato mondo delle necessità della Difesa; ma non solo, ovviamente. Oltre i lanciatori, esiste pure una ristrettezza riguardante le basi di lancio per cui Stati Uniti, Cina e anche l'Europa sono impegnate nella ricerca di nuove opportunità da creare a latitudini diverse. In altre parole, sono necessari più lanciatori e più basi di lancio per affrontare una crescita connessa soprattutto alla creazione di costellazioni satellitari sia civili che militari.

Considerando il complesso panorama, a livello nazionale, è in corso anche il programma HAX25 che mira ad un'autonomia di lancio facendo ricorso all'uso di un jet in grado di trasportare e lanciare un vettore. Il progetto approvato dal Comitato interministeriale per le politiche aerospaziali è realizzato dal Consiglio Nazionale delle Ricerche con la partecipazione di due società: T4i di Padova per l'innovativo propulsore ibrido e GVM per il sistema avionico di controllo e comando. Il programma è in corso da alcuni anni per verificare sia alcune tecnologie che aspetti aerodinamici legati alle operazioni in volo. Questi test sono stati effettuati dal Poligono Interforze in Sardegna con un lancio suborbitale legato alla

propulsione, e voli in Florida di alcuni simulacri non attivi e in scala ridotta del vettore effettuati con lo Starfighter F-104 e Alphajet. Dopo la serie di test preparatori, il 22 aprile si è arrivati al collaudo a lungo inseguito: il lancio di un vettore funzionante dall'ala di un Alphajet. Ciò, ha consentito di verificare l'efficace gestione del lancio dal velivolo, il sistema di propulsione e il controllo della traiettoria. Il decollo è avvenuto dall'Ellington Airport vicino a Houston (Texas). Dopo il distacco dal jet, il vettore lungo cinque metri e acceso prima del distacco, ha seguito un arco parabolico in un'area riservata di cento chilometri nel Golfo del Messico, attivando i riferimenti Starlink e arrivando alla quota calcolata di 98,5 chilometri.

L'elemento innovativo è sicuramente il sistema di propulsione ideato da T4i che nel vettore HAX25 era formato da quattro motori funzionanti ad acqua ossigenata con un materiale plastico come comburente e combustibile. Il valore di questo tipo di propulsore è che si può spegnere e riaccendere a seconda delle necessità, oltre ad essere più semplice ingegneristicamente. "In esso, precisa Daniele Pavarin, Ceo e fondatore della società - sono integrati apparati innovativi, come le micropompe ad esempio, concepiti secondo criteri molto economici che rendono l'insieme competitivo sul mercato del settore".

"Il test ha concluso positivamente una prima fase di sviluppo dimostrando una corretta concezione del programma - sottolineano Lucia Paciucci project manager e Pantaleone Carlucci responsabile tecnico alla guida del progetto all'interno del Cnr -. Ciò, permette di guardare alla seconda fase già delineata per arrivare alla meta stabilita".

Le attività finora condotte, sono state sostenute da un finanziamento di 12 milioni di euro. Davanti si apre quindi la seconda fase che ha per obiettivo un vettore di maggiori dimensioni in grado di lanciare dalla quota di tangenza del jet satelliti inizialmente di 120 chilogrammi, sino ad arrivare, gradualmente, a 400 chilogrammi. A livello internazionale (negli Stati Uniti, Cina e Russia), ci sono state in passato esperienze analoghe molto ristrette senza favorire alcuna evoluzione. Adesso i contesti e le tecnologie sono mutati e quindi la sfida può essere affrontata con occhi diversi. L'obiettivo del programma italiano è di arrivare a disporre di un lanciatore non vincolato da una base di lancio e soprattutto pronto a trasportare in orbita satelliti con ridotto preavviso per rispondere a improvvise necessità, come in genere sicurezza e difesa possono richiedere. L'opportunità dell'aviolancio, una volta dimostrata l'efficacia e il vantaggio economico, potrebbe essere una delle soluzioni per rispondere e superare il collo di bottiglia esistente per un più facile accesso allo spazio.



