airpress
a17

MENSILE SULLE POLITICHE PER L'AEROSPAZIO E LA DIFESA
Maggio 2026

Strait Forward

M. Annati, M. Braccioli, E. Braw
N. Childs, J. Coito, E. Credendino
J. G. Foggo, C. Petrioli, B. D. Sadler
F. Sanfelice di Monteforte, G. Valentino

L'intervista

Il potere del mare
Roberta Pinotti

SPACE

Satelliti in tilt per un chip

Marco Lisi

SKY

Pattugliatori, è tempo di scegliere

Gregory Alegi


SPACE FOR LIFE
CREDIAMO NELLO SPAZIO COME
NUOVO ORIZZONTE DELL'UMANITÀ
PER COSTRUIRE UNA VITA SULLA TERRA
MIGLIORE E SOSTENIBILE.
ThalesAlenia
a Thales / Leonardo company
Space

Editoriale

Da oggi quando leggeremo di un drone armato che ha colpito un obiettivo, oppure di un missile che ha centrato un target grazie alle informazioni fornite in tempo reale da un software programmato dall'Intelligenza artificiale, non potremo che pensare a papa Leone XIV e alla sua prima enciclica, che, non a caso si chiama *Magnifica Humanitas*. Nell'affermazione dirompente dell'Intelligenza artificiale, il pontefice ha scelto una posizione politica e netta, tracciando un perimetro di umanità oltre il quale si diventa "eretici", si rinnega la propria origine. Perché se l'IA significa progresso, efficienza, velocità nelle scelte, automatizzazione, questa tecnologia applicata alla guerra significa deresponsabilizzare, disumanizzare, rendere le operazioni a volte amorali, trasformando le vittime in dati. Nella forza della tecnologia e del progresso inevitabile, il papa prova a circoscrivere una potenza che tende a non avere confini. Lo stesso Henry Kissinger prima di morire aveva definito la pervasività e la potenza dell'IA come una sfida che sarebbe stata per il pianeta più pericolosa di quella atomica nel 1900. Il papa ci invita a riflettere prima che sia troppo tardi e che la magnifica invenzione diventi "più" magnifica dell'uomo, che lo travolga, insomma. Una discussione etica che negli Usa ha visto, di recente, contrapposti il Pentagono e Anthropic (la realtà della Silicon Valley che ha creato Claude, il modello di IA che utilizzano le Forze americane nelle operazioni militari), ossia la stessa società invitata, con il suo fondatore Christopher Olah, alla presentazione del testo di Leone nella città del Vaticano. E presto ricevuta, con l'altro fondatore Dario Amodei, anche dal nostro governo. I pontefici, nella storia, hanno spesso ammonito contro le guerre, ma questa volta è diverso. Con il suo primo testo, Leone fa emergere un legame tra l'IA e il conflitto, convinto che la tecnologia possa rendere più "accettabile" e quindi far considerare giusta una guerra. Un ruolo subdolo, dal quale diffidare. Stessa postura per le armi autonome, viste da Leone come l'elemento che toglie all'uomo la capacità di distinguere il bene e dal male e di sottrarsi alle proprie responsabilità durante una guerra. Insomma, la Chiesa ha fornito agli addetti ai lavori del mondo della Difesa una bussola preziosa per governare le nuove sfide tecnologiche, guardando oltre e rimettendo al proprio posto l'etica, prima della piena rivoluzione dell'IA.

Flavia Giacobbe

Indice

Airpress
Agenzia stampa aeronautica tecnica politica
Registrazione Tribunale di Roma n. 10311 del 7/4/1965. Registrazione R.O.C. n. 9884

Editore Base per altezza s.r.l.
corso Vittorio Emanuele II, 18 · 00186 Roma

telefono 06 454 73 850 · fax 06 455 41 354
partita iva 05831150966

Rivista fondata da Fausto Alati

Direttore responsabile
FLAVIA GIACOBBE

Redazione
RICCARDO LEONI
MARCO DE ROBERTIS

Progetto grafico
BLUEFORMA DESIGN

Impaginazione e grafica
INTORNO DESIGN

Per comunicati, abbonamenti, pubblicità
airpress@formiche.net

Recapito a cura di Fdc Services srl

Numero chiuso in redazione
il 26 maggio 2026

Finito di stampare
il 28 maggio 2026

Stampato in Italia
da Rubettino print

Viale Rubbettino, 10
88049 Soveria Mannelli

Contributors

ENRICO CREDENDINO

Ammiraglio di squadra, capo di Stato maggiore della Marina militare emerito. Entrato in accademia navale nel 1980, è stato a capo della Squadra navale, della Forza anfibia italo-spagnola, del Gruppo navale italiano e della forza europea Eunavfor nell'operazione Atalanta. È stato inoltre comandante dell'operazione Ue Eunavfor Med Sophia e comandante delle Scuole della Marina, ricoprendo anche altri incarichi di vertice negli Stati maggiori della Marina e della Difesa.

ROBERTA PINOTTI

Presidente della fondazione del Polo nazionale della dimensione subacquea. Già ministro della Difesa con i governi Renzi e Gentiloni, prima donna a ricoprire l'incarico nella storia italiana, ha successivamente presieduto la commissione Difesa del senato della Repubblica dal 2020 al 2022. Eletta al Parlamento nel 2001, è stata anche presidente della commissione Difesa della Camera dei Deputati e sottosegretaria alla Difesa nell'esecutivo Letta.

FERDINANDO SANFELICE DI MONTEFORTE

Ammiraglio, esperto di affari militari, docente di Studi strategici e presidente di Mediterranean insecurity. Già comandante della fregata Maestrale e dell'incrociatore Andrea Doria, è stato capo di Stato maggiore della Seconda divisione navale. Ha guidato le Forze navali alleate del sud Europa e l'operazione Nato Active endeavour, rappresentando poi l'Italia ai comitati militari Nato e Ue. È stato a capo della Pubblica informazione della Marina e direttore di Rivista marittima.

JAMES GORDON FOGGO III

Ammiraglio della Marina degli Stati Uniti e preside del Center for maritime strategy, è stato comandante delle Forze navali Usa in Europa-Africa, dell'Allied Jfc di Napoli e della sesta Flotta Usa. Diplomato nel 1981 all'Accademia navale degli Stati Uniti, Foggo è stato comandante di sottomarini, e tra i suoi comandi c'è stato il sottomarino d'attacco Uss Oklahoma City nel 1998 e il sesto squadrone sottomarini nel 2007.

CHIARA PETRIOLI

Professoressa di Informatica e ingegneria all'Università di Roma La Sapienza, dove dirige due laboratori e ha ricoperto ruoli di *leadership*, tra cui prorettrice per *scouting*, *fundraising* e incubazione Pmi. Fondatrice e ceo di WSense, è tra le ricercatrici più citate a livello internazionale, con numerosi premi nell'ambito dell'innovazione e dell'Internet of underwater things.

MARCO LISI

Inviato speciale per lo Spazio del ministero degli Affari Esteri e membro del CdA dell'Agenzia spaziale italiana. Già executive manager dell'Esa, è stato chief technical advisor della European Gnss agency e special advisor della Commissione europea. In precedenza ha ricoperto ruoli manageriali in Telespazio nei settori aerospazio, difesa e telecomunicazioni. Laureato in Ingegneria alla Sapienza, è autore di brevetti internazionali e oltre 350 pubblicazioni tecniche.

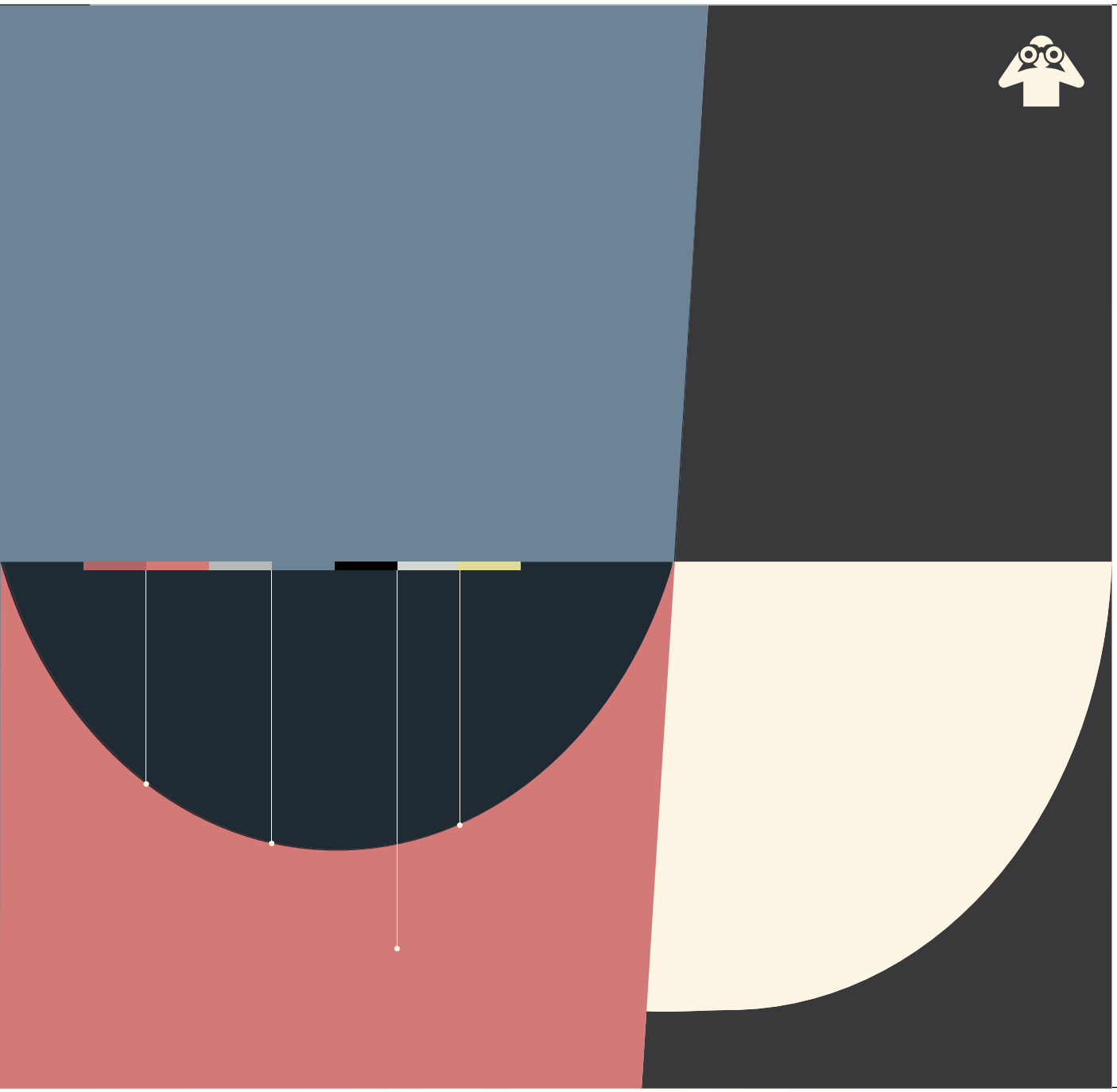
Il mare non è lo sfondo dell'economia italiana: ne è il motore. Quando quel motore si inceppa, il conto lo paga il Paese intero. Teheran ha riproposto il copione della guerra delle petroliere, integrandolo con tecnologie come mine a ormeggio, droni kamikaze, missili costieri, spoofing e manipolazione dei dati per indurre deviazioni di rotta. Una guerra ibrida in cui l'arma più efficace non è stata la più costosa o la più visibile. È stata quella nascosta sott'acqua: silenziosa, invisibile, attiva ben prima che qualcuno potesse intervenire

Le nuove armi *dell'acqua*

ENRICO CREDENDINO
capo di Stato maggiore della Marina emerito

Come diceva Jacques-Yves Cousteau, noi veniamo dal mare e dipendiamo dal mare. Basta guardare una fotografia della Terra per capirlo: il 70% della superficie è di colore blu. Eppure per troppo tempo abbiamo trattato il mare come uno sfondo, uno spazio neutro delle nostre attività. Per l'Italia questo equivoco ha un costo che non possiamo più permetterci di ignorare. La direttiva strategica per la sicurezza nel Mediterraneo allargato ha finalmente sancito per iscritto una verità che la Marina sosteneva da tempo: l'Italia è una potenza regionale a prevalente connotazione marittima. Questo significa che oltre il 90% delle nostre merci viaggia via mare. Che il gas che riscalda le nostre case arriva per gasdotti sottomarini dall'Algeria con il Transmed, dalla Libia con il Greenstream, dall'Azerbaijan con il Tap. Che il 40% del nostro *import-export* transita per il canale di Suez. Che il 98% delle comunicazioni digitali globali — non i satelliti, come si crede comunemente, ma i cavi in fibra ottica posati sui fondali — connettono l'Europa con l'Asia e l'Africa passando proprio per il Mediterraneo, che da solo, pur rappresentando l'1% della superficie d'acqua mondiale, ospita il 20% del traffico dati del pianeta. Il mare non è lo sfondo dell'economia italiana: ne è il motore. E ogni volta che quel motore si inceppa, il conto lo paga il Paese intero.

Il 23 marzo 2021, una portacontainer lunga quattrocento metri (la Ever Given) si incagliò in diagonale nel canale di Suez, bloccandolo completamente per sei giorni. Oltre quattrocento navi rimasero bloccate alle due estremità. *Bloomberg* calcolò perdite per circa dieci miliardi di dollari al giorno. Le compagnie che non potevano aspettare furono costrette a circumnavigare il Capo di Buona Speranza: seimila chilometri in più, fino a venti giorni aggiuntivi di navigazione, trecentomila dollari di extra-carburante per ogni superpetroliera, significativo aumento dei premi assicurativi a causa di rischi operativi e marittimi mag-



giori. Non ci fu alcun atto ostile, nessuna strategia militare: solo una nave finita di traverso per il vento. Eppure bastò a paralizzare una quota significativa del commercio mondiale, con code nei porti, mancanza di *container* e noli impegnati, per settimane.
La lezione non fu metabolizzata con la velocità necessaria. Dal dicembre 2023, i ribelli Houthi dello Yemen hanno attaccato sistematicamente il traffico commerciale nel mar Rosso. Missili, droni, minacce di abbordaggio: il risultato è che decine di compagnie armatoriali hanno sospeso la rotta per Bab el-Mandeb e il canale di Suez, dirottando le flotte verso l'Africa. I tempi di percorrenza da Asia a Europa sono passati da sette a venti giorni. Il traffico passeggeri nel Mediterraneo ha subito un calo drastico. Il prezzo di un *container standard* da Shanghai a Genova è salito da circa 1.400 a oltre seimila dollari. I porti italiani, specialmente quelli orientali, hanno visto contrarsi in modo significativo i volumi di movimentazione.
Ma c'è una conseguenza sistemica che mi preoccupa ben oltre i dati di breve periodo. Se le rotte mediterranee perdono affidabilità, il traffico tende a spostarsi strutturalmente verso i grandi *hub* del nord Europa (Rotterdam, Amburgo, Anversa), serviti da rotte atlantiche che aggirano l'instabilità del Mare nostrum. Ogni crisi prolungata è un argomento in più per chi valuta di scegliere la via del nord. Per un Paese come l'Italia, che del Mediterraneo fa il proprio vantaggio geografico naturale, perderne la centralità non è una questione di geopolitica astratta: è una questione di sistema produttivo, di occupazione, di competitività del Made in Italy. La geografia ci ha donato una posizione invidiabile al centro del Mediterraneo. Non possiamo permettere che le crisi ce la sottraggano per inerzia.
Se la Ever Given fu un incidente e gli Houthi un attore non statale, ciò che è accaduto a Hormuz dal 28 febbraio 2026 è qualcosa di qualitativamente diverso: la chiusura deliberata, da parte di uno Stato, del principale *chokepoint* energetico del pianeta, attraverso cui passava circa il 20% della produzione mondiale di petrolio. I transiti commerciali sono crollati del 97% in poche settimane. Il Brent ha toccato i cento dollari al barile, con effetti immediati su energia, fertilizzanti e inflazione globale. In pratica, Teheran ha riproposto il copione della "guerra delle petroliere" degli anni Ottanta, integrandolo però con le nuove tecnologie *unmanned*.
La strategia ha combinato in modo inedito strumenti vecchi e nuovi: mine navali a ormeggio (un'arma antica, economica, devastante e difficilissima da contrastare) droni *kamikaze* di superficie, missili costieri a corto raggio, *spoofing* dei segnali Gnss, manipolazione dei dati Ais per creare navi fantasma o indurre deviazioni di rotta fatali. Una guerra ibrida in cui il dominio cibernetico e quello fisico si sono fusi in modo indistinguibile. In questo scenario, l'arma più efficace non è stata la più costosa o la più visibile. È stata quella nascosta sott'acqua: silenziosa, invisibile, attiva ben prima che qualcuno potesse intervenire.
Ed è qui che arrivo al cuore di questa riflessione. Il dominio subacqueo è la nuova, vera, quinta dimensione fisica del conflitto. Quando si parla di terra, mare, cielo e spazio, il "mare" viene inteso come superficie. Un errore concettuale grave, perché le leggi fisiche che regolano la dimensione subacquea sono completamente diverse. I satelliti non vedono sott'acqua: l'onda elettromagnetica non penetra la colonna d'acqua. Gli operatori umani possono agire autonomamente fino a seicento metri con gli scafandri rigidi; inoltre, il teatro appartiene alle macchine. E, nel Mediterraneo, le profondità raggiungono i cinquemila metri.
Eppure è lì, in quell'ambiente che conosciamo meno della superficie di Giove (con l'80% degli alti fondali ancora inesplorato e solo il 2% degli abissi mappato) che si trovano le infrastrutture che tengono in vita la nostra economia e la nostra connettività. Colpir-

INTERNET OF UNDERWATER THINGS L'espressione indica reti di sensori, *modem* acustici, veicoli autonomi e nodi di raccolta dati distribuiti sotto la superficie del mare e capaci di comunicare tra loro. È l'equivalente subacqueo dell'Internet delle cose, ma in un ambiente molto più ostile, dove i segnali radio funzionano male e la trasmissione avviene soprattutto per via acustica. Il vantaggio è enorme. Queste reti consentono monitoraggio continuo, rilevazione di anomalie e raccolta di dati in tempo reale attorno a cavi, gasdotti e altre infrastrutture critiche che oggi restano spesso quasi invisibili.

le significa colpire senza firma, senza attribuzione immediata, in un ambiente dove raccogliere prove è tecnicamente quasi impossibile con i mezzi tradizionali. Il sabotaggio del Nord Stream nel settembre 2022 ha aperto questa stagione. Hormuz l'ha confermata e radicalizzata. E il teatro si è popolato di nuovi attori: la Cina conduce un'ampia attività sistematica di mappatura dei fondali dall'Indo-Pacifico all'Artico; la Russia ha sviluppato sistemi subacquei a propulsione nucleare concepiti per operare contro infrastrutture critiche in acque profonde.

Le nuove tecnologie ci impongono di rispondere con due capacità distinte ma inscindibili: monitorare e difendere. Non è possibile difendere ciò che non si vede. Il monitoraggio persistente dei fondali (attraverso reti di sensori distribuiti, sistemi di comunicazione acustica multi-frequenza operativi fino a tremila metri di profondità, piattaforme connesse nell'*Internet of underwater things*) ci consente per la prima volta di costruire una vera *underwater situation awareness*: sapere chi va dove e perché nei nostri fondali, rilevare anomalie fisiche o acustiche in prossimità delle infrastrutture critiche, trasmettere dati in tempo reale. Integrate con sistemi di intelligenza artificiale per l'analisi predittiva, queste reti trasformano la sorveglianza da reattiva in anticipatoria. La difesa attiva richiede poi sciami di veicoli autonomi subacquei (Auv e Rov cooperanti) sommergibili di nuova generazione, capacità di risposta rapida in profondità. Non le grandi piattaforme visibili e vulnerabili del passato: reti distribuite, modulari, difficili da neutralizzare con un singolo colpo.

La Marina militare non ha aspettato che le crisi rendessero urgente ciò che era già strategicamente evidente. Nel 2023 è stato lanciato il Polo nazionale della dimensione subacquea, con sede a La Spezia: un *hub* tecnologico che riunisce Difesa, grandi gruppi industriali (Fincantieri, Leonardo, Saipem, Eni, Sparkle) Pmi, università e centri di ricerca, per un totale di 251 operatori economici. Come ho sottolineato all'ultimo Transregional seapower symposium a Venezia di fronte ai capi di Stato maggiore di 67 Marine di tutto il mondo, la sfida degli abissi non si vince in ordine sparso: occorre mettere insieme tutto il *cluster* marittimo, con la stessa logica sistemica che ha fatto grande la corsa allo spazio. Nel subacqueo siamo ancora indietro rispetto a quella corsa, ma abbiamo un vantaggio competitivo che sarebbe imperdonabile non sfruttare. Il Polo è quella visione resa istituzione concreta, con linee di indirizzo approvate, priorità tecnologiche identificate e bandi di ricerca già operativi. Parallelamente, dopo il Nord Stream è stato istituito a Santa Rosa (sede del Comando in capo della Squadra navale – Cincnav) il Centro per la sorveglianza delle infrastrutture critiche subacquee, che sovrintende l'operazione Fondali sicuri. Ogni giorno, da quella centrale operativa multidominio, mezzi navali, subacquei e aerei della Marina (con il supporto della rete radar costiera) sorvegliano in tempo reale i tratti di mare percorsi dal Tap, dal Greenstream, dal Transmed e dai cavi di comunicazione che connettono l'Italia al mondo.

Adesso è il momento di correre. Esattamente come nella fisica, quando si crea un vuoto qualcuno lo riempie, e se non saremo noi a farlo, lo farà un'altra nazione. Sarebbe un errore grave non cogliere l'attimo: le crisi di questi anni (la Ever Given, gli Houthi, Hormuz) non sono anomalie destinate a non ripetersi. Sono la normalità del nuovo ordine marittimo mondiale. Il Polo nazionale e Santa Rosa sono la dimostrazione che l'Italia è in campo. La sfida è restare in prima linea con la stessa determinazione con cui, ogni giorno, la Marina militare presidia i nostri fondali.

Accanto ai sottomarini nucleari tradizionali ci sono oggi mini-sommergibili, droni subacquei autonomi, siluri intelligenti, mine, piattaforme senza insegne e navi civili trasformate in piattaforme operative. La vera lezione è questa: la superiorità navale convenzionale non garantisce più automaticamente la libertà di navigazione

Dal mar Nero a Hormuz, come cambiano tattiche e mezzi

MASSIMO ANNATI
contrammiraglio in congedo ed esperto di armamenti navali

Per oltre quarant'anni, le Marine occidentali hanno continuato a prepararsi a una battaglia che non è mai arrivata. Portaerei, gruppi da battaglia, superiorità aerea, controllo delle rotte oceaniche. Tutto concepito per uno scontro simmetrico tra grandi flotte. Nel frattempo, però, la guerra navale ha preso un'altra direzione. Non più la ricerca del dominio del mare distruggendo la flotta nemica: oltre alla tradizionale protezione delle linee di comunicazione marittima, è emersa la capacità di mantenere il nemico a distanza di sicurezza dalle proprie coste, o comunque dalle proprie aree d'interesse.