L'Accesso allo Spazio Richiede un Nuovo Paradigma

Programma HA25X: La rivoluzione strategica dell'avolancio italiano per superare il collo di bottiglia orbitale.



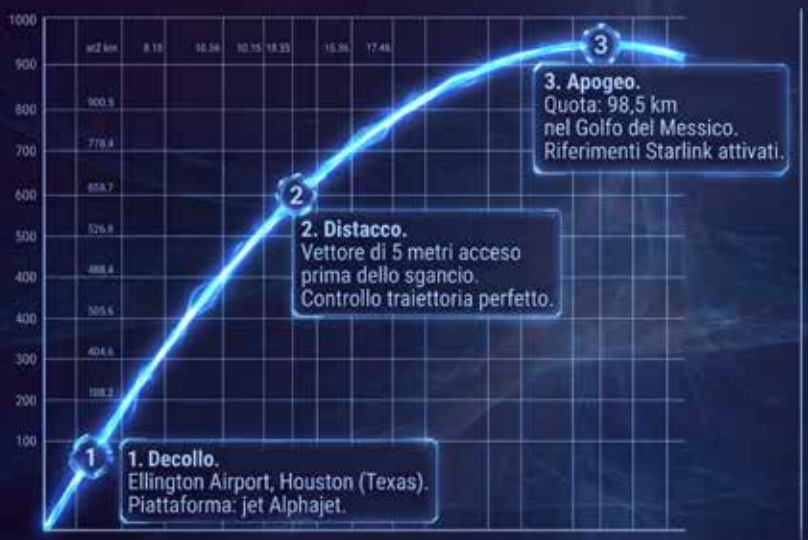
DATI TELEMETRICI PRELIMINARI

VELOCITÀ DI RILASCIO:	MACH 0.8
ANGOLO DI ATTACCO:	25 GRADI
ACCELERAZIONE INIZIALE:	4.5 G
CAPACITÀ ORBITALE CRITICA:	98% (TARGET)

IMPATTO STRATEGICO

RIDUZIONE COSTI LANCIO:	40%
ACCESSO RAPIDO LEO:	< 48 ORE
INDIPENDENZA NAZIONALE:	100%

Anatomia di un Successo: Il Test di Houston del 22 Aprile



1. Decollo.
Ellington Airport, Houston (Texas).
Piattaforma: jet Alphajet.

2. Distacco.
Vettore di 5 metri acceso prima dello sgancio.
Controllo traiettoria perfetto.

3. Apogeo.
Quota: 98,5 km
nel Golfo del Messico.
Riferimenti Starlink attivati.



Avionica (GMV):
Sistema proprietario per il controllo preciso della traiettoria.

Coordinamento (CNR):
Validazione aerodinamica, 12 M€ investiti nella Fase 1.

Propulsione Ibrida (T4i):
4 motori ad acqua ossigenata. Riaccensione on-demand, design economico con micropompe.

Roadmap e Vantaggio Tattico per la Difesa

Metrica	Lanciatori Convenzionali	Aviolancio HA25X
Dipendenza da Basi	Alta (Spazioporti terrestri)	**Zero (Operabile da piste standard)**
Preavviso di Lancio	Mesi o Anni	**Ridottissimo (On-demand)**
Uso Primario	Grandi carichi pianificati	**Sicurezza, Difesa e urgenze tattiche**

Evoluzione Fase 2



Step 1: Dimostrazione (Attuale).
Validazione suborbitale completata. 12 M€ investiti.

Step 2: Prossimo Obiettivo.
Lancio da quota di tangenza con payload di 120 kg.

Step 3: Target Finale.
Scalabilità fino a satelliti da 400 kg in orbita.