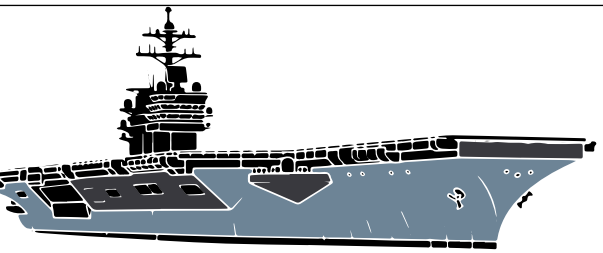
Questo cambiamento ha iniziato a manifestarsi in modo brutale già nel mar Nero. L'Ucraina, priva di una vera e propria marina militare, ha comunque inflitto danni enormi alla Flotta russa del mar Nero utilizzando sistemi relativamente economici, adattabili e difficili da contrastare. Droni navali di superficie, missili terrestri, ricognizione satellitare commerciale, droni aerei e operazioni coordinate in tempo reale hanno trasformato un attore militarmente inferiore in una minaccia credibile per una delle maggiori Marine del mondo.

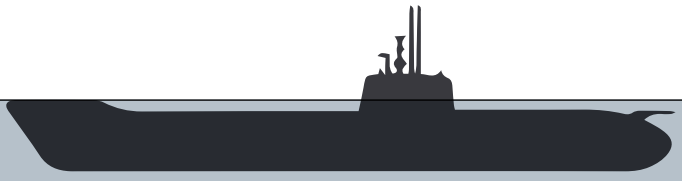
L'elemento più innovativo non è tanto il singolo mezzo, ma la combinazione dei domini. Un drone aereo individua il bersaglio, il dato viene trasmesso via satellite e un barchino esplosivo, guidato da remoto grazie a satelliti di comunicazione commerciali con bassa latenza, completa l'attacco. È la logica delle operazioni multi dominio applicata al mare. E soprattutto è una guerra che premia la saturazione, il numero, la dispersione e il basso costo. Le immagini dei droni marini ucraini che colpiscono unità russe a Sebastopoli hanno prodotto un effetto psicologico forse ancora più importante di quello operativo. Per la prima volta, piccole imbarcazioni senza equipaggio hanno dimostrato di poter minacciare navi da guerra sofisticate, obbligandole a ritirarsi dai porti o a modificare radicalmente le procedure operative. Il messaggio è chiaro: una piattaforma da miliardi può essere messa fuori combattimento da sistemi che costano poche decine di migliaia di euro.

Da allora il fenomeno si è esteso. Negli ultimi mesi si sono moltiplicati gli attacchi con droni marini contro le petroliere legate alla cosiddetta flotta fantasma russa nel Mediterraneo orientale. Episodi spesso poco chiari, attribuzioni incerte, dinamiche ibride che si collocano in quella zona grigia dove sabotaggi, guerra economica e operazioni clandestine tendono ormai a sovrapporsi. Anche il ritrovamento di un drone marino in una grotta dell'isola greca di Lefkada suggerisce quanto queste tecnologie stiano diventando pervasive, accessibili e sempre più difficili da tracciare.

Il punto centrale è che il teatro costiero sta tornando a essere uno spazio estremamente ostile. Per decenni le Marine della Nato hanno privilegiato l'oceano aperto,

BOLLA A2/AD La sigla indica una combinazione di capacità pensate per impedire all'avversario di entrare in un'area o di operarvi liberamente una volta penetrato. Missili costieri, mine, droni, sensori distribuiti, batterie mobili e piattaforme subacquee concorrono a creare una zona in cui il costo del passaggio diventa troppo alto. Il punto decisivo è che non serve controllare stabilmente il mare per ottenere un vantaggio strategico. Basta renderlo abbastanza pericoloso da rallentare, deviare o scoraggiare il traffico e le forze nemiche.





dove radar, sonar e superiorità aerea garantivano ampi margini di sicurezza. Oggi gli scenari più pericolosi sono invece gli stretti, gli arcipelaghi, le acque ristrette, i chokepoints. Ambienti nei quali piccoli mezzi veloci, droni subacquei, mine intelligenti e missili costieri possono creare bolle di interdizione molto efficaci.
È esattamente la strategia perseguita da anni dall'Iran nello stretto di Hormuz. Teheran sa perfettamente di non poter affrontare frontalmente la US Navy in uno scontro convenzionale e ha quindi costruito una dottrina fondata sull'asimmetria. Non punta a controllare il mare, ma a negarlo all'avversario abbastanza a lungo da produrre effetti politici ed economici globali.
I Pasdaran dispongono oggi di uno strumento estremamente articolato. Motoscafi armati di razzi e missili leggeri, batterie costiere mobili, droni suicidi a lungo raggio, mine navali, piccoli sommergibili, droni subacquei e imbarcazioni esplosive senza equipaggio. Sistemi relativamente economici, spesso ridondanti, distribuiti lungo coste frastagliate e facilmente occultabili.
Lo stretto di Hormuz rappresenta il terreno ideale per questo tipo di guerra, con acque basse, traffico commerciale densissimo e spazi ristretti. Una petroliera non può manovrare liberamente e un gruppo navale deve mantenere rotte prevedibili, restando sempre in vista da terra, mentre le minacce possono emergere da qualunque direzione, che si tratti di una batteria missilistica nascosta, di una mina sottomarina, di un motoscafo kamikaze, di un drone lanciato da terra o persino di una nave civile dotata di armamento in modo occulto.
L'esperienza delle *Tanker Wars* degli anni Ottanta avrebbe dovuto lasciare un insegnamento duraturo. Allora bastarono mine rudimentali, missili cinesi e sciami di piccoli barchini per mettere sotto pressione il traffico petrolifero mondiale e danneggiare seriamente unità americane. Oggi quelle stesse minacce sono molto più sofisticate. Eppure molte marine occidentali continuano a essere strutturate principalmente per conflitti simmetrici tradizionali ad alta intensità.
Il problema riguarda anche il rapporto costo-efficacia. Abbattere un drone da 50mila dollari con un missile antiaereo da due milioni è economicamente insostenibile nel lungo periodo e lo stesso vale per l'impiego di grandi unità navali contro sciami di bersagli piccoli, veloci e sacrificabili. Una guerra navale che tende quindi a favorire chi riesce a saturare il sistema difensivo avversario.
Anche il dominio subacqueo sta cambiando rapidamente. Accanto ai sottomarini nucleari tradizionali ci sono oggi mini-sommergibili, droni subacquei autonomi e siluri intelligenti capaci di operare vicino alle coste, contro porti, cavi sottomarini e infrastrutture energetiche offshore. In questo scenario la distinzione

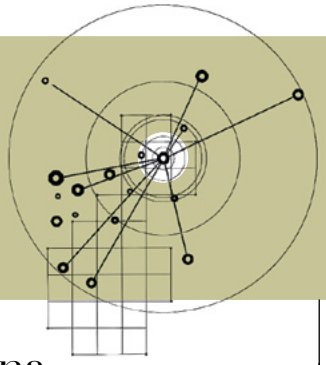
Italia e India stringono nuovi accordi sulla difesa

Italia e India rafforzeranno la cooperazione sulla difesa con una nuova cornice politica e industriale che amplia il rapporto bilaterale e lo inserisce in un partenariato più strutturato. Nel bilaterale tra Giorgia Meloni e Narendra Modi sono stati firmati una Roadmap per la cooperazione tra le industrie della difesa e una Dichiarazione congiunta d'intenti per rafforzare la collaborazione nel settore, mentre le relazioni tra i due Paesi sono state elevate al rango di Partenariato strategico speciale.
Il punto centrale della nuova intesa è la costruzione di un rapporto più profondo sul piano industriale e tecnologico. La Roadmap individua come aree prioritarie la cooperazione tecnologica, la coproduzione e il co-sviluppo di sistemi d'arma, in particolare elicotteri, piattaforme e armamenti navali e strumenti di guerra elettronica.
Accanto alla dimensione produttiva prende forma anche un livello più stabile di consultazione politico-militare. Italia e India hanno concordato di valutare un dialogo militare strutturato ad alto livello su base annuale, in aggiunta ai canali già esistenti. I due Paesi si sono inoltre impegnati a promuovere esercitazioni congiunte e corsi interforze, mentre è stato avviato un Dialogo sulla sicurezza marittima per incrementare coordinamento, scambio di informazioni e condivisione di pratiche operative nel dominio navale.
In parallelo agli accordi bilaterali, è stato sottoscritto un memorandum tra la Guardia di Finanza e il Directorate of Enforcement indiano sulla cooperazione finanziaria e l'antiriciclaggio, mentre sono state avviate discussioni per un accordo sullo scambio e la mutua protezione delle informazioni classificate e per un'intesa sul rafforzamento della cooperazione di polizia.
Gli accordi si inseriscono nel quadro del Piano d'azione strategica congiunta 2025-2029, adottato dai due leader a margine del G20 di Rio de Janeiro del novembre 2024, e consolidano un percorso di progressiva intensificazione dei rapporti bilaterali, segnato dalla presenza di Modi al G7 in Italia nel giugno 2024 e dalla visita di Meloni al G20 in India del 2023.
Sul piano industriale, Leonardo e Adani Defence & Aerospace hanno siglato un memorandum d'intesa per sviluppare in India un ecosistema industriale integrato nel settore elicotteristico destinato alle Forze armate indiane, con una progressiva localizzazione produttiva e delle attività di manutenzione, supporto logistico e addestramento. Nel settore della guerra elettronica è presente anche ELT Group, in linea con la crescente attenzione di Nuova Delhi verso queste capacità.
Sul fronte navale, Fincantieri ha stretto accordi di cooperazione strategica con Cochin Shipyard Limited, mentre, nella componentistica critica, Poggipolini ha acquisito una quota di maggioranza dell'indiana Aero Fasteners, mentre Ala Group ha sottoscritto un memorandum con Tvs Supply Chain Solutions per collaborare nel mercato indiano dell'aerospazio e della difesa.
•

tra guerra e non-guerra diventa sempre più sfumata. Mine che non esplodono, forse neppure posate, ma che bloccano il traffico commerciale per semplice deterrenza. Droni marini senza insegne. Navi civili trasformate in piattaforme operative. Attacchi difficili da attribuire con certezza. In altre parole, il mare sta diventando uno spazio permanente di competizione ibrida.
La vera lezione, dal mar Nero, al mar Rosso, a Hormuz, è probabilmente questa. La superiorità navale non garantisce più automaticamente la libertà di navigazione. Una grande marina può dominare l'oceano aperto e trovarsi comunque vulnerabile, o comunque incapace di proteggere il traffico mercantile nelle acque ristrette. Per questo molte potenze stanno oggi investendo non soltanto nella proiezione di forza, ma anche nella capacità di creare proprie bolle A2/AD (Anti-access/Area-denial) allo scopo di ostacolare le operazioni dell'avversario in aree di specifico interesse, ricorrendo a soluzioni asimmetriche.
La guerra navale del 21esimo secolo appare sempre meno fondata sul prestigio delle grandi piattaforme e sempre più sulla resilienza, sulla dispersione, sull'integrazione dei sensori e sulla velocità decisionale. Non vince necessariamente chi possiede la nave più potente, ma chi riesce a rendere il mare troppo pericoloso per l'avversario.

FLOTTA FANTASMA Con questa espressione si indica l'insieme di petroliere e navi commerciali usate per aggirare sanzioni, controlli assicurativi e tracciamento internazionale. Operano spesso con proprietà opache, registri deboli, spegnimento dei *transponder* e catene societarie difficili da ricostruire. In un contesto di conflittualità ibrida diventano qualcosa di più di un semplice strumento economico. Possono confondere attribuzioni, trasportare carichi sensibili, sostenere traffici strategici e perfino offrire copertura a operazioni ostili. Sono il volto marittimo della zona grigia tra commercio globale e confronto geopolitico.

WARTECH



di LUIGI MARTINO*

La dottrina orbitale della Cina *e le sue implicazioni strategiche*

Lo spazio non è più un ambiente di supporto alle operazioni militari terrestri. È diventato un dominio autonomo del conflitto, con una propria logica strategica e attori sempre più intenzionati a trasformare capacità tecnologiche in vantaggio operativo. La Cina, in particolare, ha avviato uno sviluppo strutturato di capacità di combattimento orbitale che merita un'analisi rigorosa. Come riportato dal *Financial Times*, già nel 2024 l'esperto militare cinese Jiang Lianju scriveva in un manuale per ufficiali della Pla: "Guardando i cieli oggi, vediamo che lo spazio è già avvolto dal fumo di un potenziale conflitto. Il controllo dello spazio per controllare la Terra rappresenta un potente incentivo strategico e militare". Non è propaganda, ma un enunciato dottrinale maturato nell'osservazione dei conflitti ad alta intensità degli ultimi decenni. Le radici teoriche di questo paradigma risalgono al 1999, quando Qiao Liang e Wang Xiangsui pubblicarono *Unrestricted Warfare*, testo chiave per comprendere l'approccio cinese alla guerra contemporanea. L'idea centrale è una guerra senza limiti di dominio: mezzi militari e non militari, cinetici e non-cinetici, integrati per paralizzare l'avversario. Lo spazio non è considerato un dominio separato, ma parte di un *continuum* bellico che comprende *cyber*, *near-space* e guerra dell'informazione. Al centro della dottrina della Pla vi è il concetto di *system destruction warfare*: non distruggere singole piattaforme, ma colpire i nodi critici di un "sistema di sistemi" per provocare una paralisi operativa a cascata. I bersagli includono comando e controllo, informazione, intelligence, logistica e potere di fuoco. In ambito spaziale questo significa operazioni contro satelliti C4ISR, reti di comunicazione, sistemi di *early warning* e infrastrutture di navigazione. Un singolo attacco (*cyber*, *jamming*, impulsi laser o detriti orbitali) può produrre effetti sistemici: perdita di *situational awareness*, interruzione del comando congiunto, impossibilità di guidare munizioni di precisione. La sequenza dottrinale cinese si articola in tre fasi: deterrenza, blocco spaziale e acquisizione della superiorità orbitale. Questo schema non è teorico. Nell'aprile 2025 il satellite americano Usa 324 ha registrato un incontro ravvicinato con i satelliti cinesi Tjs-16 e Tjs-17, osservati dal Pentagono come potenziali piattaforme di sorveglianza. Gli Stati Uniti hanno già definito alcune manovre cinesi come *dogfighting in space*. Nel 2022 il satellite Shijian-21 ha utilizzato un braccio robotico per spostare un satellite Beidou dismesso verso un'orbita cimitero a 36mila chilometri, dimostrando capacità di cattura fisica in ambiente Geo. Nel 2024 cinque satelliti sperimentali cinesi hanno inoltre eseguito manovre ravvicinate multiple in formazione. La Pla investe anche in sciami di micro-satelliti, sistemi di intelligenza artificiale per operazioni autonome, piattaforme *near-space* e infrastrutture di *quantum key distribution* per comunicazioni resistenti all'intercettazione. La Cina punta inoltre a dispiegare oltre 37mila satelliti tra il 2024 e il 2030. La risposta americana punta sulla resilienza delle costellazioni Leo, come Starlink, che rendono più difficile una degradazione sistemica attraverso colpi singoli. Ma entrambe le superpotenze sono consapevoli di un rischio strutturale: in un ambiente dove gli *asset* sono *dual-use* e l'attribuzione è complessa, il vantaggio del *first strike* incentiva la *preemption*. Per l'Europa, e per l'Italia in particolare, questa evoluzione va oltre la dimensione militare. Le infrastrutture satellitari sostengono telecomunicazioni, sistemi finanziari, catene di approvvigionamento e servizi di navigazione civile. Un conflitto orbitale, anche limitato e combattuto con strumenti non cinetici, produrrebbe effetti immediati e difficilmente controllabili sulle società avanzate.

SYSTEM DESTRUCTION WARFARE

È il cuore della visione cinese del conflitto moderno. Non punta prima di tutto a distruggere singole piattaforme, come un satellite o un missile, ma a colpire i nodi che tengono insieme l'intero sistema operativo dell'avversario. L'obiettivo è provocare una paralisi a cascata, interrompendo comando, comunicazioni, navigazione, allerta e capacità di fuoco. Applicato allo spazio, questo approccio trasforma l'orbita in un punto di pressione sistemica. Colpire pochi *asset* o reti chiave può bastare a degradare funzioni essenziali molto più in basso, fino a incidere direttamente su operazioni militari e infrastrutture civili.

* docente di Intelligence and National security all'Università di Firenze

I mari tornano a essere il vero campo di prova della competizione tra grandi potenze, in una fase che assomiglia sempre più a una nuova Guerra fredda. La potenza navale di domani non riguarderà solo le navi da guerra, ma la capacità di proteggere commercio, infrastrutture e mercati

La Guerra Fredda ora si gioca in mare

BRENT D. SADLER
senior research presso l'Allison Center for National Security

Gli ultimi anni hanno concentrato un'intera vita di lezioni cruciali per i leader nazionali e navali, rilevanti mentre il mondo entra in una nuova Guerra fredda. È un'epoca che contrappone, da un lato società dominate dallo Stato e guidate dalla Cina, e dall'altro le società e i mercati liberi, ancora predominanti, guidati dagli Stati Uniti.

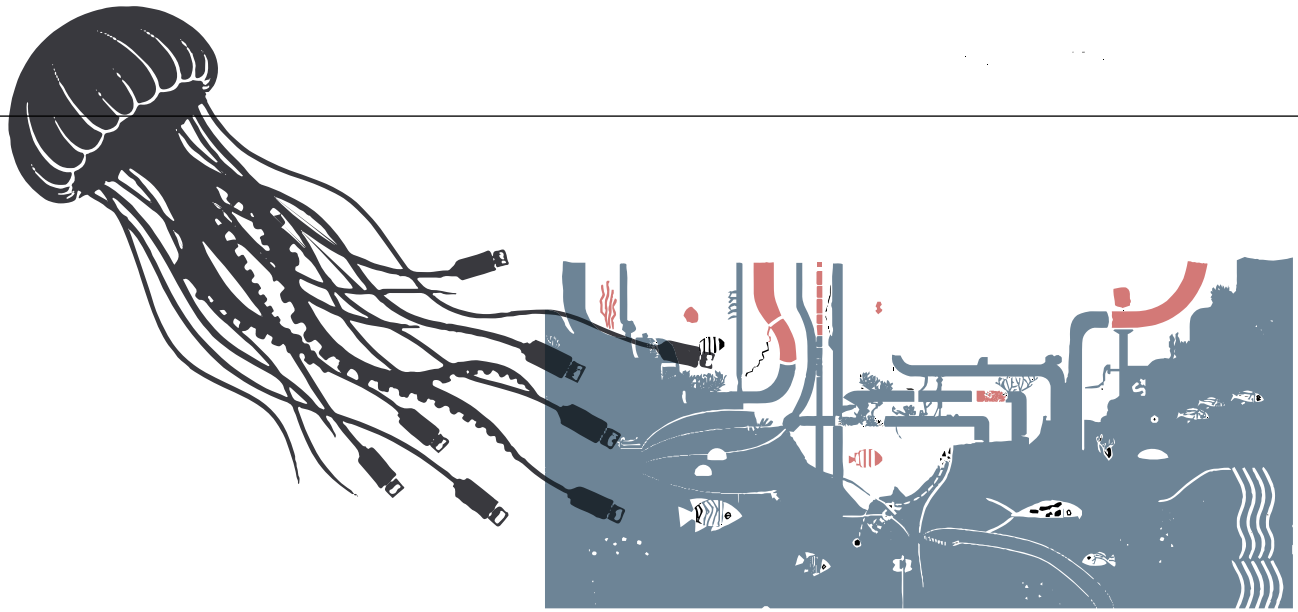
E gli eventi mondiali indicano che il *round* iniziale di questa nuova Guerra fredda si deciderà in mare: attacchi al traffico marittimo internazionale nello stretto di Hormuz e nel mar Rosso, attacchi letali contro trafficanti di narcotici e interdizione delle navi della flotta ombra.

La potenza marittima conta perché rende le economie più resistenti alla coercizione, garantisce all'industria l'accesso alle materie prime e offre la massima flessibilità su dove e come applicare il potere nazionale. Per questo motivo, qualunque potenza dominerà in mare manterrà l'iniziativa e il controllo dei mercati globali: un'osservazione formulata per la prima volta oltre cento anni fa.

Il libro di Alfred Thayer Mahan, *The influence of sea-power on history*, influenzò il primo presidente "navalista" americano, Theodore Roosevelt, nella sua ricerca di una Marina degna del commercio globale della giovane nazione. Il più grande contributo di Mahan fu mostrare la correlazione tra potenza navale, commercio globale e *status* di grande potenza. Una correlazione confermata anche dalle lezioni delle guerre napoleoniche, che posero fine all'impero veneziano, e dalle guerre mondiali, che avviarono il lento declino dell'impero britannico. Nonostante la perdurante rilevanza dell'opera di Mahan, i recenti eventi mondiali rendono chiaro che il mondo sta cambiando, con tecnologie emergenti, dinamiche finanziarie marittime e nuove applicazioni del potere navale.

Nel marzo 2021, la nave portacontainer Ever Given si incagliò nel canale di Suez, bloccandolo per una settimana e causando mesi di perturbazioni al traffico marittimo globale. Fu un promemoria del fatto che il commercio globale è vulnerabile nei principali colli di bottiglia, come dimostrato dall'invasione russa dell'Ucraina nel febbraio 2022, che ha sconvolto le forniture globali di cereali; dagli attacchi degli Houthi contro il traffico marittimo seguiti agli attacchi di Hamas contro

REGISTRI DI BANDIERA DI COMODO Sono registri navali offerti da Stati che consentono a navi e armatori stranieri di battere la loro bandiera con controlli spesso limitati e obblighi meno stringenti. Questo sistema riduce costi e vincoli, ma crea anche opacità su proprietà reale, standard di sicurezza e responsabilità giuridiche. Nel caso delle flotte ombra il problema diventa strategico, perché queste bandiere rendono più difficile attribuire condotte illecite, far rispettare sanzioni o applicare regole marittime condivise. Non è quindi solo una questione amministrativa. È uno dei modi con cui il commercio globale può essere piegato a finalità di elusione e coercizione.



Israele del 7 ottobre 2023; e attualmente dal conflitto con l'Iran, che ha bloccato il traffico navale attraverso lo stretto di Hormuz. Il punto è che la geografia conta, e i *chokepoint* marittimi sono sempre più al centro dell'attenzione e della competizione tra grandi potenze. Con l'aumentare delle tensioni in Asia, aspettatevi di sentire parlare molto di più dello stretto di Malacca, dello stretto di Luzon e dello stretto di Miyako.

Canali e oleodotti costruiti dall'uomo possono mitigare solo fino a un certo punto la tirannia della geografia. L'oleodotto Est-Ovest dell'Arabia Saudita e l'oleodotto degli Emirati Arabi Uniti aggirano i *chokepoint* marittimi, ma sono vulnerabili agli attacchi, rendendo necessari più oleodotti sostenuti dal trasporto marittimo. Un esempio è il gasdotto del "corridoio centrale", che collega il petrolio dell'Asia centrale all'Europa aggirando la Russia e offrendo un'alternativa agli oleodotti esistenti che attraversano la Turchia. Ma anche con questo sforzo, il trasporto marittimo resta essenziale quando gli oleodotti vengono interrotti: il mar Nero è uno spazio marittimo conteso dalla seconda invasione dell'Ucraina da parte di Putin, nel febbraio 2022. Di conseguenza, le Marine saranno sempre più chiamate a proteggere le infrastrutture sottomarine vitali, inclusi i cavi sottomarini per le comunicazioni digitali, che facilitano oltre diecimila miliardi di dollari di scambi commerciali.

L'intelligenza artificiale non è una bacchetta magica, ma svolge un ruolo fondamentale perché consente di usare enormi quantità di dati per individuare e prevedere eventi marittimi-chiave. Questa capacità è essenziale per riconoscere modelli sospetti di comportamento in mare, intercettare le navi della flotta ombra che eludono le sanzioni, interdire i trafficanti illeciti di narcotici e localizzare le navi da guerra nemiche. Perché sia efficace, è necessaria un'ampia copertura di sensori alimentata da una vasta rete di piattaforme senza equipaggio. Le grandi navi da guerra con equipaggio, tuttavia, continueranno a esistere per controllare e sostenere questi sistemi senza equipaggio, imponendo ciò che i leader navali definiscono una "flotta bilanciata".

Quando arriva il momento di ingaggiare le minacce, la capacità di portare l'armamento sul bersaglio è fon-

damentale. È per questo che le portaerei e le navi da guerra con grandi capacità missilistiche continueranno a essere presenti ancora a lungo nel futuro. Questa lezione si è manifestata nei cieli sopra l'Iran e mentre gli Stati Uniti sostengono un blocco punitivo. Inoltre, l'impiego di grandi navi da guerra, come quelle di classe Lewis B. Puller, capaci di imbarcare squadre d'assalto per abbordare e sequestrare in mare le navi della flotta ombra, si è rivelato cruciale in questa nuova era.
Sebbene l'interdizione dei contrabbandieri, il sequestro delle navi della flotta ombra o il controllo dei *chokepoint* siano resi possibili dalla presenza navale, le navi commerciali non salpano senza carico o senza profitto. È qui che entra nell'equazione il costo imposto dagli assicuratori e le forze navali devono diventarne più consapevoli. Nel caso del conflitto con l'Iran, il traffico marittimo neutrale che trasportava la maggior parte delle esportazioni mondiali di petrolio è stato di fatto bloccato senza che una sola nave venisse affondata. La causa principale: i tassi assicurativi di protezione e indennizzo, normalmente pari allo 0,25% del valore di una nave media da 300 milioni di dollari, sono saliti fino a un proibitivo 4%. La lezione è che la fiducia nel passaggio sicuro sarà fondamentale per garantire che i mercati liberi restino resilienti alla coercizione.
Ma la flotta ombra non gioca secondo queste regole, ed è resa possibile da responsabilità difficili da far rispettare da parte dei registri di bandiera: la nazione responsabile di garantire che le navi rispettino i requisiti di sicurezza e ambientali concordati a livello internazionale. La flotta ombra di oggi non è un'aberrazione storica. Nei primi giorni della Seconda guerra mondiale, gran parte del traffico commerciale tedesco era assicurato a Londra (come le flotte commerciali di oggi) e di conseguenza i relativi manifesti di carico e le rotte di navigazione erano noti, rendendo più facile per gli Alleati interdire il traffico nemico fino a quando la Germania non se ne rese conto. Oggi, sistemi automatici di identificazione satellitare, facilmente manipolabili, che trasmettono i dettagli delle navi come richiesto dal diritto internazionale, insieme a registri di bandiera di comodo scarsamente regolamentati, significano che non esistono soluzioni semplici né per far rispettare le moderne regole marittime né per condurre un blocco navale moderno in tempo di guerra.
L'intelligenza artificiale abbinata ai sistemi robotici consente alle macchine di assumere compiti troppo pericolosi, ripetitivi o che richiedono elevati gradi di precisione. Nella guerra navale, le battaglie del mar Nero stanno offrendo uno scorcio di ciò che riserva il futuro: a parte i droni, il conflitto contro gli Houthi nel mar Rosso e contro l'Iran nel Golfo Persico non ha ancora offerto il tipo di insegnamenti forniti dalla guerra in Ucraina.
L'evento decisivo che ha risvegliato i *leader* navali sulla nuova realtà è stato l'affondamento, nell'aprile 2022, dell'ammiraglia russa del mar Nero: l'incrociatore Moskva. Quella nave fu affondata utilizzando dei droni per distrarre l'equipaggio mentre missili da crociera lanciati da terra la colpivano. Quell'evento riguardò meno l'uso dei droni e più l'astuzia degli ucraini, forti della loro esperienza con la tecnologia e le tattiche russe. Ciononostante, aprì gli occhi alle Marine militari (da Pechino a Washington) sul fatto che le navi da guerra moderne possono essere attaccate con successo da terra e che i sistemi senza equipaggio svolgeranno un ruolo-chiave nelle future battaglie navali. Da allora, l'Ucraina ha lanciato una campagna navale pur senza una Marina, affidandosi interamente a piattaforme senza equipaggio per allontanare la Marina russa dalla Crimea, privandola di ogni rifugio nel mar Nero e arrivando persino ad attaccare navi da guerra fino al mar Caspio, da dove i missili da crociera russi Kalibr venivano lanciati contro l'Ucraina.
Quanto alla Marina degli Stati Uniti, nel 2025 essa ha istituito uno squadrone senza equipaggio con base a San Diego, ha dispiegato flottiglie senza equipaggio nel Pacifico e nella primavera del 2021 ha lanciato un missile a lungo raggio da una nave senza equipaggio.
Il futuro è già qui, mentre anche la Cina si è lanciata

ARTE DI GOVERNO NAVALE L'espressione richiama un'idea più ampia della semplice superiorità militare in mare. Significa usare la potenza navale per orientare mercati, proteggere rotte, rassicurare alleati, esercitare pressione economica e sostenere una strategia nazionale su scala globale. In questa visione la Marina non agisce solo quando scoppia una guerra, ma opera continuamente nello spazio intermedio tra deterrenza, presenza e coercizione. È un concetto classico, ma oggi torna centrale perché la competizione tra grandi potenze si gioca sempre più sulla capacità di influenzare i flussi marittimi senza arrivare subito allo scontro aperto.

L'Italia nel radar di Anthropic

Anthropic guarda a Roma in una fase in cui l'intelligenza artificiale non è più solo terreno di innovazione tecnologica, ma anche spazio di legittimazione politica, culturale e regolatoria. La presenza del cofondatore Christopher Olah alla presentazione dell'enciclica di Leone XIV sul rapporto tra persona e IA, seguita dall'arrivo nella capitale del ceo Dario Amodei per incontri con i vertici istituzionali italiani, colloca l'Italia dentro una traiettoria che riguarda insieme etica dell'innovazione, investimenti e posizionamento europeo delle grandi aziende del settore.
Fondata nel 2021 da Dario Amodei, dalla sorella Daniela e da un gruppo di ex ricercatori di OpenAI, Anthropic è diventata una delle principali realtà globali dell'IA generativa con la famiglia di modelli Claude. Nel 2026 la società ha chiuso un *round* di finanziamento da circa 30 miliardi di dollari, raggiungendo una valutazione indicata in circa 380 miliardi, mentre continua a espandersi con il sostegno di partner come Amazon e Google e di grandi investitori internazionali. Il gruppo sta rafforzando in particolare le applicazioni professionali, il *coding* e l'automazione, dentro una strategia che combina modelli, infrastrutture cloud e capacità di calcolo.
La tappa italiana arriva mentre Anthropic amplia la propria presenza europea. La società ha aperto uffici a Parigi e Monaco, aggiungendoli alle sedi già attive a Londra, Dublino e Zurigo, e ha registrato una forte crescita nell'area Emea sia in termini di ricavi sia nel numero dei grandi clienti aziendali. Sullo sfondo c'è anche la ricerca di accordi per nuovi *data center* in Europa, con attenzione al Sud del continente. In questo quadro l'Italia può rappresentare non solo un mercato, ma anche un punto di accesso a un ecosistema istituzionale e industriale rilevante per la prossima fase di espansione.
Il nodo centrale è però anche simbolico. Anthropic ha costruito parte della propria identità pubblica sul tema dell'IA orientata a criteri etici, una linea che negli Stati Uniti l'ha portata a uno scontro con il Pentagono sulle salvaguardie incorporate nei modelli. Il dialogo con il Vaticano e con Roma si inserisce così in una strategia che punta a rafforzare il profilo della società in Europa, dove il rapporto tra innovazione, regole e consenso pubblico resta particolarmente sensibile. L'eventuale approdo italiano andrebbe letto dentro questa doppia chiave, industriale e culturale, con Roma come luogo di incontro tra investimenti, regolazione e legittimazione del nuovo potere tecnologico.
•

in una corsa frenetica per perfezionare la propria flotta di piattaforme navali senza equipaggio, le quali talvolta finiscono sulle coste dei Paesi vicini, come un drone sottomarino cinese ritrovato nell'aprile 2026 su una spiaggia indonesiana. Ma, a differenza del combattimento ravvicinato di trincea in Ucraina, i sistemi navali senza equipaggio dovranno eccellere in operazioni autonome su grandi distanze e per lunghi periodi.
La necessità dell'Ucraina di condurre attacchi a distanza, come quello contro Novorossiysk mediante sciami di droni, e i progressi nella guerra elettronica stanno accelerando lo sviluppo di sistemi pienamente autonomi. Entrambe le parti in questa guerra hanno cercato di superare le interferenze di segnale usando inizialmente cavi in fibra ottica per controllare i droni sulla linea del fronte. Ma ciò presenta limitazioni inaccettabili, portando entrambe le parti a impiegare sempre più droni con un grado di autonomia più elevato.
Per le nazioni americane e della Nato, le forze navali devono confrontarsi con una gamma di minacce operando una flotta bilanciata su grandi distanze. Questo spingerà le Marine militari ad adottare sistemi senza equipaggio capaci di dispiegamenti a lungo raggio e dotati di un alto grado di autonomia, capaci di funzionare in un moderno ambiente conteso dal punto di vista dei segnali.
La nuova guerra Fredda non sarà una ripetizione di quella precedente, che si aprì con eserciti schierati l'uno di fronte all'altro attraverso il varco di Fulda. È già qui e si è aperta con una competizione per i mercati e per l'influenza sui mari. I successi esitanti dell'America in Venezuela e in Iran potrebbero essere il presagio di una nuova arte di governo navale americana. Ciò ha esposto la vulnerabilità della Cina e la sua dipendenza dalle navi della flotta ombra, prefigurando una risposta che utilizzi la sua notevole leva nel trasporto marittimo commerciale e il controllo di oltre cento porti strategici in tutto il mondo.

Non è la prima volta che la rivalità tra Iran e occidente si impernia sul passaggio attraverso lo stretto di Hormuz. Dal 1979, Teheran è ricorsa più volte a questa strategia, trasformando un collo di bottiglia energetico in una leva geopolitica. Il segreto non è bloccare completamente il passaggio, ma rendere l'attraversamento rischioso ai limiti dell'accettabile

Chiudere un chokepoint, *istruzioni per l'uso*

FERDINANDO SANFELICE DI MONTEFORTE
ammiraglio e docente di studi strategici

Dall'ormai lontano 1979, da quando l'Iran ha assunto una posizione antiamericana, e in generale antioccidentale, il traffico mercantile che attraversa lo stretto di Hormuz è diventato ostaggio dei periodici ricatti del governo di Teheran, tesi a far recedere l'occidente da pressioni considerate inaccettabili.
Lo stretto, in effetti, per le sue caratteristiche, si presta bene a questo genere di azioni da parte degli Stati litoranei, quando essi vogliono interdire il traffico in zona. Interrompere il traffico mercantile è facile, vista la notevole lunghezza dello Stretto, pari a 104 miglia nautiche (167 chilometri); in particolare la sua ampiezza minima è di 21 miglia nautiche (32 chilometri), proprio in corrispondenza del porto militare iraniano di Bandar Abbas e dell'isola di Qeshm, che gli è di fronte, e viene sfruttata come bastione avanzato. Alle forze iraniane, quindi, basta affacciarsi fuori dal porto per colpire le navi di passaggio. La presenza di altre piccole isole prossime alla costa iraniana, cui si aggiunge l'esistenza di scogli e di bassi fondali, costringe le navi a seguire percorsi fissi, seguendo lo schema di separazione del traffico, una situazione che aumenta la vulnerabilità di chi attraversa lo stretto.
In teoria, anche i Paesi della sponda meridionale dello stretto (gli Emirati Arabi Uniti e l'Oman) potrebbero colpire il traffico mercantile di passaggio, ma i loro interessi economici sono tutti in favore del libero transito del commercio attraverso questo braccio di mare. L'Iran, quindi, è l'unico Paese che costituisce una minaccia immanente per il traffico marittimo.
L'interesse dei Paesi occidentali sul flusso di oro nero in uscita dal Golfo è notevole, anche se non altissimo, visto che il 15% del loro fabbisogno energetico proviene proprio da quest'area.
Non bisogna però dimenticare che Hormuz è l'unica via d'uscita (e d'ingresso) per il traffico marittimo tra i Paesi del golfo Persico e il resto del mondo. Ogni volta che viene chiuso, infatti, le nazioni litoranee non


27°
26°
25°
54°
55°
56°
57°

riescono più a esportare i loro prodotti, principalmente idrocarburi, il cui ammontare medio è di 20 milioni di barili l'anno, senza contare il gas.
I disagi per i Paesi litoranei, oltretutto, non si limitano al blocco delle esportazioni di petrolio: la chiusura dello stretto li priva di derrate alimentari, importate in quantità rilevante dato che la terra, in questi Paesi, non riesce a sfamare la sempre più numerosa popolazione. Viene poi il rischio di non essere più riforniti degli altri beni che sostengono lo sviluppo dell'area e assicurano il livello di benessere degli abitanti.
Non è la prima volta che queste chiusure, da parte dell'Iran, si verificano: basti ricordare che, durante la cosiddetta Guerra delle petroliere, nel 1988, mentre l'Iraq attaccò le navi che imbarcavano il petrolio iraniano nel terminale dell'isola di Kharg, nel nord del Golfo, l'Iran decise di premere sugli occidentali affinché imponessero al governo di Baghdad di cessare le ostilità, e per questo bloccò lo stretto di Hormuz.
A tal fine, i Pasdaran e le Forze armate iraniane si dotarono di piccole e veloci imbarcazioni, che non solo servivano per abbordare o colpire con armi leggere le petroliere, ma anche per posare mine lungo le rotte dello stretto. A questi mezzi, di costo limitato e quindi disponibili in grandi numeri, si aggiunsero i missili costieri antinave Silkworm, forniti dalla Cina, e posizionati lungo la costa, spesso in postazioni mobili e quindi difficilmente contrastabili.
Nel 1988 il numero di petroliere attaccate nel golfo Persico durante la guerra tra l'Iraq e l'Iran aveva raggiunto un livello preoccupante: al nord, l'Iraq aveva attaccato 283 navi, mentre a sud l'Iran ne aveva attaccate 168. Il governo di Washington decise allora di scortare le petroliere che battevano bandiera Usa, ottenendo il rientro sotto la propria giurisdizione di molte loro navi che avevano utilizzato bandiere-ombra fino a quel momento.
Il 14 aprile 1988, però, la Uss Samuel B. Roberts, mentre operava nel Golfo, urtò una mina e subì gravi danni. Per ritorsione, a Washington fu decisa l'operazione Praying Mantis, che il 18 aprile successivo portò alla distruzione di gran parte delle unità navali iraniane. In quegli anni, nel frattempo, la Us Navy aveva mantenuto nel punto più stretto di Hormuz una corazzata della classe Iowa, la cui protezione la rendeva invulnerabile ai missili Silkworm iraniani, e la cui presenza costituiva un deterrente efficace per evitare attacchi nella zona.
Quando però, per risparmiare sui costi di esercizio, la Us Navy decise di sostituirla con un incrociatore, e inviò lo Uss Vincennes, questa unità abbatté per errore un aereo di linea, causando la morte di 290 persone, tra passeggeri ed equipaggio.
Dopo la fine della guerra tra l'Iraq e l'Iran non ci furono più attacchi contro il traffico mercantile che transitava per Hormuz fino al 4 luglio 2019, quando i Pasdaran ripresero le azioni di disturbo contro i mercantili, per rappresaglia contro il sequestro a Gibilterra della petroliera iraniana Grace 1, con l'accusa di aver violato le sanzioni internazionali imposte alla Siria di Assad.
Per far cessare questi attacchi, l'Europa inviò navi da guerra dei Paesi membri, attivando l'operazione Emasoh/Agénor, il 20 gennaio 2020, ma nel 2024, visto che erano da tempo cessati gli attacchi da parte dei Pasdaran, la missione fu quietamente fatta scomparire, in modo da consentire ai Paesi membri di dirottare le navi per fronteggiare la minaccia posta dagli Houthi nello stretto di Bab-el-Mandeb.
Dal 28 febbraio 2026, in conseguenza dell'attacco americano e israeliano all'Iran, accusato di voler produrre armi atomiche, siamo di nuovo di fronte alla chiusura dello stretto. La differenza rispetto al 1988, però, è che in tutti questi anni l'Iran ha fortificato l'isola di Qeshm e creato postazioni protette lungo la

OPERATION PRAYING MANTIS Fu la vasta operazione navale lanciata dagli Stati Uniti il 18 aprile 1988 dopo che la fregata Uss Samuel B. Roberts aveva urtato una mina iraniana nel Golfo. Non fu una semplice rappresaglia simbolica, ma una dimostrazione di forza costruita per colpire piattaforme petrolifere usate a fini militari e unità navali iraniane, ristabilendo deterrenza e libertà di navigazione. Il suo peso storico sta qui. Mostrò che la guerra delle petroliere poteva rapidamente trasformarsi in uno scontro diretto tra Iran e Us Navy, con effetti strategici ben oltre il singolo incidente che l'aveva innescata.

costa dello stretto. Anche se l'ammiraglio Brad Cooper, a capo del Centcom (Comando centrale Usa), ha riferito che le forze Usa, nel corso dell'operazione Epic Fury hanno eliminato "oltre il 90% di quello che era un imponente arsenale di mine navali fatto di oltre ottomila ordigni, attraverso oltre 700 attacchi aerei mirati", numerose mine sono state posate nelle acque dello stretto, missili e droni sono ancora usati e gli attacchi, a mezzo di piccole imbarcazioni continuano. Questa maggiore resilienza ai bombardamenti Usa contro le forze iraniane nello stretto ha indotto il governo di Washington a decretare un "contro blocco", per impedire alle petroliere cariche di idrocarburi iraniani di uscire dal Golfo, mentre quelle che interessano all'occidente, circa un migliaio, sono bloccate agli ingressi dello stretto.
Le conseguenze di questa situazione, per i nostri Paesi, sono purtroppo ben visibili anche al comune cittadino, e i tentativi da parte della diplomazia internazionale di trovare un *modus vivendi* si moltiplicano. La realtà è che gli Usa sono pressati dai Paesi arabi del Golfo affinché costringano Teheran a rinunciare alle armi nucleari, mentre il governo iraniano ritiene il possesso di queste ultime una essenziale garanzia di sicurezza. Rimane poi il problema della disponibilità di capacità (navi, armi e mezzi) in grado di contrastare la moltitudine di piccole imbarcazioni, pilotate o radioguidate, appoggiate da droni, che costituiscono una minaccia per il traffico che attraversa i passaggi obbligati, in inglese *chokepoint*.
Per liberare, infine, le acque dello stretto dalle mine che sono state posate, più o meno a casaccio, da parte dei barchini dei Pasdaran sono necessarie le unità specialistiche, note come cacciamine. A tal proposito, è stata chiamata in causa pure la nostra Marina, che nel 1991 inviò questo tipo di mezzi per eliminare gli ordigni subacquei ancora esistenti nelle acque del golfo Persico, e lo fecero in modo egregio; due nostre unità sono appunto partite in questi giorni per Gibuti, in modo da essere pronte a ripetere l'operazione di sminamento, qualora le circostanze lo permetteranno.
Non va dimenticato, però, che nessuna Marina al mondo dispone di capacità di sminamento in un teatro di guerra, in pieno combattimento, che siano realmente efficaci. Il raggiungimento di un armistizio è quindi indispensabile, per consentire alle nostre unità cacciamine di poter operare.
Quanto durerà questa situazione? Non si possono fare previsioni. Solo l'Italia, che ha mantenuto rapporti cortesi, se non cordiali, con la dirigenza di Teheran è in grado di agire, come nel passato, facendo da ponte tra le parti e aiutarle a raggiungere un compromesso sia pur parziale, che consenta la ripresa dei traffici attraverso lo stretto.