ZQ-3

ZHUQUE-3 ATTERRA CON SUCCESSO, ANCHE LA CINA HA I SUOI RAZZI RIUTILIZZABILI

Il successo di LandSpace segna un passaggio importante per il programma spaziale commerciale cinese.
Il primo stadio dello Zhuque-3 è rientrato sulla terraferma dopo aver portato in orbita il satellite Honghu-03



Il 19 agosto 2026 lo Zhuque-3 Y2 di LandSpace ha raggiunto l'orbita e, contemporaneamente, ha riportato sulla Terra il proprio primo stadio, completando un atterraggio verticale nella provincia del Gansu. Il lancio è avvenuto alle 7.35, ora di Pechino, dalla Dongfeng Commercial Space Innovation Pilot Zone. Circa sei minuti dopo la separazione degli stadi, il booster ha concluso la discesa nella zona predisposta per il recupero, a circa 390 chilometri dal punto di partenza. Il primo stadio ha modificato l'assetto, utilizzato i motori durante la discesa e completato la frenata finale fino a posarsi sulle proprie gambe. Il secondo stadio ha invece proseguito la missione, portando il satellite Honghu-03 nell'orbita prevista.

Per la Cina commerciale è un passaggio significativo perché porta nel settore privato una tecnologia finora dimostrata soprattutto negli Stati Uniti. Un booster recuperabile consente infatti, almeno in prospettiva, di distribuire il costo di costruzione su più missioni e di aumentare la frequenza dei lanci. Il vantaggio economico, tuttavia, non deriva dal solo recupero: deve essere accompagnato da procedure rapide di ispezione, manutenzione e ricondizionamento. La vera prova industriale sarà, quindi, il ritorno in servizio dello stesso hardware.

LandSpace arriva a questo risultato dopo il fallimento del primo tentativo. Il 3 dicembre 2025 lo Zhuque-3 aveva raggiunto l'orbita, ma il recupero del primo stadio non era riuscito. Il volo di agosto dimostra che l'azienda ha trasformato quell'esperienza in una procedura di rientro controllato e atterraggio verticale. Il vettore utilizza ossigeno liquido e metano ed è progettato fin dall'origine per la riutilizzabilità.

La Cina, però, sta sperimentando più soluzioni contemporaneamente e il 10 luglio 2026 il Long March-10B, sviluppato dall'apparato spaziale statale, aveva completato un test di recupero mediante

cattura con rete su una piattaforma marittima. Zhuque-3 utilizza, invece, il rientro propulsivo e l'atterraggio autonomo sulla terraferma. Sono due architetture differenti per raggiungere lo stesso obiettivo: trasformare il primo stadio da elemento monouso in componente riutilizzabile di una catena di lancio.

La differenza rispetto al passato non è soltanto tecnologica. La crescita delle costellazioni satellitari aumenta la domanda di lanci frequenti per comunicazioni, osservazione della Terra, navigazione e servizi Internet. In questo scenario la capacità di lanciare, recuperare e rilanciare un vettore può diventare un fattore determinante della competitività spaziale. Il razzo tende così a trasformarsi da prodotto destinato a una singola missione, in una piattaforma operativa utilizzabile più volte.

È questo il modello che SpaceX ha reso operativo con il Falcon 9 e che anche Blue Origin sta sviluppando. La Cina cerca ora di costruire una propria filiera, combinando il grande apparato spaziale statale con società commerciali come LandSpace. Il prossimo passaggio sarà decisivo: l'azienda ha indicato l'obiettivo di riutilizzare il booster recuperato entro sei mesi, mentre il progetto prevede un primo stadio capace, nelle intenzioni progettuali, di effettuare numerosi voli. Si tratta però di obiettivi ancora da dimostrare sul piano operativo.

L'Europa prepara i propri dimostratori

La competizione sulla riutilizzabilità coinvolge anche l'Europa, che si trova tuttavia in una fase ancora sperimentale. Il programma di riferimento è Themis, sviluppato dall'ESA con ArianeGroup, un dimostratore destinato a verificare le tecnologie necessarie per uno stadio riutilizzabile. Il veicolo utilizza il motore Prometheus, alimentato a ossigeno liquido e metano.