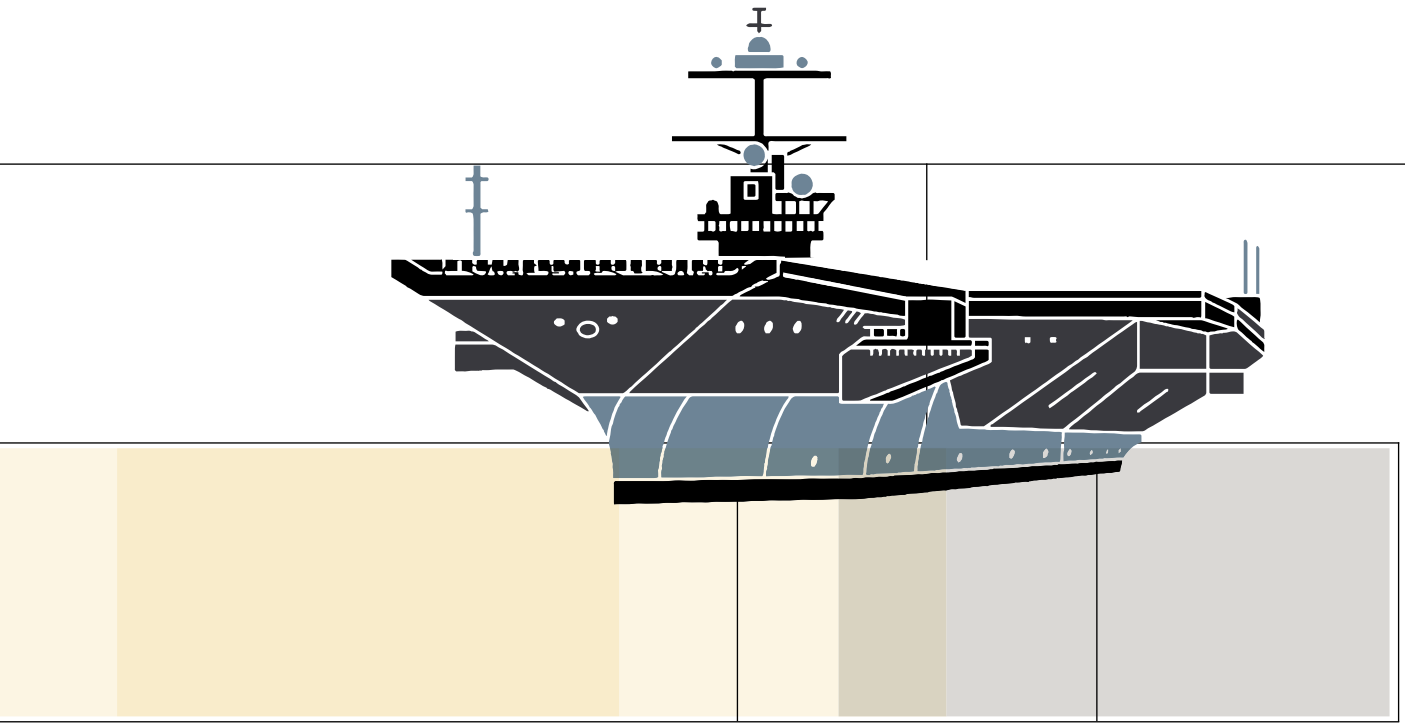
L'industria cantieristica italiana si conferma un modello osservato con interesse anche negli Stati Uniti, dove il rilancio della produzione navale spinge a guardare alle esperienze degli alleati. Al centro c'è la capacità di unire forza commerciale, innovazione di processo e tecnologie avanzate, dalla prefabbricazione ai gemelli digitali, fino alla robotica

Perché gli Usa guardano al modello italiano nella cantieristica

JAMES GORDON FOGGO III
ammiraglio e già comandante dell'Allied joint forces command a Napoli

Mentre gli Stati Uniti rinnovano il proprio interesse e i propri investimenti nella cantieristica commerciale e militare, è utile esaminare le migliori pratiche industriali dei nostri alleati e *partner*. Il Center for maritime strategy di Washington ha recentemente completato uno studio completo su cinque Paesi diversi, intitolato *Pier review: leveraging the allied maritime industrial base for Us shipbuilding*. Questo articolo riassume i risultati dello studio relativi alla notevole innovazione guidata dalla base industriale marittima italiana. In quanto nazione costiera, i governi italiani che si sono succeduti hanno ritenuto nel proprio interesse investire nella base industriale marittima. Questi investimenti hanno dato frutti in termini di rafforzamento della sicurezza nazionale e del Pil. Nel 2024-2025, l'Italia ha dispiegato la Cavour nel Pacifico occidentale in solidarietà con alleati e partner contro l'aggressività cinese nel mar Cinese meridionale e nello stretto di Taiwan, operando con successo per sei mesi in un teatro estero senza una base di supporto significativa. Questo dispiegamento ha dimostrato le capacità della Marina italiana e la sua abilità di estendere il proprio raggio d'azione ben oltre il continente europeo. Nulla di tutto ciò sarebbe stato possibile senza una solida base industriale marittima e senza la sinergia creata tra cantieristica commerciale e militare. L'industria cantieristica italiana rimane una forza economica significativa in Italia, con un orientamento all'*export* valutato in 9,1 miliardi di euro. Il successo italiano nella cantieristica navale è dovuto a una varietà di fattori, tra cui una popolazione istruita, un'abbondante forza-lavoro, una base industriale avanzata e capacità manifatturiere marine allo stato dell'arte, oltre a una diversità di infrastrutture portuali e cantieri navali distribuiti nel Paese, capaci di produrre navi da guerra sofisticate; il settore della cantieristica civile offre tuttavia un modello di *business* più redditizio per la base industriale marittima. Nel 2022, infatti, l'Italia ha fornito il 36% delle navi da crociera mondiali. Sebbene l'Italia sia anche il maggiore esportatore mondiale di *superyacht*, con oltre il 19% della quota globale, è altresì in grado di produrre petroliere, portarinfuse, navi cargo, unità di supporto *offshore* e navi *roll-on/roll-off* (RoRo). Il fiore all'occhiello italiano per la produzione di navi di lusso è il cantiere Fincantieri di Monfalcone, sulla

SMART SHIPYARD L'espressione indica un cantiere navale trasformato in ambiente produttivo digitale, dove progettazione, logistica, lavorazioni e controllo qualità vengono collegati in tempo reale. Non si tratta solo di usare più robot, ma di far dialogare sensori, *software*, gemelli digitali e linee automatizzate dentro un unico processo continuo. Il vantaggio è doppio. Da un lato si riducono tempi morti, errori e rilavorazioni. Dall'altro si crea un sistema industriale più capace di assorbire complessità crescente, che è poi la vera sfida quando si passa da una nave commerciale standard a piattaforme molto sofisticate.



costa adriatica. Durante la conduzione dello studio *Pier review*, ho avuto l'opportunità di visitare Monfalcone, dove ho maturato un notevole apprezzamento per l'autonomia e la digitalizzazione lungo la linea di produzione. Fincantieri promuove l'innovazione nella base industriale marittima attraverso un approccio in quattro parti che comprende antenne dell'innovazione, sollecitazione di *start up*, competizione interna e un istituto di ricerca nazionale. Fincantieri sta attualmente trasformando Monfalcone in uno *smart shipyard* allo stato dell'arte per il XXI secolo, con un piano di sviluppo quinquennale (2026-2030) e investimenti complessivi pari a 1,9 miliardi di euro nei propri stabilimenti. Questi aggiornamenti si concentrano sull'industrializzazione intelligente a supporto dei gemelli digitali, automatizzando attività altamente complesse e ripetitive normalmente svolte da esseri umani. La linea di produzione del cantiere di Monfalcone impiega una varietà di capacità robotiche industriali; gemellaggio digitale; tracciamento logistico in tempo reale; intelligenza artificiale e realtà aumentata e manifattura additiva. Per esempio, droni autonomi vengono integrati per un monitoraggio strutturale rapido e non invasivo e per il controllo qualità, alimentando dati in tempo reale nel gemello digitale per la manutenzione predittiva. Ho osservato diversi sistemi di saldatura robotica o cobotica nel cantiere di Monfalcone. Il cantiere sta installando linee di saldatura laser e di lavorazione dei profili allo stato dell'arte, inclusa tecnologia Pema, per gestire la maggiore precisione richiesta dalle mega-navi oltre le 200mila tonnellate. Inoltre, in collaborazione con Comau, il cantiere ha introdotto il robot mobile per la saldatura (MR4Weld), un sistema indipendente che utilizza *software* di visione integrato per localizzare e saldare giunti in acciaio. I robot mobili per la saldatura promuovono opportunità di *upskilling* per i lavoratori, offrendo al contempo una risposta proattiva alla carenza globale di professionisti della saldatura. Questo sistema può essere utilizzato in prossimità di saldatori umani impegnati in altre attività, ed è valutato in grado di migliorare la produttività di un fattore pari a tre. Nel complesso, i robot mobili per la saldatura offrono risparmi significativi in termini di tempo e costi rispetto ai processi manuali. Robot umanoidi, capaci di svolgere una serie di compiti mentre si muovono

nell'ambiente complesso e ingombro del cantiere navale, sono attualmente in fase di test a Monfalcone. Uno dei vantaggi dei robot umanoidi è la loro intelligenza e capacità di muoversi e svolgere servizi di saldatura in modo sicuro ed efficace all'interno di uno scafo dopo il posizionamento di moduli o componenti. Sebbene robot e cobot siano ormai una componente importante della fase di prefabbricazione, l'impiego di robot umanoidi all'interno dello scafo rappresenta un cambiamento potenzialmente dirompente, che potrebbe contribuire "alla sostenibilità a lungo termine di attività altamente intensive e specializzate". Il cantiere Fincantieri di Monfalcone utilizza gemelli digitali per creare repliche virtuali, basate sui dati, delle navi da crociera, integrando Internet delle cose, modellazione 3D e IA per ottimizzare la costruzione dalla progettazione fino alla produzione. Questa tecnologia consente il monitoraggio in tempo reale della costruzione, la simulazione dell'assemblaggio e analisi predittive per migliorare l'efficienza, ridurre i rischi e garantire che la nave *as-built* corrisponda al progetto digitale. I gemelli digitali vengono avviati nella fase di progettazione, creando modelli 3D ad alta fedeltà che evolvono in basi di riferimento *as-built*, consentendo un assemblaggio rapido e accurato. Il cantiere simula i processi produttivi, utilizzando IA e modelli digitali per rilevare tempestivamente le interruzioni e ripianificare, riducendo i tempi di attraversamento e aumentando l'efficienza. Sensori su attrezzature e materiali alimentano dati in tempo reale nel gemello digitale, monitorando l'avanzamento della costruzione, le scorte di materiali, per esempio le lamiere d'acciaio, e l'utilizzo delle risorse. I gemelli digitali prevedono potenziali problemi strutturali o guasti delle apparecchiature durante la fase di costruzione, facilitando la manutenzione proattiva e garantendo standard qualitativi elevati. I modelli virtuali aiutano a pianificare il complesso e avanzato allestimento di cabine e macchinari prima dell'installazione fisica, migliorando la sicurezza e riducendo il lavoro in sito. Fincantieri utilizza modelli 3D per creare controparti virtuali delle navi, consentendo a progettisti e ingegneri di simulare scenari operativi, verificare le scelte progettuali e ottimizzare il prodotto finale prima dell'inizio della costruzione fisica. Attraverso il programma Fincantieri for the Digital future, i costruttori navali possono indossare caschi Vr/Ar, realtà virtuale e realtà aumentata, per valutare l'accuratezza nell'allestimento navale di un compartimento, fornendo competenze in un ambiente sicuro e simulato. Abbracciando il miglioramento dei processi, Fincantieri ha raggiunto un'efficienza straordinaria investendo nella prefabbricazione dei moduli nel processo di progettazione-costruzione. Monfalcone sta attualmente producendo moduli da 15 tonnellate metriche, pronti per l'installazione, nel processo di produzione modulare in bacino di carenaggio. Non solo questi moduli sono già equipaggiati con tubazioni e sistemi elettrici pronti per essere integrati con il resto dello scafo, ma sono anche verniciati o rivestiti a polvere, rendendo questo l'unico cantiere osservato dal Cms che completa tale processo prima dell'integrazione. Fincantieri stima di aver ridotto le ore di produzione della manodopera di un fattore pari a cinque completando la maggior parte del lavoro sui moduli, inclusa la verniciatura finale, prima della consegna del modulo al bacino di carenaggio per il posizionamento, la saldatura e l'assemblaggio, compreso il posizionamento dei moduli del ponte con parabrezza e gruppi tergicristallo completamente integrati. Di conseguenza, sia l'Italia sia Fincantieri offrono una presenza significativa per nuove costruzioni di navi da guerra, rompighiaccio o unità ausiliarie, nonché la capacità di modernizzare e riparare navi più anziane presenti in inventario. Fincantieri ha inoltre ampliato le proprie operazioni oltre i confini italiani. Gestisce quattro cantieri navali negli Stati Uniti, tra cui tre con sede in Wisconsin focalizzati sulla costruzione e riparazione navale — Fincantieri Marinette Marine, Fincantieri Bay Shipbuilding e Fincantieri Ace Marine — e una struttura di riparazione con sede a Jacksonville, in Florida, Fincantieri Marine Repair. La società possiede inoltre tre cantieri navali norvegesi, due cantieri rumeni e uno in Brasile e Vietnam. Queste acquisizioni hanno contribuito ad ampliare la portata dell'industria cantieristica italiana e a sostenere la penetrazione di Fincantieri in mercati globali diversificati. L'emergere di queste aree di concentrazione

COBOTICA Il termine unisce collaborazione e robotica e descrive sistemi pensati per lavorare accanto agli esseri umani, non in uno spazio separato e recintato come avveniva nella robotica industriale classica. In un cantiere navale questo cambia molto, perché permette di automatizzare attività pesanti o ripetitive senza espellere il lavoro umano dal processo, ma spostandolo verso supervisione, programmazione e controllo. La cobotica è quindi anche una risposta alla scarsità di manodopera specializzata. Più che sostituire il saldatore, ne trasforma il ruolo e rende il cantiere meno dipendente da competenze sempre più difficili da reperire.

Crosetto fa il punto sui dossier aperti

A margine della presentazione della nuova piattaforma digitale della Difesa, Guido Crosetto ha indicato alcune delle principali priorità del dicastero, tra crisi internazionali, missioni militari e le scelte legate al tema delle spese militari. Il quadro che emerge è quello di un'amministrazione chiamata a muoversi su piani diversi, dalla gestione operativa dei teatri più sensibili fino alle decisioni politiche e finanziarie necessarie a sostenere gli impegni italiani.
Sul fronte del Golfo, il ministro ha confermato la disponibilità dell'Italia a far avvicinare i cacciamine della Marina allo stretto di Hormuz, precisando però che il loro eventuale impiego dipenderà dalle condizioni di sicurezza e dal contesto diplomatico internazionale. Le unità sarebbero già pronte a muoversi dalla Sicilia, ma non sono navi concepite per operare in un contesto di guerra senza un adeguato supporto. Per questo, ha spiegato il ministro, sarebbe necessario affiancarle con una nave di sostegno logistico e una adibita alla protezione attiva. Nella lettura del ministro, uno dei passaggi più rilevanti per capire l'evoluzione della crisi resta il confronto tra Stati Uniti e Cina, considerate le due potenze più in grado di incidere sugli equilibri internazionali, nonché le più suscettibili di subire le ricadute economiche di una destabilizzazione prolungata dell'area e dei traffici commerciali.
Crosetto si è soffermato anche sul Libano e sul futuro della missione Onu Unifil, rimarcando come il quadro attuale sia profondamente diverso da quello in cui la missione era stata impostata originariamente. L'Italia, garantisce Crosetto, intende mantenere un ruolo centrale e sta lavorando a una proposta da presentare alle Nazioni Unite, pur nella consapevolezza che il percorso politico resta complesso. Nell'ipotesi delineata dal ministro, un eventuale riequilibrio della presenza internazionale dovrebbe coinvolgere anche Paesi *extra*-europei, comprese le nazioni islamiche, per tenere conto della composizione politica, religiosa e sociale del contesto libanese. Dietro questa impostazione c'è anche una valutazione più ampia sulla stabilità del Mediterraneo e sulle possibili conseguenze regionali di una crisi non contenuta.
L'ultimo nodo riguarda le risorse europee e in particolare il programma Safe, sul quale una decisione da parte del Mef sarebbe attesa entro la fine del mese. Crosetto ha spiegato di non considerare difesa ed energia come priorità in competizione, ma ha ricordato che la scelta finale spetta al ministero dell'Economia, compatibilmente con i vincoli fiscali e di bilancio del Paese.
•

della base industriale marittima ha contribuito a creare un ecosistema che comprende istituzioni accademiche di eccellenza, industria e infrastrutture di supporto, tutti elementi a beneficio del Pil italiano. Inoltre, la distribuzione diversificata delle strutture di manutenzione e dei bacini di carenaggio di Fincantieri potrebbe consentire all'Italia di svolgere un ruolo più ampio nel supportare la manutenzione e la riparazione di navi americane che altrimenti dovrebbero rientrare negli Stati Uniti, in particolare quelle operanti nei teatri europeo o mediorientale. L'industria cantieristica italiana è certamente diventata un *leader* globale nella produzione commerciale di navi da crociera, il che consente al suo principale costruttore di navi da guerra di rimanere commercialmente sostenibile e di superare gli alti e bassi finanziari di un mercato volatile.

Adottando un'automazione di livello mondiale e un approccio alla cantieristica orientato ai processi, Fincantieri ha tracciato un modello per il dominio commerciale, sviluppando al contempo molti processi che potrebbero rivelarsi applicabili allo sviluppo di navi militari. La disponibilità di Fincantieri a specializzarsi nella propria cantieristica commerciale concentrandosi sulle navi da crociera presenta un percorso convincente per gli Stati Uniti e per altre nazioni marittime che intendono ritagliarsi una nicchia nel mercato commerciale. La capacità dell'Italia di identificare e valorizzare i propri punti di forza nella progettazione navale ha consentito ad aziende come Fincantieri di concentrare la propria ricerca e sviluppo sul perfezionamento dei processi cantieristici e sull'individuazione di modi innovativi per incorporare tecnologie dirompenti e progettare e costruire le proprie navi.

La Royal Navy prova a ripensarsi come forza ibrida, combinando piattaforme tradizionali, sistemi senza equipaggio e capacità autonome per rispondere a minacce più rapide e a risorse sempre più limitate. La visione lanciata da Londra punta a rilanciare il ruolo britannico nell'Atlantico e nella Nato, ma resta appesa a un nodo decisivo, cioè la capacità di tradurre ambizione e innovazione in numeri, tempi e strumenti davvero sostenibili

La flotta ibrida è la nuova sfida della Royal navy

NICK CHILDS
senior fellow for Naval forces and maritime security presso il IISS

Il Regno Unito potrebbe trovarsi di fronte a un punto di svolta nella propria traiettoria come potenza navale. Alla recente International sea power conference di Londra, il capo professionale della Royal navy (Rn) britannica, il Primo Lord del mare generale Sir Gwyn Jenkins, ha lanciato un appello all'industria e ad altri *stakeholder* affinché contribuiscano a trasformare la Rn in una forza ibrida composta da piattaforme e sistemi avanzati con equipaggio, senza equipaggio e autonomi. Ma determinare come sarà questa flotta ibrida, e come verranno bilanciate queste diverse capacità, sarà fondamentale per il successo della visione del generale Jenkins. E, sotto questo profilo, permangono interrogativi e incertezze significativi.

La maggior parte delle principali marine occidentali è alle prese con la crescente consapevolezza di avere bisogno di una correzione di rotta per affrontare le minacce emergenti in mare e l'accelerazione del ritmo del cambiamento tecnologico. Le lezioni operative del mar Nero e dello stretto di Bab el-Mandeb, i persistenti vincoli di risorse, nonostante alcuni aumenti di bilancio promessi, le strozzature sul personale e i problemi di capacità industriale fanno sì che una semplice ricostituzione delle capacità navali in senso tradizionale non sia un'opzione. D'ora in poi, le marine dovranno fare le cose in modo diverso.

Anche il Primo Lord del mare ha sottolineato l'urgenza di cambiare rotta e il fatto di essere impegnato in una missione quadriennale per fornire entro il 2029 una rinnovata capacità di combattimento, nota come Warfighting ready plan 2029. Questo senso di urgenza, ancora una volta, è un tema comune tra i membri della Nato.

Gli obiettivi-chiave per la Rn sono una rinnovata capacità nell'Atlantico e nell'Europa settentrionale, in linea con la priorità attribuita dal governo britannico agli impegni Nato. Il concetto di "Atlantic bastion" prevede nuove piattaforme con equipaggio di fascia alta, come la fregata Type-26 e il velivolo da pattugliamento marittimo P-8A Poseidon, integrate con nuove reti di sensori remoti, veicoli senza equipaggio e autonomi, e trattamento dei dati assistito dall'IA per affrontare una

ATLANTIC BASTION Non è un semplice *slogan* operativo, ma l'idea di trasformare l'Atlantico settentrionale in uno spazio di sorveglianza e deterrenza continua contro la rinnovata minaccia russa, soprattutto subacquea. La formula implica che navi di fascia alta, pattugliatori marittimi, sensori remoti e sistemi senza equipaggio lavorino come una rete unica, capace di vedere prima, classificare meglio e reagire più in fretta. Il punto decisivo è che la superiorità non dipende più solo dal numero di scafi in mare, ma dalla densità informativa dell'intero sistema.

Type-26

Type-45

HMS Lancaster

rinnovata minaccia russa di superficie e subacquea. A ciò si affiancherà "Atlantic shield", il futuro contributo della marina alla difesa aerea e missilistica integrata del Regno Unito e dell'Europa settentrionale, che incorporerà nuove piattaforme missilistiche senza equipaggio. Infine, vi sarà "Atlantic strike", che comporterà una capacità d'attacco ibrida basata su portaerei e una forza anfibia trasformata. Il generale Jenkins prevede la presenza, già l'anno prossimo, di un dimostratore di *jet* veloce senza equipaggio a bordo di una portaerei.
Sebbene altre flotte alleate affrontino sfide simili a quelle della Rn, queste pressioni sono, per certi versi, più acute per la Rn. La sua flotta ereditata dal passato è stata ridotta a minimi storici. Sotto il peso di costi di manutenzione galoppanti e carenze di equipaggi, unità navali obsolete vengono ritirate prima che i loro sostituti siano pronti. Vari nodi legati a sottoinvestimenti – in particolare nella costruzione di nuove navi da guerra – sono arrivati al pettine proprio nel momento peggiore. Il recente ritiro, senza sostituzione immediata, della fregata dispiegata in Medio Oriente, Hms Lancaster, ha evidenziato quanto la Rn sia attualmente sotto pressione. Anche il numero di fregate Rn in servizio è stato ridotto ad appena sette e il totale delle unità di scorta, inclusi i problematici cacciatorpediniere Type-45, ad appena 13.
Sebbene vi sia una *pipeline* di nuove navi in costruzione, aumentarla nel breve periodo non è un'opzione. Di conseguenza, adottare e introdurre rapidamente nuove tecnologie potrebbe essere l'unico approccio realistico, insieme al ricorso agli alleati per contribuire a colmare le lacune attuali. Una maggiore integrazione con gli alleati e l'incorporazione di nuove tecnologie sono inoltre chiaramente fondamentali per ristabilire una massa efficace e fornire vantaggio operativo in futuro.
Le piattaforme convenzionali con equipaggio potrebbero essere ancora considerate dalla Rn un elemento centrale nell'equilibrio della nuova flotta, non da ultimo come navi madre per molti dei nuovi sistemi senza equipaggio e autonomi, ma in quali numeri e con quale livello di capacità non è del tutto chiaro. Eppure, nel lungo periodo, sembra certo che continueranno a essere

Usa e Cuba, cresce la pressione nei Caraibi

L'arrivo della Uss Nimitz nelle acque caraibiche antistanti Cuba riporta al centro una domanda che a Washington circola da tempo. Gli Stati Uniti stanno preparando una nuova stretta contro l'Avana sul modello di quanto avvenuto in Venezuela. Il contesto è quello di un'isola travolta da una crisi energetica sempre più grave, mentre la Casa Bianca intensifica pressione politica, giudiziaria e militare contro il regime cubano.
Il precedente pesa. Tra agosto 2025 e gennaio 2026 gli Stati Uniti avevano costruito nei Caraibi un dispositivo militare attorno al Venezuela, culminato con l'operazione Absolute resolve e con la cattura di Nicolás Maduro. Alla rimozione del presidente era seguita una ridefinizione completa dei rapporti tra Washington e Caracas. Da allora il caso cubano è apparso sempre più come il possibile capitolo successivo della strategia americana nell'emisfero occidentale.
La crisi dell'isola si è aggravata proprio dopo la caduta di Maduro. Fino a gennaio il Venezuela copriva circa il 20% delle importazioni energetiche cubane, pari a 26.500 barili al giorno. Con il cambio di regime quel flusso si è azzerato, mentre le misure americane contro chi commercia petrolio con L'Avana hanno scoraggiato fornitori alternativi. Le conseguenze sono blackout fino a 22 ore al giorno, paralisi dei trasporti, difficoltà negli ospedali, carenze idriche e forti ricadute sui servizi pubblici essenziali.
Su questo sfondo si inserisce anche l'incriminazione di Raúl Castro da parte del dipartimento di Giustizia americano per l'abbattimento di due aerei civili nel 1996. Sul piano formale il volto del regime resta Miguel Díaz-Canel, ma il peso politico del nome Castro continua a contare dentro gli apparati di sicurezza. L'atto d'accusa assume quindi anche il significato di un messaggio rivolto all'intera leadership cubana.
Anche sul piano diplomatico il linguaggio si è fatto più duro. Marco Rubio ha ammesso che la possibilità di una soluzione negoziata resta bassa, mentre il direttore della Cia John Ratcliffe ha lasciato intendere che Washington prenderebbe in considerazione un impegno con il governo cubano solo in presenza di cambiamenti sostanziali.
Il dispositivo militare schierato attorno a Cuba resta per ora più limitato di quello visto contro il Venezuela. Non ci sono quindi elementi sufficienti per parlare di un intervento imminente. Tuttavia tra crisi energetica, pressione giudiziaria, segnali politici e presenza navale, il confronto con L'Avana sembra entrare in una fase nuova.
•

un elemento critico nelle principali missioni di deterrenza navale e non soltanto nel combattimento ad alta intensità. Dopotutto, la visione della Rn e l'ambizione del governo britannico includono ancora chiaramente l'impegno con alleati e partner a sostegno degli interessi del Regno Unito, al di là della sola Nato e dell'Atlantico.
Il precedente governo britannico aveva delineato ambizioni di ricrescita del numero di cacciatorpediniere e fregate della Rn e di produzione di un ritmo costante di ordini per altre unità navali, così da rilanciare la capacità dei cantieri britannici nell'ambito di una strategia nazionale di costruzione navale. Dalla prospettiva attuale, ciò può apparire inaccessibile e irrealizzabile, e la minaccia e la tecnologia potrebbero aver superato quegli obiettivi.
Oltre alla questione del futuro numero di fregate, è chiaramente in corso una nuova riflessione sul futuro programma destinato a sostituire i cacciatorpediniere da difesa aerea Type-45 e sulla futura configurazione delle nuove navi anfibie nell'ambito del progetto Multi-role strike ship, entrambi programmi critici. Vi è quindi nuova incertezza su come tutto questo si svilupperà, ma si intravede anche un'opportunità sia per i fornitori navali tradizionali sia per i nuovi attori tecnologici.
Vi è anche la questione se la nuova tecnologia possa essere fornita alla scala e alla velocità ora previste. Molte delle nuove tecnologie senza equipaggio e autonome sono, come ha suggerito il Primo Lord del mare, già realtà scientifica anziché fantascienza. Tuttavia, in alcune aree, per esempio alcune delle più grandi piattaforme senza equipaggio per oceano aperto che fanno parte della nuova visione, e che saranno fondamentali per sostenere i futuri dispiegamenti di gruppi operativi, i piani sono ancora soltanto allo stadio concettuale.
Solo se tutto questo tornerà, la visione ibrida della Rn manterrà la sua promessa. E solo se equilibrio e scala saranno corretti, la Rn sarà in grado di conservare un ruolo di primo piano nell'affrontare le minacce che essa e gli alleati del Regno Unito dovranno fronteggiare nella sfera navale.

MULTI-ROLE STRIKE SHIP L'espressione indica il progetto con cui Londra sta ripensando il futuro delle proprie navi anfibie, spostandole da una logica tradizionale di trasporto e sbarco verso una piattaforma molto più flessibile, capace di combinare presenza, attacco, supporto a droni e operazioni distribuite. In sostanza, non si cerca soltanto una nuova nave, ma una nuova funzione navale. Questo rende il programma cruciale, perché dalla sua configurazione dipenderà il modo in cui la Royal navy immagina di proiettare forza in un ambiente dove massa, vulnerabilità e rapidità tecnologica stanno cambiando insieme.

STRATEGICAMENTE

di ANDREA MARGELLETTI*

Prevalere nel dominio cibernetico *prima, durante e dopo l'ingaggio*

Lo spettro cyber rappresenta in modo ormai più che consolidato lo spazio per eccellenza in cui possono dipanarsi senza sosta e spesso in contemporanea l'intero ambito di dinamiche che caratterizzano lo scenario strategico attuale. Attraverso i livelli fisico, logico-sintattico e umano-cognitivo, le fasi di cooperazione, competizione e conflitto, di pace, crisi e guerra, si fondono e confondono, tramutando l'intima dipendenza da digitalizzazione e informatizzazione di ogni articolazione delle società contemporanee in un teatro costantemente minacciato, contestato e conteso. Una prospettiva resa fin troppo evidente dall'apparentemente inarrestabile incremento annuale di attacchi cibernetici, sempre più spesso affinati e abilitati dal ricorso a strumenti di intelligenza artificiale. *Malware, ransomware* e *wiper*, nonché Denial of service (Dos) e Distributed denial of service (Ddos), rappresentano infatti voci di un vocabolario divenuto pericolosamente comune e in gran parte conseguenza della sincrasi malevola tra azioni meramente criminali e attività statuali o para-statuali alla frontiera della conflittualità ibrida.
Sicurezza e resilienza nel dominio cibernetico si delineano dunque in modo acclarato come premesse indispensabili e priorità assolute per il funzionamento stesso di istituzioni, economie e comunità, ma la lotta nel *cyber*-spazio non si limita alla sola difesa delle infostrutture nazionali, bensì permea profondamente il modo per preparare, pianificare e condurre operazioni militari ovunque e ognitempo. La capacità di penetrare le reti di potenziali avversari, di manovrare occultamente al loro interno, di estrarre informazioni e di generare effetti trasversali attraverso le dimensioni fisica, virtuale e cognitiva è divenuto infatti un cardine imprescindibile della deterrenza. Tanto come attività isolate, quanto più se integrate e sincronizzate in azioni multi-dominio, queste garantiscono infatti di predisporre e nell'*extrema-ratio* imporre sempre un confronto o scontro irrimediabilmente impari e asimmetrico a un potenziale avversario. Dal contributo alla preparazione informativa dell'ambiente operativo (Ipoe – Intelligence preparation of the operational environment), alla disattivazione di reti e sistemi critici per il funzionamento del dispositivo militare contrapposto, fino al sovraccarico cognitivo e alla confusione decisionale degli operatori nemici, il dominio cibernetico, e soprattutto la capacità di prevalervi, è non solo un abilitante fondamentale al successo di un'operazione, ma ne costituisce un elemento organico prima, durante e dopo l'ingaggio.

Se l'ineffabilità del *cyber*-spazio spesso ne previene la comprensibilità, impedendo di cogliere appieno l'impatto delle attività attraverso lo stesso, il successo spettacolare, in termini strettamente militari, di alcune delle più decisive operazioni dell'ultimo anno dà estrema concretezza a quanto la primazia nel dominio cibernetico possa risultare dirimente. Operazioni come Midnight hammer in Iran o Absolute resolve in Venezuela, condotte dagli Stati Uniti, includono infatti una panoplia di azioni sinergiche nel dominio cibernetico volte a massimizzare la conoscenza di obiettivi e difese, garantire la sorpresa tattica e operativa, contribuire a proteggere le forze e amplificare gli effetti delle attività cinetiche tradizionali. Gli attacchi *cyber* rappresentano infatti in questi casi occulta premessa, decisivo supporto e lascito ritardante di operazioni ad altissimo impatto. Presenti sul, o meglio nel, bersaglio ben prima del tonare delle esplosioni e ancora attivi attraverso le reti mentre il rombo della battaglia si acquieta.
Se il presente della competizione strategica è permeato da un incessante confronto nel dominio cibernetico e la sicurezza delle infostrutture rappresenta un requisito imprescindibile in patria e all'estero, essere in grado di penetrare, sorvegliare, disarticolare e degradare quelle avversarie sarà sempre più dirimente per la credibilità della deterrenza e il successo della difesa.

IPOE

La sigla indica la Intelligence preparation of the operational environment, cioè l'insieme delle attività con cui si studia in anticipo un teatro operativo per capire come funziona, dove sono i punti deboli e quali condizioni possono favorire o ostacolare un'azione militare. Nel dominio *cyber* questo lavoro assume una forma ancora più profonda, perché significa mappare reti, accessi, dipendenze digitali, flussi informativi e vulnerabilità nascoste. Non è ancora l'attacco, ma è ciò che lo rende possibile. Chi domina questa fase parte con un vantaggio decisivo prima ancora che il conflitto diventi visibile.

* presidente del CeSI

L'attenzione internazionale era catturata dalla crisi in Venezuela, ma nel Baltico si consumava una nuova ondata di sabotaggi contro i cavi sottomarini, con sei infrastrutture danneggiate in pochi giorni. L'episodio ha riaperto il nodo della vulnerabilità della regione e ha messo alla prova i meccanismi di deterrenza costruiti dopo i casi precedenti

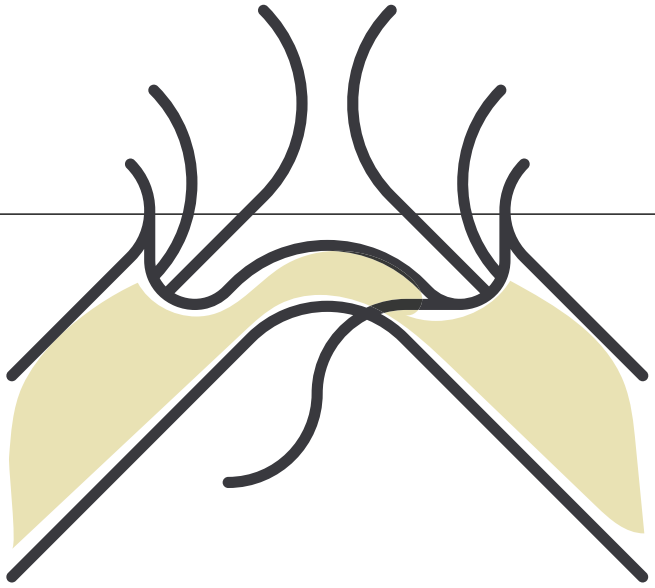
Intanto nel Baltico i sabotaggi proseguono

ELISABETH BRAW
senior fellow presso l'Atlantic Council

Mentre il mondo guardava lo spettacolare rapimento del presidente venezuelano Nicolás Maduro da parte delle forze statunitensi, eventi drammatici si stavano svolgendo anche nel mar Baltico e nel golfo di Finlandia. Ma, con il Venezuela al centro dell'attenzione mondiale, pochi hanno prestato attenzione alle acque del Nord Europa . È un peccato, perché nel giro di meno di una settimana, sei cavi sono stati danneggiati lì. Dopo una pausa durata un anno, lo spettro dei sabotaggi sembra essere tornato. Ora, con la Nato distratta dalla crisi sulla Groenlandia, la domanda è che cosa possano fare gli Stati occidentali contro questi attacchi. L'intervento statunitense del 3 gennaio in Venezuela è stato un'operazione perfettamente adatta alla televisione: esplosioni, oscurità ed elicotteri a bassa quota che trasportavano le truppe scese a terra, che hanno catturato Maduro e sua moglie e li hanno portati fuori dal Paese. Non c'è da stupirsi che ampie parti del mondo non riuscissero a pensare e parlare d'altro.

Dall'altra parte del pianeta si stava svolgendo un dramma completamente diverso. Il 31 dicembre, un cavo dati che collega Finlandia ed Estonia ha avuto un malfunzionamento, ed è diventato rapidamente chiaro che era stato colpito da un oggetto esterno. Le autorità finlandesi ed estoni hanno presto individuato il probabile responsabile tra le navi in attraversamento nel golfo di Finlandia: la nave cargo Fitburg, battente bandiera di Saint Vincent e Grenadine, in rotta dal porto russo di San Pietroburgo verso Haifa, in Israele, e che si trovava sopra il cavo nel momento in cui questo ha smesso di funzionare. Inoltre, le autorità finlandesi hanno potuto constatare che la nave sembrava trascinare l'ancora. Con un'operazione rapida, la Guardia di frontiera finlandese si è avvicinata alla nave sospetta, che era passata dalla zona economica esclusiva estone a quella finlandese, e gli ha ordinato di entrare nelle acque territoriali finlandesi. La Finlandia è il tipo di Paese che rispetta la Convenzione delle Nazioni Unite sul diritto del mare. Non appena la Fitburg è entrata nelle acque territoriali, è comparso un elicottero finlandese, dal quale sono scesi agenti di polizia che hanno preso il controllo della nave. Stava effettivamente trascinando l'ancora. Le autorità hanno fermato sia la nave sia il suo equipaggio: marinai provenienti da Russia, Georgia, Kazakistan e Azerbaigian. Il presidente finlandese Alexander Stubb ha scritto un *tweet* sulla vicenda, mentre la polizia, l'autorità doganale e la guardia di frontiera hanno tenuto una conferenza stampa. Nell'ottobre 2023, quando un cavo e un gasdotto nel golfo di Finlandia furono colpiti dalla portacontainer di proprietà cinese Newnew Polar Bear, una risposta così rapida e risoluta era inconcepibile. Da allora, gli incidenti frequenti che hanno coinvolto cavi hanno reso le nazioni del mar Baltico più esperte e immensamente più

BALTIC SENTRY È il nome dato alla nuova funzione di pattugliamento e allerta creata nel mar Baltico dopo la serie di sabotaggi ai cavi e alle infrastrutture sottomarine. Più che una singola missione, è un dispositivo di sorveglianza continua fondato su presenza navale, coordinamento tra Paesi rivieraschi e capacità di reazione rapida. Il suo valore sta soprattutto nella deterrenza. Rendere visibile che il mare è osservato serve a ridurre lo spazio d'azione di chi conta sull'ambiguità, sui tempi lenti e sulla difficoltà di attribuire subito un sabotaggio.



coordinate. Ma c'era un altro elemento nel viaggio di Capodanno della Fitburg attraverso il golfo di Finlandia: anche un secondo cavo era stato danneggiato. Apparteneva alla società svedese Arelion, che aveva subito il danneggiamento di uno dei suoi cavi durante il viaggio distruttivo della Newnew Polar Bear nell'ottobre 2023. Ne parlerò, insieme ad altri incidenti, nel mio prossimo libro, *The Undersea War*. La Fitburg, in effetti, stava trascinando l'ancora da diverse ore quando le autorità finlandesi l'hanno fermata. Questa dinamica sembrava tutt'altro che accidentale, soprattutto considerando l'enorme attenzione ricevuta dalla serie di tagli ai cavi nel mar Baltico iniziata con la Newnew Polar Bear. Non sapere che la propria nave stesse trascinando l'ancora è una scusa difficilmente credibile dopo diversi incidenti di alto profilo, nonostante gli equipaggi abbiano sostenuto tale versione. Dopo che la petroliera ombra Eagle S ha tagliato cinque cavi il giorno di Natale del 2024, le nazioni del mar Baltico e la Nato hanno creato rapidamente nuove procedure. Hanno istituito Baltic sentry, essenzialmente una funzione di pattugliamento e allarme nel mar Baltico. Hanno poi creato Nordic warden, un sistema di rilevamento basato sull'intelligenza artificiale. Avevano già migliorato la condivisione delle informazioni. Sembrava funzionare. Dai danni della Eagle S nel golfo di Finlandia, per mesi nessuna ancora era stata accidentalmente trascinata sul fondale baltico. "Dall'inizio di Baltic Sentry, non è successo nulla. Quindi questo significa che la deterrenza sta funzionando", ha dichiarato l'ammiraglio Giuseppe Cavo Dragone, il massimo ufficiale militare della Nato, al *Financial Times* nel novembre 2025. Ma solo fino a Capodanno. Il problema non riguardava soltanto i due cavi tagliati a san Silvestro. Altri tre cavi erano stati danneggiati nei giorni precedenti. Le autorità pensavano che ciò potesse essere legato alle condizioni meteorologiche, ma nessuno ne era sicuro, visto che il tempo in quei giorni non era stato particolarmente severo. Il 3 gennaio si è spezzato anche un cavo che collega Lituania e Lettonia, da dove prosegue verso l'Estonia. Le autorità lettoni hanno risposto rapidamente, identificando e fermando la nave che sembrava aver causato il danno. L'equipaggio è stato collaborativo, il che era un segnale positivo: i sabotatori di cavi difficilmente coopererebbero con le autorità locali. Ma si è rivelata essere la nave sbagliata. I lettoni stanno ancora cercando il sospetto. I finlandesi, nel frattempo, hanno arrestato uno dei membri dell'equipaggio della Fitburg, un azero, e imposto un divieto di viaggio ad altri due. In totale, sei cavi hanno avuto malfunzionamenti nel mar Baltico intorno a Capodanno. Anche se il maltempo fosse stato il responsabile in uno o due casi, si tratta comunque di una situazione grave. In effetti, questo sembra essere il primo caso in assoluto di sei

I Marine puntano ai droni gregari entro il 2029

Il Corpo dei Marine degli Stati Uniti sta accelerando sul programma dei Collaborative combat aircraft (Cca) e punta a ricevere entro il 2029 i primi esemplari operativi dell'Mq-58 Valkyrie, il drone sviluppato da Kratos destinato a operare in sinergia con i caccia con equipaggio, in particolare gli F-35. Il traguardo segna una prima scadenza concreta in un percorso che per i Marine serve non solo ad aumentare capacità operative e flessibilità in scenari ad alta minaccia, ma anche a costruire un ponte verso la futura architettura del combattimento aereo. La prima fase ruoterà attorno a una versione dell'Mq-58 dotata di carrello di atterraggio e capace di operare da piste convenzionali, superando la logica delle precedenti sperimentazioni basate su varianti lanciate con razzi e prive di recupero su pista. L'obiettivo è aumentare il riutilizzo del sistema e renderlo più sostenibile sul piano operativo. Il primo volo di questa variante è atteso entro l'estate, mentre i prototipi operativi dovrebbero essere assegnati nel 2029 allo squadrone Vmx-1 in Arizona, dove verranno usati per *test* tattici e sviluppo dei concetti d'impiego.
Accanto al progetto Valkyrie, i Marine stanno però valutando anche altre soluzioni industriali con aziende come General Atomics, Anduril e Northrop Grumman. L'idea è di ampliare progressivamente la famiglia dei Cca, includendo piattaforme con capacità di decollo corto o verticale, più coerenti con la dottrina *expeditionary* del Corpo e con l'impiego degli F-35B. In questa logica conta la possibilità di operare con minore dipendenza da piste lunghe e infrastrutture esposte.
Sul piano delle missioni, la priorità iniziale viene assegnata alla guerra elettronica. I primi Mq-58 dovrebbero infatti essere impiegati come piattaforme per disturbo, supporto e saturazione dello spazio elettromagnetico. Il velivolo ha però già mostrato un ventaglio più ampio di possibilità, dal trasporto di munizioni aria-aria e bombe di piccolo diametro, fino al ruolo di vettore per il lancio di droni più piccoli. Resta comunque una forte componente sperimentale. Il programma non è ancora entrato in una fase di acquisizione formale e molte scelte, dalle configurazioni tecniche ai profili di missione, saranno definite attraverso i *test* dei prossimi anni. Il programma diventa così uno dei passaggi con cui i Marine cercano di tradurre l'integrazione tra velivoli con equipaggio e sistemi autonomi in una capacità operativa più stabile e meno sperimentale.
•

cavi messi fuori uso nel giro di pochi giorni nelle stesse identiche acque. Le prove contro i tre membri dell'equipaggio della Fitburg, il cui proprietario è un azero con stretti legami con la Russia, sono chiaramente solide, e potrebbero ancora emergere sospetti negli altri casi.
Dopo quasi un anno di apparente calma sottomarina nel mar Baltico, lo spettro del taglio dei cavi è tornato. Questo ha effetti pratici, perché anche nel Baltico, ricco di cavi, trovarsi con sei cavi fuori uso è una questione seria. Finché i cavi restano fuori servizio la regione si trova, di fatto, in una situazione di vulnerabilità acuta. Se altri cavi si rompessero prima che questi siano stati riparati, la connettività ne risentirebbe.
Poi c'è l'aspetto della sicurezza. Gli sforzi delle nazioni rivierasche per mantenere sicuro il loro piccolo mare potrebbero non aver funzionato. Che cosa possono fare adesso? Di certo non coinvolgere la Nato, che – come il mondo ha appreso in modo drammatico – affronta una crisi esistenziale sulla Groenlandia. In effetti, il fondale baltico potrebbe essere il punto di snodo in cui diventa chiaro che la Nato è entrata in quella crisi esistenziale. Questo lascia alle nazioni del mar Baltico il compito di trovare un altro modo per rafforzare la protezione. È una fortuna che si siano esercitate: sebbene Baltic Sentry porti un'etichetta Nato, sono le stesse nazioni del Baltico a eseguirla. Ma l'esito più allarmante potrebbe essere questo: i sabotatori concluderanno che il mondo è distratto da altri eventi. Il dramma di Capodanno nel Baltico ha ricevuto soltanto l'attenzione mediatica più superficiale e, considerando le notizie dal Venezuela e da altrove, non sorprende affatto. Chi può prestare attenzione alle rotture dei cavi quando gli Stati Uniti depongono governanti o quando valutano di impadronirsi di un territorio alleato e di entrare in guerra contro l'Iran?
I potenziali sabotatori e i loro possibili sostenitori potrebbero, in effetti, concludere che ora hanno campo libero per colpire queste infrastrutture. Saprete della loro decisione quando le comodità e le necessità della vostra vita quotidiana si faranno più lente o, Dio non voglia, indisponibili.

Riproponiamo l'articolo "*Baltic Cable-Cutting Is Back*", apparso su www.foreignpolicy.com.


NORTHROP GRUMMAN
Italia
Missione compiuta. Ovunque. Sempre
High and Medium Accuracy Inertial Navigation System
per garantire il successo della missione in ambienti ostili
NG Italia Leading the Way
For more information, please contact: Northrop Grumman Italia S.p.A Marketing and Sales.Phone: +39 06 911 922 90
marketing@northropgrumman.it http://www.northropgrumman.it

L'intervista

Il potere del mare *tra industria, ricerca e difesa*

Intervista a
Roberta Pinotti
già ministro della Difesa e presidente della Fondazione Polo nazionale della dimensione subacquea

a cura di Riccardo Leoni

Dal Baltico a Hormuz, passando per il mar Rosso, tutti i conflitti recenti ci stanno comunicando il medesimo messaggio: la conflittualità navale e sottomarina sta evolvendo rapidamente. Le vastità oceaniche, un tempo silenziose e popolate solo da pochi sottomarini, si fanno oggi sempre più affollate di attori, infrastrutture, sistemi e minacce. L'Italia, Paese la cui proiezione geopolitica è fortemente influenzata dalla sua posizione centrale nel Mediterraneo, non può esimersi dall'apprendere questa lezione. Ne abbiamo discusso con Roberta Pinotti, già ministro della Difesa e presidente della Fondazione Polo nazionale della subacquea.

Presidente, oggi si sente tanto parlare di spazio, mentre molto meno spesso si parla della dimensione subacquea. Eppure, episodi come i sabotaggi ai cavi sottomarini nel Baltico o il blocco dello stretto di Hormuz ci raccontano un'altra storia. Perché l'*underwater* è diventato un ambito così strategico, non solo per l'Italia ma anche a livello internazionale?