Nel luglio 2026 Themis ha completato a Esrange, in Svezia, una wet dress rehearsal, cioè una prova generale delle operazioni di preparazione e rifornimento del veicolo. Il percorso porterà a un primo volo dimostrativo, inizialmente limitato a un breve hop suborbitale. L'Europa non dispone, quindi, ancora di una capacità equivalente al recupero orbitale dimostrato da LandSpace, ma sta costruendo progressivamente le tecnologie necessarie per arrivarci.

La questione europea non riguarda soltanto il lanciatore, la riutilizzabilità richiede un sistema integrato nel quale propulsione, controllo del volo, strutture, protezione termica, atterraggio, infrastrutture e manutenzione siano progettati per operare come un'unica catena. È questa integrazione che determina la possibilità di trasformare un dimostratore tecnologico in un servizio di lancio.

L'Italia punta sull'aviolancio

In questo scenario, l'Italia sta sviluppando una strada complementare. Il crescente fabbisogno di accesso allo spazio impone infatti non soltanto nuovi lanciatori, ma anche infrastrutture e modalità di lancio più flessibili. Il programma governativo Aviolancio, coordinato dal Cnr per conto della Presidenza del Consiglio dei Ministri, punta a sviluppare un sistema di lancio aviotrasportato a propulsione ibrida, destinato a rafforzare una capacità nazionale autonoma e flessibile di accesso allo spazio.

Il programma ha compiuto un passaggio concreto il 22 aprile 2026 con la prima missione dimostrativa del sistema suborbitale. Il dimostratore HAX25 è stato trasportato da un Dornier Alpha Jet decollato dallo Houston Spaceport e rilasciato in un'area riservata del Golfo del Messico. Il test ha verificato l'intera catena operativa, dall'integrazione del vettore sul velivolo alle interfacce meccaniche ed elettriche, dall'avionica al monitoraggio in tempo reale, fino al rilascio e al volo autonomo.

Il valore dell'aviolancio è soprattutto nella flessibilità. Un vettore trasportato da un aereo può essere portato nell'area di lancio senza dipendere integralmente da una piattaforma verticale fissa e può modificare il punto di rilascio in funzione delle condizioni operative. Il Cnr sottolinea, inoltre, la possibilità di riprogrammare una missione con poche ore di anticipo, caratteristica particolarmente interessante per attività scientifiche e tecnologiche e, in prospettiva, per esigenze di sicurezza e sperimentazione suborbitale.

L'HAX25 non è ancora un lanciatore orbitale operativo: il dimostratore appartiene alla fase suborbitale del programma. Il progetto complessivo prevede però anche la progettazione preliminare del veicolo di inserimento orbitale e delle infrastrutture necessarie alla gestione di un microlanciatore. L'obiettivo è quindi costruire progressivamente una capacità di accesso allo spazio che possa affiancare le tradizionali modalità di lancio.

Una nuova economia del lancio

Zhuque-3, Themis e Aviolancio rappresentano tre momenti diversi della stessa trasformazione. La Cina sta già dimostrando in volo il recupero di primi stadi attraverso soluzioni differenti; l'Europa sta verificando con Themis le tecnologie per arrivare alla riutilizzabilità; l'Italia lavora su un'architettura aviotrasportata orientata alla flessibilità e all'autonomia dell'accesso allo spazio.

La posta in gioco è la capacità di rispondere a una domanda crescente senza moltiplicare nella stessa proporzione costi, tempi e infrastrutture. La riutilizzabilità è una risposta possibile, mentre l'aviolancio rappresenta un'altra modalità per aumentare la flessibilità operativa. Entrambe indicano un cambiamento di paradigma: il lancio spaziale tende a diventare un servizio disponibile con maggiore frequenza, nel quale contano non soltanto la potenza del vettore, ma anche la rapidità con cui può essere preparato, impiegato e, quando previsto, nuovamente utilizzato.

Per LandSpace il prossimo traguardo sarà dunque più importante dell'atterraggio del 19 agosto: dimostrare che il booster recuperato può tornare a volare. Per l'Europa sarà invece decisivo trasformare Themis da dimostratore in tecnologia applicabile ai futuri lanciatori. Per l'Italia, la sfida sarà portare l'aviolancio dalla dimostrazione suborbitale a una capacità concreta di accesso allo spazio. È su questa capacità di passare dal singolo test alla continuità operativa che si giocherà la nuova competizione spaziale.