La corsa allo spazio è iniziata alla fine degli anni Cinquanta, ma soltanto negli ultimi anni abbiamo iniziato a parlare concretamente della necessità di approfondire conoscenza e tecnologia del mondo sottomarino. In parte

MEDITERRANEO ALLARGATO

L'espressione indica una visione strategica in cui la sicurezza dell'Italia non si esaurisce nel mare che bagna direttamente le sue coste, ma si estende a un arco molto più ampio che comprende aree come il Corno d'Africa e l'Indo-Pacifico. Il punto è semplice. Crisi, traffici, instabilità e minacce che nascono lontano possono avere effetti diretti su energia, commercio e sicurezza nazionale. Per questo il Mediterraneo non viene più letto come uno spazio chiuso, ma come il centro di una rete di connessioni geopolitiche molto più vasta.

La dimensione subacquea è diventata un terreno decisivo per la sicurezza, l'economia e la proiezione geopolitica dell'Italia. Tra cavi sottomarini, traffici energetici, mine e nuove tecnologie, il Paese è chiamato a costruire una strategia integrata, capace di unire Difesa, industria e ricerca

questo ritardo è stato dovuto al fascino esercitato dalla conquista dello spazio sulle grandi potenze, ma esiste anche una ragione tecnologica molto concreta: conoscere e utilizzare i fondali marini è estremamente complesso per via delle condizioni proibitive dell'ambiente abissale. Solo recentemente lo sviluppo delle tecnologie ha consentito di affrontare con maggiore determinazione questa sfida. Non è un caso che negli ultimi due anni la mappatura dei fondali sia passata da poco più del 20% a circa il 30%. Cresce infatti l'esigenza non soltanto di conoscere e utilizzare il mare, ma anche di difenderlo. Lei ha citato il Baltico e la crisi nello stretto di Hormuz, ma possiamo pensare anche al mar Rosso: gran parte dei traffici mondiali passano dal mare e, soprattutto, sotto il mare transitano il 95% delle comunicazioni globali, attraverso i cavi sottomarini. A questo si aggiunge il trasporto delle fonti energetiche. Il mare oggi è una risorsa fondamentale per lo sviluppo economico e per la sicurezza delle nostre società, ed è quindi indispensabile proteggerlo.

L'Italia, lo sappiamo, occupa una posizione centrale nel Mediterraneo, ma oggi il quadro strategico nazionale si estende ben oltre, dal Corno d'Africa all'Indo-Pacifico. Quanto pesa questa centralità e quali responsabilità comporta per il nostro Paese?

Quando ero ministro della Difesa, nel 2015, lavorammo al Libro bianco della Difesa, un documento strategico che analizzava le sfide presenti e future. In quel contesto venne utilizzato, forse una delle prime volte in maniera ufficiale, il concetto di "Mediterraneo allargato". Era chiaro che il Mediterraneo rappresentasse il centro della nostra proiezione geopolitica, ma era altrettanto evidente che le dinamiche che interessano il Corno d'Africa o l'Indo-Pacifico avessero ricadute dirette sulla sicurezza e sullo sviluppo dell'Italia. Gli eventi successivi hanno dimostrato quanto quell'intuizione fosse corretta. L'Italia è una piattaforma naturale proiettata sul mare, ma per molto tempo non abbiamo dato alla dimensione marittima la centralità che meritava, forse anche perché le nostre capitali, quella politica ed economica, non sono città di mare. Oggi però questa consapevolezza sta crescendo, anche grazie a iniziative che stanno riportando il mare al centro del dibattito strategico nazionale.

La Marina militare italiana dispone dei cacciamine tra i più avanzati d'Europa. In uno scenario come quello di Hormuz, dove le mine sottomarine rappresentano uno strumento di guerra ibrida e di interdizione dei traffici energetici, quale ruolo potrebbe giocare l'Italia?

Molte marine nel tempo hanno progressivamente dismesso i cacciamine, considerandoli mezzi ormai superati. La Marina militare italiana invece ha sempre ritenuto strategica questa capacità strategica. Certamente i cacciamine svolgono ancora oggi un ruolo importante nello sminamento di residuati bellici delle guerre mondiali presenti nei nostri mari, ma la scelta di mantenere e sviluppare questa componente si è rivelata lungimirante anche rispetto al futuro. Con l'aumento delle infrastrutture sottomarine e delle attività che si svolgono sotto il mare, cresce infatti la necessità di protezione. Va dato merito alla Marina di aver saputo leggere in anticipo le traiettorie strategiche. Nei prossimi anni, inoltre, queste capacità saranno ulteriormente rafforzate con nuove dotazioni. È fondamentale non perdere competenze operative e tecnologiche che oggi risultano sempre più decisive.

Lei guida la Fondazione del Polo nazionale della dimensione subacquea. Quali sono le principali sfide di questa realtà e perché è stato importante dotare l'Italia di una struttura di coordinamento nazionale che fino a pochi anni fa non esisteva?

L'inaugurazione del Polo è avvenuta nel dicembre 2023, mentre la Fondazione è nata nel maggio 2025, ma il

TECNOLOGIE DUALI

Nel mondo *underwater* il carattere duale delle tecnologie è ancora più marcato che altrove. Sensori, robot autonomi, sistemi di comunicazione, materiali e *software* nati per usi civili come energia, archeologia, ricerca o cantieristica possono essere rapidamente adattati a sorveglianza, protezione di infrastrutture o operazioni di sicurezza. Questo cambia il modo in cui si costruisce un ecosistema nazionale, perché l'innovazione non nasce più dentro compartimenti chiusi ma dall'incontro tra filiere differenti. Il vantaggio strategico, quindi, non dipende solo da chi investe di più, ma da chi riesce a collegare meglio mondi industriali che prima si parlavano poco.

L'intervista

percorso parte ancora prima, dalle norme inserite nella legge di bilancio del 2023. Sono state fatte due scelte strategiche. La prima è stata quella di attribuire alla Marina militare una responsabilità specifica sulla dimensione subacquea. La seconda è stata la creazione di un Polo nazionale interministeriale. Non è infatti un progetto che riguarda soltanto il ministero della Difesa: coinvolge il ministero delle Imprese e del Made in Italy, il ministero dell'Università e della Ricerca e, successivamente, anche il ministero del Mare. Questo significa lavorare fin dall'inizio in una logica integrata. L'altro elemento decisivo è la collaborazione tra pubblico e privato. Lo sviluppo tecnologico *underwater* avrà certamente implicazioni strategiche e di sicurezza, ma rappresenta anche un enorme potenziale industriale. Oggi il Polo riunisce grandi aziende, Pmi, *start up*, università e centri di ricerca. La struttura operativa sviluppa progetti di ricerca destinati a diventare prototipi e, successivamente, prodotti industriali. È una sfida fondamentale per costruire una strategia nazionale coerente e non frammentata.

Quando si pensa all'*underwater* si pensa subito a competenze molto specialistiche e strettamente tecniche. Quali sono, secondo lei, le professionalità e i saperi decisivi per costruire un ecosistema italiano all'avanguardia, anche quelli meno intuitivamente legati a questo mondo?
Serviranno certamente professionalità altamente specializzate e tecniche, ma credo che molte delle figure necessarie le andremo a delineare a mano a mano che cresceremo nella conoscenza e nelle tecnologie. Per questo è importante che nel Polo siano presenti non solo 20 grandi aziende e 177 fra Pmi e *start up*, ma anche 63 tra università e centri di ricerca: si dovrà adeguare rapidamente la formazione alle nuove esigenze che emergeranno. Allo stesso tempo non dobbiamo pensare a competenze esclusivamente settoriali. Lavorando sui progetti del Polo abbiamo scoperto che tecnologie sviluppate in ambiti avanzati come l'automotive o lo spazio possono essere estremamente utili anche per il mondo subacqueo. Allo stesso tempo non dobbiamo pensare a competenze esclusivamente settoriali. L'innovazione nascerà proprio dall'incontro tra saperi diversi.

Guardando al futuro, quali saranno le sfide decisive nella dimensione subacquea e come dovrà muoversi l'Italia per farsi trovare pronta, sia nella tutela dei propri interessi strategici sia nel contesto internazionale?
Le sfide riguardano certamente il monitoraggio dei fondali, la protezione dei cavi sottomarini, le contromisure anti-mine e lo sviluppo di sistemi autonomi. Ma i fondali rappresentano anche una risorsa ancora in gran parte inesplorata. Si parla già di agricoltura subacquea, senza dimenticare il patrimonio archeologico custodito dai mari e il tema delle terre rare. Naturalmente tutto questo pone anche un problema di regole. Le normative internazionali sui fondali marini sono datate rispetto alle nuove tecnologie oggi disponibili. Non bastano regole nazionali e neppure europee: serve una *governance* internazionale capace di stabilire rapidamente limiti, possibilità e divieti. La sfida sarà trovare un equilibrio tra sviluppo tecnologico, interessi strategici e tutela dell'ecosistema marino, che deve restare la priorità assoluta.

CONTROMISURE ANTI-MINE

Non indicano solo la rimozione degli ordigni una volta scoperti, ma l'insieme delle tecnologie e delle procedure usate per individuare, classificare, neutralizzare e prevenire la minaccia delle mine navali. È un campo che oggi torna decisivo perché questi ordigni restano economici, difficili da rilevare e capaci di bloccare rotte vitali con investimenti limitati. In uno scenario marittimo moderno, le contromisure anti-mine non servono soltanto a riaprire un passaggio. Servono a garantire continuità ai traffici, protezione alle infrastrutture e credibilità alla deterrenza.

ACQUE AGITATE

di FABIO CAFFIO*

Il blocco navale, questo sconosciuto *nel nuovo disordine dei mari*

Ormai quasi dimenticato, benché considerato un relitto di epoche passate, il blocco navale è tornato di prepotenza sulla scena internazionale giungendo a condizionare le nostre vite coi suoi effetti economici a cascata. E già, perché il blocco navale è sì un metodo di guerra marittima, ma soprattutto un mezzo per soffocare l'economia del nemico vietando a qualsiasi nave, anche neutrale, di avere contatti con suoi tratti di costa o porti.
Parlare di guerra sembrerebbe essere improprio e obsoleto alla luce della Carta delle Nazioni Unite. Correttamente, si dovrebbe quindi parlare di conflitto armato, oltre che per Hormuz (dove Stati Uniti e Israele agiscono in difesa legittima verso l'Iran per prevenire l'uso dell'arma atomica) anche per il blocco della striscia di Gaza da parte di Israele nell'ambito delle ostilità contro Hamas.
La tattica di interdire le coste avversarie si è consolidata nel XVI secolo, all'epoca della navigazione a vela. Il modello è stato quello dell'antico assedio terrestre a singole città. In questo modo, la guerra marittima è uscita dal ristretto ambito delle antiche operazioni di abbordaggio e di cannoneggiamento per acquisire una più vasta configurazione che coinvolge in alto mare i mercantili neutrali che abbiano relazioni commerciali con un avversario. In mare, anche in tempo di pace (e questa è oggi la situazione internazionale anche se la pace è "violenta") i belligeranti possono dunque legittimamente interferire con la libertà di navigazione dei neutrali a condizione di fare un uso non eccessivo dei loro diritti.
Nei secoli passati c'erano stati abusi verso la libertà di navigazione dei neutrali, finché con la Dichiarazione di Parigi del 1856 e la Dichiarazione di Londra del 1909 (entrambe mai divenute trattati internazionali) si fissarono come requisiti del blocco la sua effettività (limitazione a una specifica zona circoscritta davanti alle coste nemiche da sorvegliare continuamente con forze navali) e imparzialità sia verso i nemici che i neutrali di qualsiasi bandiera. Questi principi furono recepiti nella legge di Guerra italiana del 1938. Essi, benché mai formalizzati in una vera e propria convenzione internazionale, assunsero valore consuetudinario durante le due guerre mondiali.
Il ricorso al blocco divenne tuttavia marginale nella metodologia delle operazioni navali perché col progresso delle artiglierie terrestri (e poi dei missili) si riteneva rischioso mantenere delle forze navali bloccanti a distanza di qualche decina di miglia dalla costa.
Si giunge così al Manuale di Sanremo del 1994 nell'ambito del quale la prassi del blocco viene rivisitata alla luce del nuovo diritto del mare codificato nell'Unclos, del diritto umanitario e dei conflitti più recenti, precisando i suoi requisiti e prevedendo alcune novità quali: lasciare imprecisato il *locus* del blocco senza menzionare la costa degli altri belligeranti oppure i tratti di costa da questi occupati; consentire la cattura per forzatura del blocco delle "navi per la quale vi sono ragionevoli motivi di ritenere che le stesse stiano forzando il blocco" anche a notevole distanza dalla zona bloccata; vietare il blocco che abbia il solo scopo di affamare la popolazione civile o negare alla stessa beni essenziali. Al tempo Israele e gli Stati Uniti contribuirono attivamente alla redazione del Manuale con propri esperti. Ed è stata proprio Israele a farne un uso sistematico con la dichiarazione di blocco della Palestina del 2009. Poi seguita dall'Arabia Saudita col blocco del sud dello Yemen nel 2015 e infine ora col blocco di Hormuz di Usa e Iran che di fatto contraddice il principio del Manuale di Sanremo per cui il transito dei neutrali in uno stretto internazionale non può essere impedito per effetto del blocco dello stesso stretto.

MANUALE DI SANREMO

A seguito dell'emanazione della Carta delle Nazioni Unite che vieta il ricorso alla guerra come metodo per risolvere le controversie tra Stati, del diritto del mare codificato nell'Unclos, delle convenzioni di Diritto umanitario di Ginevra, della prassi instauratasi nel corso di conflitti come quello delle Falkland/Malvinas e Iran/Iraq si è formato un nuovo *corpus* di norme consuetudinarie costituenti il Diritto dei conflitti armati sul mare. In attesa di pervenire a una nuova convenzione internazionale in materia (sinora mai messa in cantiere), su iniziativa dell'Istituto internazionale di Diritto umanitario di Sanremo e del Comitato internazionale della Croce Rossa di Ginevra è stato redatto nel 1994 il Sanremo Manual on international law applicable to armed conflicts at sea, compilazione privata non vincolante predisposta da un gruppo di esperti non rappresentanti i Paesi di appartenenza.

* ammiraglio in congedo, esperto di Diritto marittimo

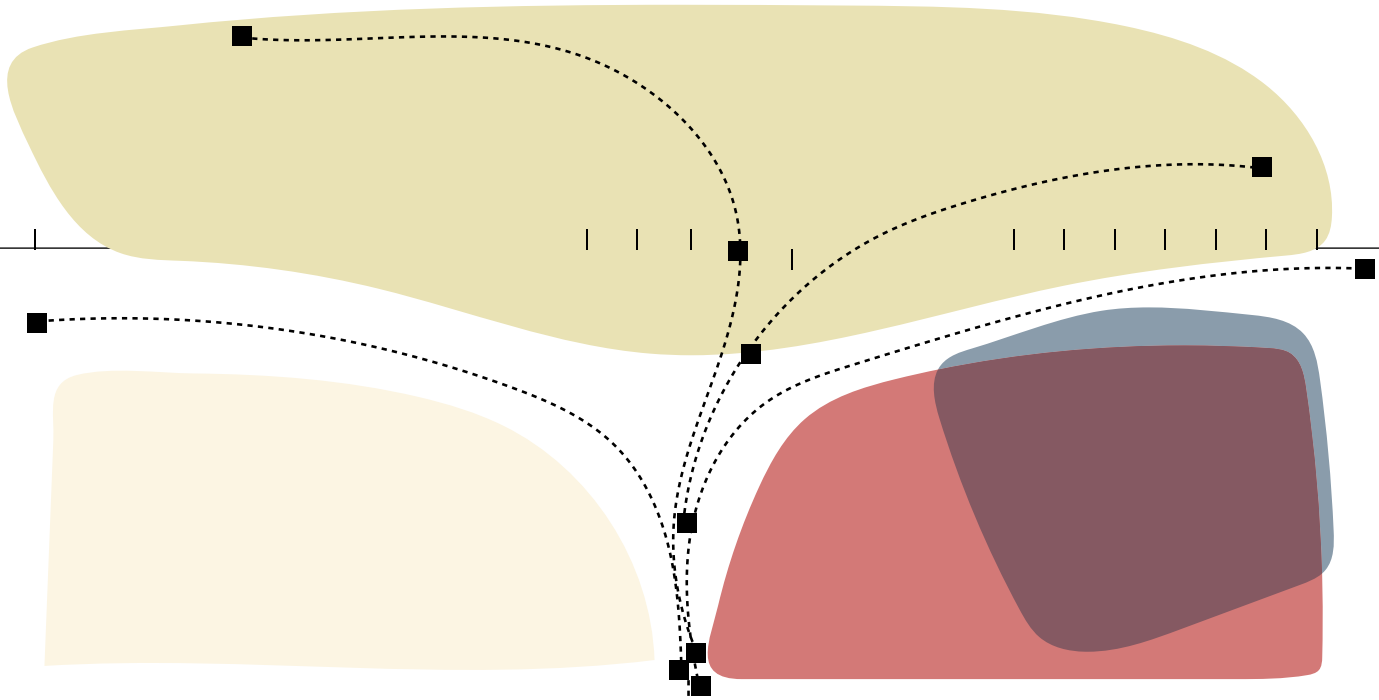
I cavi sottomarini sono il sistema nervoso della globalizzazione digitale. Il punto di svolta per la loro protezione è rappresentato dal fiber sensing. Fino a tempi recenti, i cavi sottomarini erano concepiti come semplici vettori, ottimizzati per capacità trasmissiva e bassa latenza. Oggi, invece, la fibra può essere impiegata anche come sensore distribuito lungo centinaia o migliaia di chilometri

Sensing, la frontiera strategica delle dorsali digitali

GIUSEPPE VALENTINO
vice presidente Backbone & infrastructure solutions di Sparkle

Nell'ecosistema digitale contemporaneo, i cavi sottomarini in fibra ottica costituiscono una infrastruttura critica essenziale: sostengono la continuità dei servizi e la sicurezza degli Stati, ovvero l'economia globale e la sovranità tecnologica. Oggi, tuttavia, queste dorsali non si limitano più a trasportare dati. L'evoluzione delle tecniche di *fiber sensing* apre la possibilità di utilizzare la stessa infrastruttura come strumento di rilevazione di eventi sismici, anomalie ambientali e potenziali interferenze ostili, collocando i cavi al centro di una nuova agenda strategica sui fondali marini.
Nel dibattito pubblico sulla trasformazione digitale, l'attenzione si concentra spesso su piattaforme, intelligenza artificiale, *cloud* e satelliti. Più raramente si guarda all'infrastruttura fisica che rende possibile questo ecosistema. Eppure, sui fondali marini transita la quasi totalità del traffico dati intercontinentale, lungo una rete che nel 2025 conta 597 sistemi attivi o in costruzione e 1.712 punti di approdo. La continuità di pagamenti, mercati finanziari, logistica, comunicazioni istituzionali e servizi digitali dipende quindi da una geografia materiale poco visibile, ma decisiva per il funzionamento delle società interconnesse.
I cavi sottomarini sono, in questo senso, il sistema nervoso della globalizzazione digitale. Non sono soltanto infrastrutture tecniche, ma corridoi di potere che incidono su rotte, ridondanze, dipendenze strategiche e capacità di attrazione di investimenti. Il controllo degli approdi, delle tratte alternative, delle stazioni di atterraggio e dei nodi di interconnessione produce infatti vantaggi economici, industriali e politici. In tale prospettiva, il Mediterraneo torna a essere un'area di rilevanza primaria: non solo spazio di traffici commerciali, ma snodo essenziale della connettività tra Europa, Africa, Medio Oriente e Asia.
Negli ultimi anni la vulnerabilità di queste dorsali è entrata stabilmente nell'agenda strategica euroatlantica. Danni accidentali, timori di sabotaggio e scenari di minaccia ibrida hanno chiarito che la sicurezza dei cavi non può più essere considerata una questione esclusivamente tecnica. L'Unione europea, con la Raccomandazione del 2024 e con il Piano d'azione sulla sicurezza dei cavi del 2025, ha impostato una risposta centrata su prevenzione, rilevamento, risposta, recupero e deterrenza. In questo quadro, la capacità di monitorare in modo più tempestivo ciò che avviene attorno alle infrastrutture subacquee diventa una componente-chiave della resilienza.
Il punto di svolta è rappresentato dal *fiber sensing*. Fino a tempi recenti, i cavi sottomarini erano concepiti come puri vettori di comunicazioni, ottimizzati per capacità trasmissiva e bassa latenza. Oggi, invece, la fibra può essere impiegata anche come sensore distribuito lungo centinaia o migliaia di chilometri.

DISTRIBUTED ACOUSTIC SENSING È una tecnica che trasforma una fibra ottica in una lunga catena di sensori distribuiti, capace di rilevare vibrazioni e microperturbazioni lungo il tracciato. In pratica il cavo non serve più solo a trasportare dati, ma anche a "sentire" ciò che accade attorno a lui, dal passaggio di una nave a un evento sismico fino a possibili interferenze sul fondale. Il salto concettuale è enorme. Una dorsale digitale diventa anche uno strumento di osservazione continua del dominio subacqueo, con implicazioni che toccano insieme resilienza delle reti, monitoraggio ambientale e sicurezza marittima.



Tecniche come il Distributed acoustic sensing (Das), lo State of polarization (Sop), l'interferometria ottica e altre architetture di *sensing* consentono di rilevare vibrazioni, deformazioni e anomalie lungo il tracciato, trasformando progressivamente la dorsale digitale in una infrastruttura capace non solo di connettere, ma anche di osservare.

Le ricadute sono rilevanti su più livelli. Sul piano scientifico e civile, questi sistemi possono rafforzare il monitoraggio sismico e oceanografico, migliorare la rilevazione dei terremoti sottomarini, contribuire significativamente al potenziamento e all'efficacia degli allarmi tsunami e ampliare la capacità di osservazione del mare profondo. Le iniziative internazionali sui cosiddetti Smart cables mirano proprio a integrare telecomunicazioni e sensoristica in una stessa infrastruttura, sfruttando i cicli di rinnovo dei cavi per generare benefici in termini di conoscenza, prevenzione del rischio e continuità operativa.

Una delle implicazioni più rilevanti riguarda il piano geopolitico e regolatorio. Un cavo in grado di rilevare variazioni dell'ambiente circostante può offrire elementi utili per una migliore conoscenza del dominio subacqueo, per monitorare l'infrastruttura e per una gestione più efficace della resilienza operativa. In questa prospettiva, il *fiber sensing* si colloca all'incrocio tra protezione dei cavi, osservazione ambientale e possibili applicazioni a supporto della sicurezza marittima. Proprio questa pluralità di funzioni ne fa un tema di crescente interesse per il dibattito di *policy*.

Per l'Europa e per il Mediterraneo, questa evoluzione assume un significato particolare. La densità delle rotte, la centralità dei collegamenti verso Africa e Medio Oriente, il peso crescente degli attori privati e la ricerca di corridoi digitali più resilienti fanno della regione un laboratorio strategico avanzato. In questo quadro l'Italia può valorizzare la propria posizione geografica, oltre che come punto di approdo e transito, come piattaforma di innovazione nel dominio subacqueo. Le sperimentazioni già avviate nel Mediterraneo indicano che la competizione futura riguarderà non soltanto la capacità di connettere, ma anche quella di monitorare, proteggere e governare le infrastrutture del fondale.

In Italia, l'evoluzione delle tecnologie associate ai cavi intelligenti si inserisce in un quadro di attenzione crescente verso la dimensione subacquea e le sue applicazioni civili, scientifiche e industriali. In questo contesto, il Polo nazionale della dimensione subacquea (Pns), una struttura coordinata dalla Marina militare, rappresenta un punto di raccordo tra amministrazioni, mondo della ricerca e soggetti industriali, favorendo lo sviluppo di progettualità e sperimentazioni nel settore e fornendo un terreno fertile allo sviluppo di capacità tecnologiche nazionali strategiche. Tra le iniziative

L'Ue sta lavorando a un suo articolo 5 su modello Nato?

A Bruxelles è in corso un lavoro tecnico per dare maggiore concretezza all'articolo 42.7 del Trattato sull'Unione europea, la clausola di mutua assistenza prevista in caso di aggressione armata contro uno Stato membro. La clausola, però, non coincide con l'articolo 5 della Nato e non può essere considerata un suo equivalente pieno. Il trattato europeo prevede l'obbligo di fornire aiuto con tutti i mezzi in proprio potere, ma precisa anche che, per i Paesi appartenenti all'Alleanza atlantica, la Nato resta il fondamento della difesa collettiva. La differenza non è solo giuridica, ma anche operativa. L'articolo 5 si appoggia a una struttura militare integrata, a una catena di comando definita e a protocolli consolidati, mentre la clausola europea non dispone di un apparato comparabile e lascia ai singoli Stati ampi margini di discrezionalità sulla forma dell'assistenza. Questo significa che l'aiuto previsto dall'articolo 42.7 può tradursi in sostegno politico, diplomatico, economico o militare, senza automatismi né garanzie uniformi. In questo contesto, il Servizio europeo per l'azione esterna ha predisposto un primo documento dedicato all'operazionalizzazione dell'articolo 42.7 e ha già svolto simulazioni riservate con gli ambasciatori del Comitato politico e di sicurezza. L'obiettivo non è creare una difesa collettiva europea sul modello Nato, ma chiarire come dovrebbero muoversi istituzioni e Stati in caso di attivazione della clausola. Il lavoro in corso prende in considerazione tre scenari. Il primo riguarda l'attacco a un Paese membro che appartiene sia all'Unione sia alla Nato, con l'eventuale attivazione parallela delle due clausole. Il secondo riguarda uno Stato membro dell'Unione che non faccia parte dell'Alleanza atlantica. Il terzo prende in esame attacchi al di sotto della soglia del conflitto tradizionale, come le aggressioni ibride. Le simulazioni servono soprattutto a stabilire ruoli, responsabilità e modalità di coordinamento tra governi e istituzioni europee. Il nodo di fondo resta però politico. Anche con procedure più chiare, la difesa continua a essere materia controllata dagli Stati membri e i trattati non attribuiscono all'Unione una competenza diretta paragonabile a quella della Nato. Più che la nascita di un vero articolo 5 europeo, il cantiere aperto a Bruxelles segnala il tentativo di rendere più credibile uno strumento finora poco utilizzato.
•

Frattasi lascia la guida dell'Acn

Bruno Frattasi ha lasciato la guida dell'Agenzia per la *cyber*-sicurezza nazionale con una lettera inviata a Palazzo Chigi nella quale ha richiamato motivi personali. Al suo posto arriva Andrea Quacivi, *manager* con esperienza nel settore informatico e già amministratore delegato di Sogei, chiamato a raccogliere il testimone in una fase particolarmente delicata per la sicurezza digitale italiana.
Frattasi era stato nominato direttore generale dell'Acn il 9 marzo 2023, dopo una lunga carriera nell'amministrazione dell'Interno. Entrato al Viminale nel 1981 e nominato prefetto nel 2005, aveva ricoperto tra gli altri gli incarichi di prefetto di Latina, capo dipartimento dei Vigili del fuoco, capo dell'Ufficio legislativo del ministro dell'Interno, capo di gabinetto al Viminale e prefetto di Roma prima del passaggio all'Agenzia. Le dimissioni chiudono così una fase iniziata con il riassetto del vertice dell'Acn nel 2023 e aprono una nuova transizione in un ambito diventato sempre più centrale per la sicurezza nazionale, la protezione delle infrastrutture critiche e il coordinamento della risposta italiana alle minacce cibernetiche.
•

avviate rientra anche il progetto Sensomar, promosso da un partenariato di grandi aziende (tra cui Sparkle), piccole e medie imprese ed enti di ricerca italiani, con l'obiettivo di sviluppare un cavo dotato di funzionalità di *fiber sensing* per attività di monitoraggio sismico, ambientale e di sicurezza. Questo progetto rappresenta non solo un'importante dimostrazione tecnologica su scala nazionale, ma anche un modo per assicurare all'Italia piena autonomia e competitività nella gestione di infrastrutture digitali sempre più multifunzionali. Più che un punto di arrivo, si tratta di un segnale dell'interesse crescente verso piattaforme sottomarine capaci di integrare connettività e osservazione.
Resta infine il profilo regolatorio. Il quadro giuridico internazionale, costruito in larga misura attorno alla posa, alla manutenzione e alla protezione dei cavi, dovrà verosimilmente confrontarsi anche con infrastrutture capaci di generare dati ambientali e informazioni utili al monitoraggio operativo. Se una dorsale privata integra anche funzionalità di *sensing*, si pongono temi di *governance* dei dati, accesso, trasparenza, responsabilità e coordinamento tra attori pubblici e privati. In questa prospettiva, la definizione di regole, standard condivisi e forme di cooperazione internazionale potrà accompagnare l'evoluzione delle infrastrutture digitali sottomarine. I cavi, infatti, oltre a sostenere la connettività globale, possono progressivamente assumere un ruolo più ampio nella conoscenza del dominio subacqueo.

SMART CABLES Con questa espressione si indicano cavi sottomarini progettati per combinare telecomunicazioni e sensoristica nella stessa infrastruttura. L'idea è sfruttare il rinnovo o la posa di nuove dorsali per integrare funzioni aggiuntive, come la misurazione di parametri sismici, pressioni, variazioni ambientali o anomalie lungo il tracciato. Il valore non è solo tecnico. Significa passare da una rete invisibile che collega continenti a una rete che produce anche conoscenza sul mare profondo, sulla continuità operativa e sulla vulnerabilità delle infrastrutture critiche che sostiene.

CYBERNETICS

di ERNESTO DAMIANI*

I recinti digitali dell'Iran *tra rete a due velocità e controllo politico*

Mentre il mondo osserva impotente l'imposizione di controlli discrezionali da parte di diversi attori sul traffico di merci nello stretto di Hormuz, un'operazione simile si sta svolgendo anche sulle dorsali in fibra ottica della regione. Il regime ha superato la fase del blackout Internet totale, troppo costosa per l'economia e difficile da gestire, e ha adottato un sistema stratificato di controllo dell'accesso per gestire una rete a due velocità, in cui le organizzazioni paramilitari e i sostenitori del governo godono di una connessione globale, mentre la popolazione è confinata in un recinto nazionale. Oggi, l'accesso a Internet in Iran non è più un diritto né un servizio, ma un privilegio politico. Il governo ha introdotto il concetto di Internet Pro o Sim bianche. Si tratta di un sistema di liste di utenti autorizzati, gestito dal Consiglio supremo del cyberspazio in collaborazione con il ministero dell'Intelligence e i Pasdaran (Irgc). Il primo livello (Elite) del sistema comprende funzionari governativi, organi di stampa di regime e aziende collegate all'Irgc. Queste utenze ricevono credenziali che consentono di aggirare i filtri. Possono accedere a X, Instagram e YouTube per diffondere la propaganda di Stato. Il secondo livello (Professionale) è composto da accademici e operatori di settori economici strategici che hanno accesso a un Internet controllato per scopi di ricerca o transazioni internazionali, sotto stretto monitoraggio. Al terzo livello (Popolazione) si trova il resto del Paese, che è collegato alla National information network (Nin), l'Intranet nazionale che ospita solo app domestiche, servizi bancari locali e siti governativi. Nel sistema, ogni utente è mappato al proprio livello tramite l'identificativo della sua Sim. Quando un utente iraniano del livello Popolazione tenta di contattare un Ip estero, gli instradatori gestiti dalla Telecommunication infrastructure company (Tic) ignorano la sua richiesta o la reindirizzano verso server interni. Il meccanismo non si basa solo sul controllo da parte di Tic del sistema di traduzione dei nomi dei siti esteri in indirizzi di rete (il Dns), ma su tecniche di Deep packet inspection (Dpi). Il sistema Dpi di Tic, installato sui border router che segnano il confine tra lo spazio di rete iraniano e quello internazionale, analizza ciascun pacchetto di dati in transito. Se rileva l'uso di protocolli crittografati tipici delle Vpn (come Tls), la connessione viene strozzata o interrotta. Sui dati in chiaro, il sistema Dpi agisce in modo bidirezionale. Prima individua e filtra i contenuti sfavorevoli al regime; poi modifica i pacchetti di risposta provenienti da siti esteri. Al contempo, permette alle organizzazioni di regime (appartenenti ai livelli Elite o Professionale) di iniettare contenuti sul web globale, mantenendo una facciata di normalità sui social media internazionali.

La comunità internazionale si trova in una posizione di impotenza per tre ragioni. Anzitutto, il regime ha nazionalizzato l'infrastruttura. Avendo il controllo fisico sui cavi e sui gateway d'ingresso (Ixp), l'Iran può decidere chi entra e chi esce dai propri confini digitali. Non esiste un pulsante esterno per riattivare le connessioni Internet provenienti da un altro Stato e bloccate al confine senza violare la sovranità territoriale. Poi, c'è la relativa inefficacia delle sanzioni che limitano l'accesso alle tecnologie Dpi occidentali. L'Iran sta sviluppando una propria industria di sorveglianza interna, rendendosi meno dipendente (e quindi meno influenzabile) dai giganti occidentali. Infine, c'è il cosiddetto dilemma dei satelliti. La distribuzione di telefoni satellitari è ostacolata dalle tecnologie di disturbo del segnale che il regime impiega nelle aree urbane. In conclusione, il modello iraniano del 2026 è un pericoloso precedente. Dimostra che una dittatura non ha bisogno di spegnere la luce per restare al potere; le basta decidere chi può vedere e chi deve restare al buio. La frammentazione della realtà che ne deriva impedisce alla popolazione di coordinarsi, mentre consente ai sostenitori di continuare a operare sulla Rete globale.

DEEP PACKET INSPECTION

È una tecnica che permette a chi controlla una rete di guardare dentro i pacchetti di dati che la attraversano, invece di limitarsi a verificarne provenienza e destinazione. In questo modo si possono riconoscere protocolli, applicazioni, contenuti e perfino tentativi di aggirare la censura, come l'uso di Vpn o connessioni cifrate sospette. Il punto decisivo è che non si tratta solo di bloccare l'accesso, ma di selezionarlo, rallentarlo, manipolarlo. È proprio questa granularità a trasformare la rete in uno strumento di governo politico, più che in una semplice infrastruttura tecnica

* presidente del Consorzio interuniversitario nazionale per l'informatica (Cini)

paper

La nuova deterrenza che corre nei fondali

JOEL COITO
military fellow presso presso il Dipartimento Difesa e Sicurezza del Csis

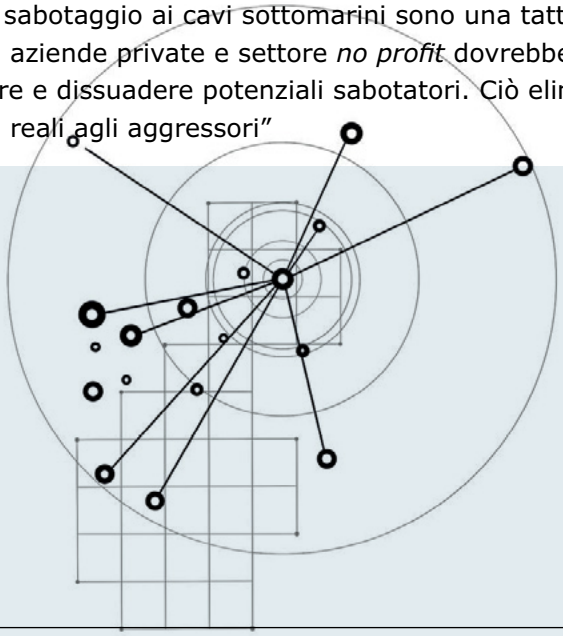
I cavi sottomarini sono essenziali per trasmettere dati e connettere i mercati internazionali. Oltre il 95% dei dati, e 10mila miliardi di dollari in transazioni finanziarie giornaliere, viaggiano a livello globale attraverso 1,5 milioni di chilometri di cavi sottomarini. L'importanza economica e l'utilità dei cavi sottomarini, sia per i governi sia per i cittadini privati, li rendono un bersaglio attraente, e vulnerabile, per attori statali e non statali, qualcosa che precedenti lavori del Csis hanno definito il "ventre molle dell'economia mondiale". Incidenti di alto profilo, tra cui il sabotaggio dei gasdotti Nord Stream 1 e 2, e distinti episodi di danneggiamento di cavi nel mar Baltico causati dal trascinamento delle ancore delle navi di proprietà cinese Newnew Polar Bear e Yi Peng 3, hanno messo in evidenza questa vulnerabilità in modo eclatante. I leader governativi se ne stanno accorgendo e la necessità di una maggiore sicurezza dei cavi è dimostrata dalla creazione da parte della Nato di una Critical undersea infrastructure network e di un Maritime centre for the security of critical undersea infrastructure. Allo stesso tempo, giganti tecnologici come Amazon, Google, Meta e Microsoft hanno effettuato investimenti sostanziali in progetti di cavi sottomarini per aumentare la ridondanza e soddisfare le esigenze di connettività e capacità associate alla crescita *record* dei *data center* e dell'infrastruttura di intelligenza artificiale.

Permane una serie di sfide per la protezione dei cavi sottomarini. In primo luogo, la maggior parte dei danni fisici ai cavi sottomarini è accidentale: di solito il risultato di ancoraggi o della pesca commerciale, e talvolta dovuto a pericoli naturali come terremoti o tsunami. Quando vi sono prove di danni intenzionali (taglio dei cavi o attacchi alle stazioni di approdo dei cavi) i commentatori hanno deplorato le deboli protezioni in tempo di pace offerte dall'attuale regime dei trattati internazionali, sanzioni "drammaticamente inadeguate" e "lacune" nell'azione penale che hanno consentito a soggetti ostili di sottrarsi a una reale responsabilità.

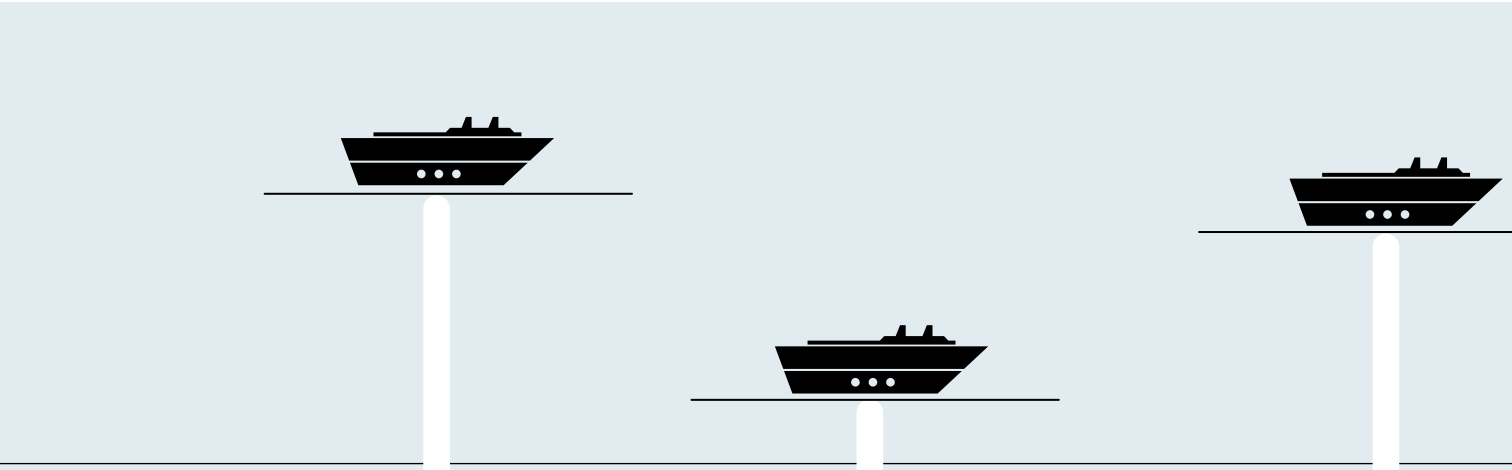
Inoltre, i trattati internazionali che disciplinano i cavi sottomarini sono datati. Il trattato di riferimento del 1884 sui cavi sottomarini, la Convenzione per la protezione dei cavi telegrafici sottomarini, potrebbe beneficiare di emendamenti volti a calibrare meglio le sanzioni rispetto ai danni causati dal danneggiamento intenzionale dei cavi. Ma grandi potenze, tra cui Cina e Russia (entrambe ampiamente accusate di aver danneggiato intenzionalmente cavi negli ultimi anni), difficilmente parteciperebbero a un simile negoziato o rispetterebbero un regime convenzio-

Si propone in queste pagine, per gentile concessione del Center for Strategic and International Studies, con traduzione integrale di Airpress, il report "Protecting Subsea Cables: Detect to Deter, Sue to Secure", consultabile su www.csis.org.

“Sebbene rari, gli attacchi di sabotaggio ai cavi sottomarini sono una tattica attraente per attori statali e non statali. Governi, aziende private e settore *no profit* dovrebbero sfruttare tecnologie all’avanguardia per individuare e dissuadere potenziali sabotatori. Ciò eliminerebbe la plausibile negabilità e imporrebbe costi reali agli aggressori”

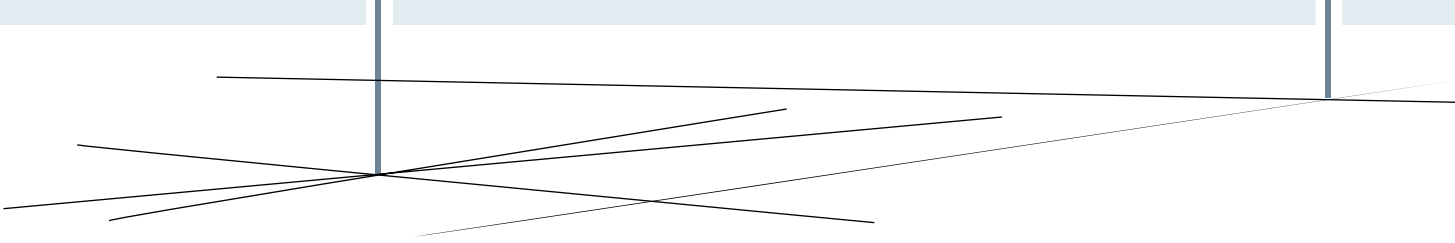


nale aggiornato. Anche quando esiste la volontà politica, il meccanismo dei negoziati internazionali procede lentamente e spesso richiede una legislazione nazionale per produrre effetti pratici.
Di conseguenza, il modo migliore per proteggere i cavi sottomarini nel breve periodo è fare luce sulle attività dei soggetti ostili. Questo può essere realizzato da governi e società private già ora, anche in assenza di un nuovo trattato o di una legislazione nazionale. Sebbene la convenzione del 1884 abbia resistito alla prova del tempo, servono più strumenti per ottenere deterrenza: danno reputazionale per gli operatori navali, identificazione pubblica e stigmatizzazione degli attori responsabili e degli Stati di bandiera inadempienti, e sanzioni finanziarie incorporate quando le compagnie di assicurazione marittima abbandonano le navi sospette o forniscono copertura solo a premi molto elevati. Ma come? Utilizzando gli stessi strumenti che stanno determinando la necessità di un maggior numero di cavi sottomarini (IA, applicazioni quantistiche e sensori avanzati) per costruire un quadro in tempo reale del dominio marittimo ed eliminare la plausibile negabilità dei soggetti ostili. Anche le soluzioni private sono sottoutilizzate. Quando si verificano danni intenzionali ai cavi sottomarini, i proprietari dei cavi dovrebbero chiedere risarcimenti e sentenze dichiarative di illegalità per favorire la deterrenza.
Una sfida ricorrente nell’applicazione del diritto marittimo è la tirannia della distanza. Tradizionalmente, i Paesi cercano di ottenere consapevolezza del dominio marittimo su vasti oceani combinando gli *input* di singole navi, aeromobili e attività di Intelligence. Trattandosi di un’operazione costosa, questa è in larga misura prerogativa dei Paesi ricchi dotati delle forze navali e degli apparati di Intelligence più capaci. Ma le tecnologie di frontiera stanno fornendo sia al settore pubblico sia a quello privato strumenti per monitorare ampi spazi marittimi a costi ragionevoli. Come ha osservato David Brewster del National security college presso l’Australian national university, queste “nuove tecnologie offrono l’opportunità di democratizzare l’accesso alle informazioni” e aiutano i Paesi più piccoli a monitorare meglio le proprie acque.
La democratizzazione dei dati marittimi favorisce un mercato privato innovativo. I satelliti commerciali a basso costo hanno “portato gran parte degli oceani sotto osservazione regolare”, e insiemi di dati un tempo impenetrabili alimentano ora visualizzazioni in tempo reale attraverso IA, *machine learning* e analisi predittiva. Alcune aziende raccolgono tramite



crowdsourcing dati del Sistema di identificazione automatica (Ais), sebbene una recente e attenta analisi rilevi la vulnerabilità dell'architettura aperta dell'Ais allo *spoofing* e all'*hacking*, e le navi cinesi abbiano ripetutamente eluso l'Ais, oppure aggregano dati provenienti da reti di navi aderenti per supportare servizi di Intelligence marittima all'avanguardia. Anche il settore *no profit* ha svolto un ruolo-chiave nello sviluppo di tecnologie per la protezione degli oceani. Skylight, basata presso Ai2, un'organizzazione *no profit* focalizzata sullo svolgimento di attività di IA per il bene comune, orienta le immagini satellitari verso comportamenti sospetti delle navi e sfrutta strumenti di IA per sostenere la conformità e applicare le norme in ambito marittimo. L'organizzazione *non profit* Global fishing watch utilizza tecnologie ad accesso aperto, insiemi di dati e visualizzazioni cartografiche per creare informazioni utilizzabili al fine di contribuire a fermare attività marittime illecite, tra cui la pesca illegale e i dragaggi clandestini. Questi stessi strumenti possono essere usati per identificare rapidamente anomalie navali indicative di sabotaggio dei cavi sottomarini, tra cui permanenze prolungate sopra infrastrutture critiche, operazioni "oscure" con Ais spento e dispiegamento di attrezzature specializzate vicino ai cavi sottomarini. Sia il settore privato sia quello pubblico possono quindi mettere in luce tentativi di attacco ai cavi sottomarini e favorire una "deterrenza tramite rilevamento".