AI Generate

ANTONIO LO CAMPO

GIORNALISTA AEROSPAZIO

GUERRE STELLARI

Dalla “Guerre stellari” di Reagan alle nuove armi spaziali annunciate da Washington. Gli Stati Uniti confermano capacità di controllo orbitale, mentre Cina e Russia denunciano la militarizzazione dello spazio

Negli anni ottanta era noto con la sigla SDI (Strategic Defense Initiative). Progetto fortemente voluto e finanziato dall’Amministrazione Reagan, e mediaticamente noto come “Guerre stellari”. Un progetto che gli USA avevano ideato come protezione dall’attacco di missili balistici nucleari. Un programma molto articolato e dispendioso, al punto tale che persino alcune missioni dello Space Shuttle, e quindi con equipaggio, vennero dedicate ad alcuni test in ambito SDI, in particolare con fasci laser.

Oggi molto è cambiato rispetto ad allora, a cominciare dal progetto stesso, ma un bel po’ di guerra fredda è rimasta. La vicenda non ha stupito gli analisti, più in generale ha stupito la prima ammissione pubblica su un programma militare di tale portata, l’annuncio alla “Air, Space, Cyber Conference” lo scorso 14 settembre, quando Troy Meink, Segretario dell’Aeronautica statunitense, nel suo intervento ha annunciato che Washington ha schierato armamenti nello spazio, il cui compito è “il controllo dello spazio”.

Meink ha aggiunto che gli Stati Uniti hanno messo in campo armi per il controllo dello spazio in orbita, capaci di difendere la Joint Force da azioni ostili di avversari: “continuiamo a garantire di essere pronti ad affrontare le sfide poste dalle minacce in continua evoluzione, ovunque esse si manifestino”. Ma, naturalmente, non è entrato nei dettagli sulla natura di tali armi, sul loro funzionamento o se fossero destinate a colpire altri oggetti nello spazio o sulla Terra.

Un portavoce della US Space Force ha comunque spiegato che il controllo dello spazio può riferirsi all’impiego di mezzi cinetici (quindi missili), e non cinetici, (quindi laser o disturbi elettronico che danneggiano senza distruggere l’obiettivo, per incidere sulle capacità avversarie). Ha anche aggiunto che «queste capacità possono essere impiegate per scopi offensivi e difensivi».

Nel 2019, durante il suo primo mandato, Trump ha istituito la Space Force come ramo autonomo delle forze armate. Nel corso del suo secondo mandato, ha annunciato il sistema di difesa missilistica “Golden Dome”, che include piani per il dispiegamento di armi statunitensi nello spazio. Trump ha, inoltre, ordinato al Pentagono di sviluppare intercettori spaziali tramite un ordine esecutivo emanato



durante la prima settimana della sua presidenza. Il Congressional Budget Office ha stimato che i soli componenti spaziali del sistema "Golden Dome" potrebbero costare fino a 542 miliardi di dollari nei prossimi 20 anni.

Si tratta di capacità che possono essere utilizzate anche a scopo dimostrativo, come è successo nel corso di esperimenti di guerre stellari noti come DA-ASAT (Direct Ascent Anti-Satellite), durante i quali un missile lanciato da terra distrugge un satellite non più operativo della stessa nazione che funge da bersaglio. Nel corso degli anni, queste azioni dimostrative sono state condotte dalla Cina (nel 2007), dagli USA (nel 2008), dall'India (nel 2019) e dalla Russia (nel 2021). Tecnicamente non è un atto bellico perché le varie nazioni hanno colpito dei loro satelliti, ma naturalmente questo tipo di test vanno ulteriormente ad impattare la situazione dei detriti spaziali presenti soprattutto nelle basse orbite.

Basti citare il test cinese del 2007 che, distruggendo un satellite a 700 km di altezza, ha prodotto 2000 frammenti, gran parte dei quali sono ancora pericolosamente in orbita, obbligando la Stazione Spaziale Internazionale a effettuare manovre di sicurezza per schivarli. Invece, i test antisatellite eseguiti da USA e India hanno distrutto oggetti a meno di 300 km di altezza e i detriti sono stati ripuliti dall'atmosfera. Considerando le stringenti nuove normative per evitare la proliferazione (ulteriore) dei detriti nello spazio, è ragionevole pensare che le armi evocate da Meink siano di tipo non cinetico e che utilizzano laser, fasci di microonde o qualche disturbo elettronico capace di accecare momentaneamente oppure di mettere definitivamente fuori uso i satelliti avversari. Chi controlla il traffico orbitale ha anche rivelato movimenti sospetti di satelliti che manovrano per avvicinarsi ad altri, magari per intercettare le trasmissioni. El'attacconondevenecessariamente essere diretto contro satelliti militari: mettere fuori uso, o anche solo disturbare, i satelliti per le comunicazioni, per esempio, creerebbe danni per tutti gli utilizzatori. Starlink sostiene di avere più volte sventato attacchi russi, senza però dare dettagli.

Subito dopo l'annuncio di Meink, la Cina ha invitato a non militarizzare lo spazio e la Russia ha risposto attraverso il portavoce del Cremlino, Dmitrij Peskov, affermando che: "lo spazio deve essere libero da qualsiasi arma". Ma è ben noto che tutte le grandi potenze spaziali (Cina e Russia comprese) dispongono di sistemi difensivi che, all'occorrenza, possono diventare offensivi. Due anni fa, gli Stati Uniti avevano avvertito che la Russia stava sviluppando una nuova arma antisatellite basata nello spazio, sebbene all'epoca la Casa Bianca avesse affermato che il pericolo non fosse imminente. Tuttavia, le notizie relative all'arma antisatellite riflettevano preoccupazioni di lunga data riguardo alle minacce spaziali provenienti da Russia e Cina, dato che gran parte delle infrastrutture statunitensi dipende dalle comunicazioni satellitari. In passato, anche gli Stati Uniti hanno dimostrato la propria capacità di abbattere satelliti dalla Terra. Per ciò che concerne gli aspetti legali, va ricordato che il noto Outer Space Treaty del 1967 non vieta categoricamente di mettere in orbita qualsiasi tipo di armi. Quello che è proibito è l'utilizzo di armi nucleari o di altre armi di distruzione di massa, vuoi in orbita terrestre vuoi nello spazio. Per questa ragione, la pratica annunciata da Meink non viola il diritto internazionale.

LA GUERRA DI MANOVRA ARRIVA IN ORBITA

La competizione nello spazio sta trasformando l'impiego militare dei satelliti. Con l'esercitazione Apollo Maneuvers 2026, lo US Space Command ha testato la capacità di riposizionare rapidamente i veicoli spaziali, modificandone l'orbita in risposta a minacce, esigenze operative o movimenti satellitari. Un satellite non deve soltanto mantenere la propria posizione, ma poter manovrare, osservare, evitare e reagire. La capacità di movimento diventa parte della deterrenza e della sopravvivenza dei sistemi spaziali. Un veicolo prevedibile può essere più facilmente monitorato e, in crisi, potenzialmente contrastato. Al contrario, la manovrabilità consente di complicare la pianificazione dell'avversario e preservare capacità essenziali per comunicazioni, intelligence, navigazione e operazioni terrestri. L'esercitazione americana assume rilievo alla luce dei progressi cinesi nelle operazioni di prossimità orbitale. Washington considera sempre più necessario disporre di sistemi capaci di operare in condizioni dinamiche e contestate. La competizione spaziale, dunque, non riguarderà solo chi possiede più satelliti, ma chi saprà manovrarli e mantenerli operativi in un'orbita contesa.

Liguria, un *mare* di borghi



Noli

REGIONE LIGURIA

lamialiguria

MINISTERO
DELLA DIFESA

DIFESA 2025 REPORT



Pdf Report
Difesa 2025