Sebbene i governi non abbiano più il monopolio degli strumenti informativi marittimi, continueranno a essere un cliente primario e un motore di tale tecnologia. Per esempio, la Futures development and integration directorate della Guardia costiera degli Stati Uniti ha recentemente pubblicato una richiesta di informazioni per valutare e sfruttare tecnologie di frontiera al fine di spostare il tradizionale paradigma della consapevolezza del dominio marittimo verso il dominio marittimo dominante (Mdd). La differenza è più che semantica: la visione della Guardia costiera per l'Mdd accoppierebbe gli *input* marittimi tradizionali provenienti da cutter, piccole imbarcazioni e aeromobili con sensori multidominio (aria, spazio, superficie e costa) e sfrutterebbe tecnologie rivoluzionarie per fornire agli operatori un quadro completo delle minacce. Quella che la Guardia costiera chiama "*pipeline* dal rilevamento all'azione" è esattamente la capacità di rilevamento delle minacce in tempo reale necessaria per fermare i danni ai cavi sottomarini (intenzionali o meno) prima che si verifichino.

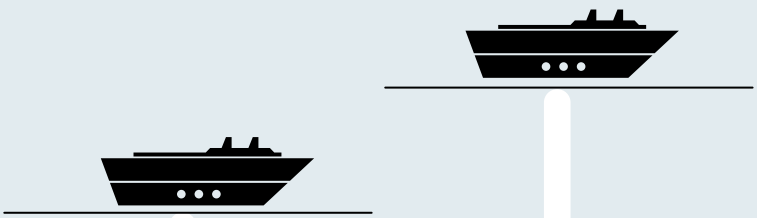


DETERRENZA TRAMITE RILEVAMENTO **Se un attore ostile sa di poter essere individuato, tracciato e reso pubblicamente riconoscibile mentre si avvicina a un cavo sottomarino, il costo dell'azione cambia prima ancora che intervengano navi o tribunali. La deterrenza nasce quindi dalla perdita della plausibile negabilità. In un dominio dove il sabotaggio si maschera spesso da incidente, rendere visibili *pattern* sospetti, rotte anomale e comportamenti oscuri significa trasformare l'informazione in una forma preventiva di protezione.**
•

PRESENZA COSTRUTTIVA **È una dottrina giuridica del diritto marittimo che consente di estendere la presa di uno Stato su condotte avvenute fuori dalle sue acque sovrane quando producono un danno concreto e diretto ai suoi interessi. Applicata ai cavi sottomarini, diventerebbe uno strumento molto importante contro chi taglia o danneggia infrastrutture in alto mare contando proprio sulla distanza dalla giurisdizione costiera.**
•

MARITIME DOMAIN DOMINANCE **La formula segna un salto concettuale rispetto alla più classica *maritime domain awareness*. Non basta più sapere che cosa accade in mare. L'obiettivo diventa fondere sensori, piattaforme, dati e analisi in una *pipeline* capace di trasformare rilevamento, attribuzione e risposta in un flusso quasi continuo. Per la sicurezza dei cavi significa passare da una postura reattiva a una capacità di intercettare per tempo anomalie e permanenze sospette prima che si traducano in sabotaggio.**
•

Né le nuove tecnologie dovrebbero sostituire la condivisione delle informazioni già esistente a livello pangovernativo o intergovernativo. Negli Stati Uniti, il processo Maritime operational threat response rimane un meccanismo di coordinamento collaudato ed efficace per consentire all'apparato interagenzia statunitense di rispondere a minacce marittime complesse, compresi i tentativi di distruggere le infrastrutture sottomarine. Analogamente, il programma Critical maritime routes dell'Unione europea per lo sviluppo delle capacità facilita il coordinamento interagenzia e la condivisione di informazioni tra enti civili e militari. Questi meccanismi di condivisione delle informazioni rafforzano la sicurezza marittima e sono in corso sforzi per modernizzare e integrare meglio fonti di Intelligence e altri dati al fine di rafforzare i risultati in termini di rilevamento e applicazione delle norme. Infine, la continua dimostrazione da parte dei governi di capacità di Intelligence raffinate, come la raccolta di Signal intelligence (Sigint) che ha portato all'individuazione di Osama bin Laden, dovrebbe indurre cautela negli attori statali e non statali che intendano sponsorizzare o realizzare attacchi ai cavi sottomarini.
Un migliore rilevamento di questi attacchi è necessario (ma non sufficiente) per una protezione completa dei cavi. Come affermato in precedenti ricerche del Csis, anche la deterrenza mediante punizione (*deterrence by punishment*) ha un ruolo da svolgere. A prima vista, il diritto statunitense offre opzioni punitive limitate per il danneggiamento volontario di un cavo sottomarino: un reato minore, fino a due anni di carcere e una multa fino a cinquemila dollari. Ma prevede anche rimedi privati e rileva esplicitamente che le sanzioni penali non impediscono un'azione per il risarcimento dei danni. Molto è stato scritto per documentare le varie sfide legate alla punizione degli attacchi ai cavi sottomarini, tra cui strumenti internazionali datati, la proprietà consortile dei cavi e cavi che attraversano più giurisdizioni. Ma le soluzioni private sono uno strumento sottoutilizzato per dissuadere i soggetti ostili, ed è tempo che i proprietari dei cavi adottino un orientamento all'azione nelle aule giudiziarie.
Google offre un esempio istruttivo. Nel novembre 2025, il gigante tecnologico ha presentato una causa in un tribunale federale contro Lighthouse, un'organizzazione criminale con sede in Cina che fornisce *software* di *phishing* e supporto a truffatori *online*. Google sostiene che Lighthouse abbia creato siti *web* falsi che includevano loghi di Google e prendevano di mira le loro vittime in oltre 120 Paesi. Google ha



presentato la causa pur non conoscendo le identità degli imputati, indicati come "Does 1–25", che rimangono in Cina. In una recente intervista con *Npr*, la *general counsel* di Google, Halimah DeLaine Prado, ha ammesso candidamente che l'obiettivo della causa era la "deterrenza" piuttosto che arrivare al processo (nello specifico, una sentenza dichiarativa secondo cui gli atti fraudolenti erano illegali). In breve, Google cerca di ottenere soluzioni private contro convenuti stranieri; potenzialmente oltre la portata giurisdizionale dei tribunali statunitensi; per danni "incalcolabili" subiti da vittime diffuse e geograficamente diversificate; al fine di dissuadere piuttosto che condannare gli autori. Sebbene la frode *online* sia sostanzialmente diversa dal sabotaggio dei cavi sottomarini, i quattro elementi fondamentali del caso elencati sopra valgono per entrambi. La causa di Google fornisce una tabella di marcia per i proprietari di cavi che cercano di dissuadere il danneggiamento dei cavi sottomarini e aumentare la consapevolezza pubblica del problema, anche se quei soggetti ostili non dovessero mai comparire in un'aula di tribunale statunitense.

In realtà, il caso giurisdizionale per la responsabilità civile potrebbe essere più solido nel contesto dei cavi sottomarini. Il professor James Kraska e la comandante Elizabeth Hutton dello Us Naval war college hanno sostenuto in modo persuasivo che la dottrina della presenza costruttiva (una dottrina giurisdizionale ben consolidata nel diritto marittimo internazionale, da tempo utilizzata nei casi di salvataggio e "inseguimento a caldo") dovrebbe applicarsi anche in caso di danneggiamento intenzionale dei cavi sottomarini. Il nucleo di questa dottrina offre agli Stati costieri una soluzione contro le navi che commettono atti illeciti in acque internazionali causando danni concreti allo Stato costiero, e ostacola i tentativi dei soggetti ostili di eludere la giurisdizione evitando le acque sovrane. I proprietari di cavi sottomarini dovrebbero perseguire questa linea argomentativa che, in caso di successo, consentirebbe a un tribunale di esercitare la giurisdizione su una nave che taglia cavi in acque internazionali perché la sua azione nefasta "è materialmente e direttamente collegata al danno o pregiudizio di porzioni della [infrastruttura critica sottomarina] che si trovano fisicamente nel mare territoriale di quello Stato costiero di collegamento".

Vi sono inoltre promettenti sviluppi legislativi e regolatori per proteggere meglio i cavi sottomarini e rafforzare la responsabilità legale per i danni intenzionali. Nel settembre 2025, la Camera dei rappre-

PLAUSIBILE NEGABILITÀ **È il vantaggio politico e operativo di chi compie un'azione ostile in modo tale da poter negare credibilmente il proprio coinvolgimento. Nel caso dei cavi sottomarini è un fattore centrale, perché il danno può sembrare frutto di maltempo, errore umano o incidente tecnico. Per questo la raccolta di prove in tempo reale conta tanto. Se si riesce a mostrare con continuità la posizione di una nave, lo spegnimento dell'Ais, il trascinamento anomalo o la permanenza sopra un tracciato sensibile, la negabilità si restringe.**
•

SENTENZA DICHIARATIVA **Non serve necessariamente a ottenere subito un risarcimento materiale o a portare in carcere i responsabili. Serve, prima di tutto, a fissare in sede giudiziaria che un comportamento è illecito. In casi transnazionali e opachi come quelli legati ai cavi sottomarini, questa funzione è tutt'altro che secondaria. Una decisione del genere costituisce un precedente, rende più chiara la responsabilità, indebolisce la narrativa dell'incidente casuale e può produrre effetti indiretti molto concreti su reputazione, assicurazione, accesso ai porti e rapporti commerciali.**
•

BANDIERA INADEMPIENTE **Nel diritto marittimo lo Stato di bandiera ha il compito di vigilare sul rispetto degli obblighi internazionali da parte delle navi che lo rappresentano. Quando non esercita davvero questo controllo, o lo esercita in modo puramente formale, diventa di fatto un facilitatore dell'opacità. Parlare di bandiera inadempiente significa quindi spostare l'attenzione dalla sola nave al sistema di responsabilità che la copre.**
•

sentanti degli Stati Uniti ha approvato l'Undersea cable control Act, che mira a impedire agli avversari stranieri di acquisire beni necessari a sostenere la costruzione, la manutenzione o l'operatività di progetti di cavi sottomarini. Due mesi dopo, al Senato è stato presentato lo Strategic subsea cables Act of 2025, che rafforzerebbe le sanzioni per il danneggiamento dei cavi sottomarini e richiederebbe al presidente di imporre sanzioni contro individui stranieri che abbiano danneggiato intenzionalmente cavi sottomarini in fibra ottica. Questi sviluppi legislativi, insieme all'attività regolatoria della Federal communication commission, focalizzata sulla sicurezza nazionale, in materia di licenze per l'approdo dei cavi sottomarini, evidenziano una crescente volontà politica di prevenire e punire meglio i danni intenzionali ai cavi; sforzi lodevoli e tempestivi. Rafforzare ulteriormente la protezione delle infrastrutture sottomarine dovrebbe essere una priorità *bipartisan*.

Un attacco a un cavo sottomarino può interrompere istantaneamente le comunicazioni globali e l'attività economica. Sebbene rari, gli attacchi di sabotaggio ai cavi sottomarini sono una tattica ibrida attraente che Cina, Russia e altri attori statali e non statali possono impiegare per imporre costi economici, interrompere servizi e seminare disordini popolari. Governi, aziende private e settore *no profit* dovrebbero sfruttare tecnologie all'avanguardia che hanno democratizzato i dati marittimi, tra cui IA, analisi predittiva e immagini satellitari orientate da segnali, per individuare e dissuadere potenziali sabotatori. La deterrenza tramite rilevamento elimina la plausibile negabilità e impone costi reali che vanno dal danno reputazionale all'aumento dei premi assicurativi. Inoltre, le azioni legali contro chi danneggia intenzionalmente i cavi sottomarini sono un meccanismo di deterrenza sottoutilizzato. Di conseguenza, i proprietari dei cavi dovrebbero perseguire con determinazione soluzioni nelle aule giudiziarie. Chiedendo risarcimenti e sentenze dichiarative di illegalità, questi proprietari gettano una luce più intensa sulla minaccia del danneggiamento dei cavi sottomarini anche quando un convenuto non può essere portato davanti a un tribunale statunitense. Negli Stati Uniti sono in corso promettenti iniziative legislative e regolatorie per ridurre le minacce ai cavi sottomarini e sanzionare i soggetti ostili. Nel frattempo, rilevare per dissuadere e fare causa per mettere in sicurezza sono strumenti che possono e dovrebbero essere utilizzati.

La sicurezza cibernetica è strettamente legata alla dimensione subacquea, dove le infrastrutture digitali sono parte integrante della superficie d'attacco. Le minacce riguardano anche le intrusioni nei sistemi di controllo, l'esfiltrazione di dati e possibili forme di sabotaggio remoto. I punti più sensibili restano le stazioni di approdo e le reti di gestione, sempre più esposte alle tattiche ibride

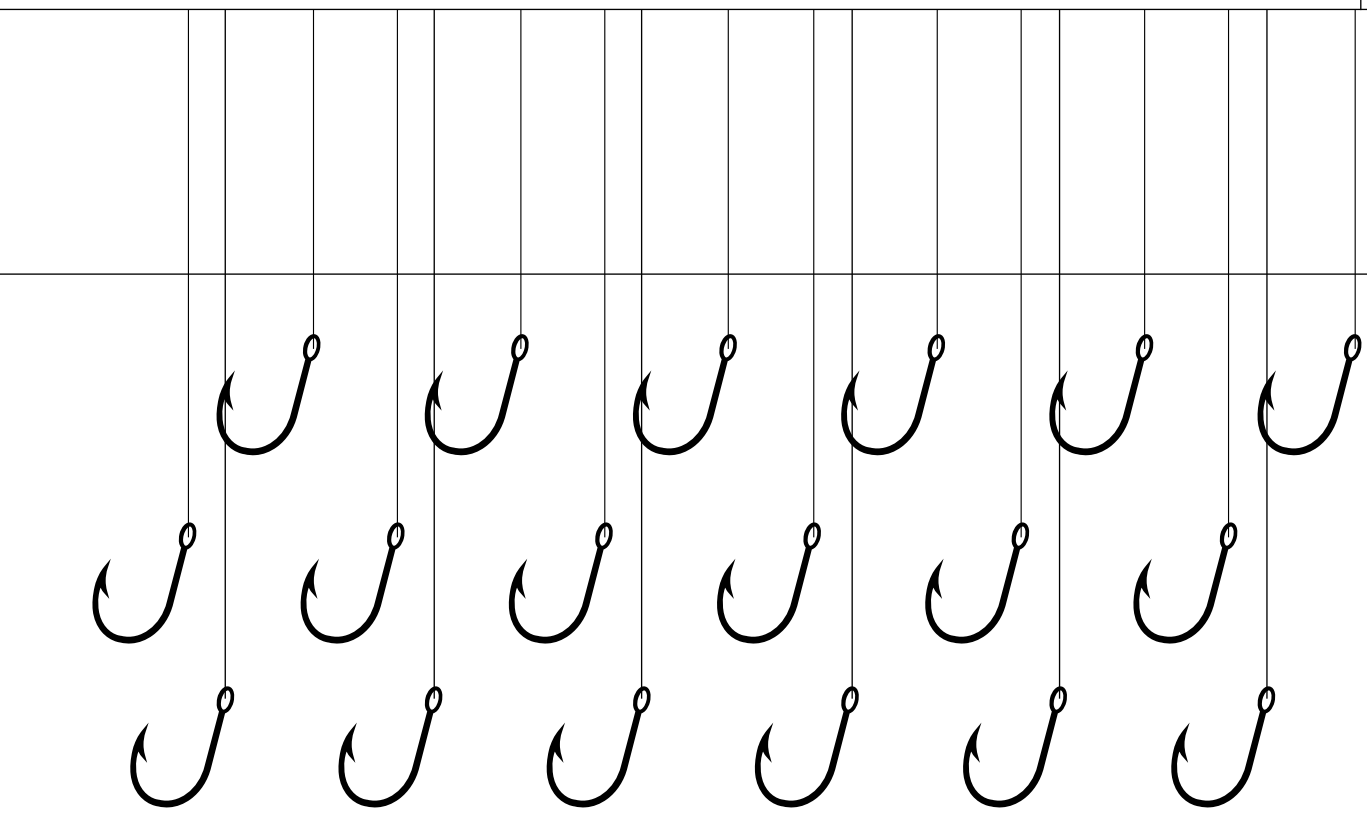
Quanta cyber-security passa dai cavi

MARCO BRACCIOLI
co-director Cybersec di Fondazione Icsa

Così come altri mondi anche l'ambiente subacqueo si sta fortemente antropizzando e in virtù di un confronto ibrido crescente tra potenze globali e regionali diventa terreno di scontro e confronto tra minaccia e deterrenza. Gli obiettivi son presto detti, a esclusione di quelli prettamente militari: piattaforme *offshore oil & gas*, reti di distribuzione ed alimentazione elettrica, fibre ottiche, campi eolici *offshore* (fissi e flottanti) e piattaforme innovative per le energie rinnovabili. La procedura di rilevamento danni segue un percorso ben preciso: rilevare e confermare il danno, localizzare, accedere all'area per l'investigazione, limitarne le conseguenze, reagire in emergenza e ripristinare. Fin qui tutto giusto, ma come prevedere o monitorare queste infrastrutture critiche? Per esempio, nel caso del gas le misure sono ben dettagliate dalla copertura anticorrosione, fino alla stesura in sottomarina di appesantimenti anti-flottaggio, mentre la pressione, la temperatura e il tasso di flusso vengono continuamente monitorati digitalmente attraverso un sistema di controllo remoto.

Secondo uno studio recente esistono globalmente 2,7 milioni di chilometri di cavi per dati ed energia e 1,2 milioni di chilometri di *pipeline oil & gas*. Il mercato *underwater* è stimato al 2050 in 400 miliardi di euro, oltre 30 miliardi in valore di soluzioni innovative e 10 miliardi in soluzioni di comunicazione subacquea. Soprattutto la spesa per l'innovazione riguarderà *data collection* e analisi, droni subacquei per monitoraggio e riparazione infrastrutture, nodi *multi-sensor* con *modem* acustici, *gateway* subacquei integrati anche alle reti *telco* e spaziali. Le principali necessità di comunicazione sia per il settore civile (infrastrutture critiche) che per quello militare (operazioni multi-dominio) sono: comunicazioni strategiche per unità subacquee che operano in profondità, scambio di dati ad alta velocità in emersione, comunicazioni tattiche bi-direzionali e a bassa latenza con unità subacquee in tutti gli scenari operativi, monitoraggio e controllo delle infrastrutture critiche sottomarine e Internet of underwater things. La sfida tecnologica è sicuramente legata alla trasmissione subacquea che può essere di tre tipi.

INTERNET OF UNDERWATER THINGS L'espressione descrive reti di sensori, *modem* acustici, *gateway* e piattaforme autonome distribuite sotto la superficie del mare e capaci di scambiarsi dati in modo continuo. È l'equivalente subacqueo dell'Internet delle cose, ma in un ambiente molto più ostile, dove comunicare è difficile e costoso. Il suo valore strategico sta nel fatto che permette di trasformare il fondale da spazio opaco a spazio monitorato, collegando infrastrutture energetiche, cavi, droni e sistemi di allerta dentro una stessa architettura digitale.



La prima è la radiofrequenza che attraversa facilmente i confini aria/acqua e non è influenzata da torbidità, salinità e gradienti di pressione. Inoltre è immune al rumore acustico, ha elevata larghezza di banda (fino a 100 Mb/s) a distanza molto ravvicinata ma è sensibile alle interferenze elettromagnetiche con una portata limitata in acqua, prediligendo quelle poco profonde. Successivamente, l'acustica è una tecnologia collaudata, con distanze fino a circa 20 chilometri, ma che presenta forti riflessioni e attenuazione durante la trasmissione attraverso il confine acqua/aria e scarse prestazioni in acque poco profonde. Inoltre, viene influenzata negativamente da torbidità, rumore ambientale, salinità e gradienti di pressione con una larghezza di banda limitata (qualche b/s fino a 20 kb/s).
Infine, l'ottica che presenta larghezza di banda ultraelevata (nel ordine di gigabit al secondo), ma non attraversa facilmente il confine acqua/aria, è sensibile a torbidità, particelle e incrostazioni marine e richiede una linea di vista diretta, un allineamento preciso dei nodi con raggio d'azione molto breve.

Venendo invece alla parte *cyber* relativa alle minacce ai cavi sottomarini, esse si possono condensare in macroaree: esfiltrazione di dati, dirottamento e presa di controllo degli *unmanned asset* per azioni malevole, *fishing*, attacco ai *data center* sottomarini e alle *pipeline*, interruzione delle comunicazioni. Un recente studio dell'International cable protection committee, tra il 2010 e il 2024, definisce che circa il 42% dei guasti ai cavi sottomarini è stato causato dall'attività di pesca e dall'ancoraggio, mentre un ulteriore 44% è in parte attribuito a sabotaggi volontari.
L'Unione europea ha istituito intorno alla struttura dei cavi sottomarini un quadro di sicurezza costituito dalle direttive Cer e Nis 2. La prima, in particolare, richiama gli Stati membri a adottare misure per rafforzare la resilienza dei soggetti critici e la protezione delle infrastrutture critiche. La seconda, invece, richiede ai soggetti che sono fornitori di infrastrutture e servizi digitali che gestiscono cavi sottomarini di proteggere i loro sistemi informatici e di rete, nonché il loro ambiente fisico da qualsiasi evento (*all-hazards*). È

stata inoltre pubblicata la Raccomandazione 2024/779 della Commissione europea per migliorare la sicurezza e la resilienza dei cavi sottomarini attraverso la mappatura di quelli esistenti (con aggiornamento almeno annuale), una valutazione di rischi, vulnerabilità e dipendenze, con specifica attenzione alla *supply chain*. Anche in tale logica si inserisce la definizione di un Cable security toolbox che definisca misure di mitigazione dei rischi, soprattutto rispetto ai fornitori ad alto rischio, lo scambio regolare di informazioni su incidenti, awareness e pratiche applicate e l'impiego di soluzioni innovative per l'individuazione e la deterrenza delle minacce contro le infrastrutture dei cavi sottomarini. Sempre più episodi recenti nel Baltico, nel Mediterraneo e nel mar Rosso sono sospettati di essere sabotaggi deliberati contro cavi di comunicazione o gasdotti, difficili da attribuire ma compatibili con operazioni di *seabed warfare*. Attori statali possono usare sottomarini, mini-sottomarini, Auv e navi civili di facciata per tagliare o danneggiare i cavi in punti strategici, creando interruzioni mirate o dimostrative nell'ambito della guerra ibrida. Oltre al taglio, una minaccia chiave è l'intercettazione clandestina del traffico: capacità militari profonde consentono di installare sonde o dispositivi lungo il cavo o nei ripetitori per leggere o deviare i flussi. In parallelo, campagne di *cyber*-spionaggio contro gli operatori mirano a ottenere accesso alle reti di gestione per monitorare o copiare comunicazioni sensibili senza interrompere il servizio. I punti più esposti sono le stazioni di approdo: qui convergono alimentazione, apparati ottici, *router* e sistemi Scada/Noc, spesso raggiungibili via rete dalle sedi centrali. Le vulnerabilità in questi sistemi possono permettere ad un attore di alterare configurazioni, spegnere segmenti di cavo, manipolare instradamenti o preparare sabotaggi fisici più precisi. I principali vettori di rischio sono: attacchi ai sistemi di controllo e supervisione della rete (con impatti sul bilanciamento e sulla continuità del servizio); sabotaggio fisico del cavo o dei punti di approdo (spesso difficile da attribuire con certezza); dipendenze da *data center*, consorzi e fornitori terzi, che ampliano la superficie d'attacco. Le misure di difesa principali sono: *asset discovery* e mappatura completa delle tratte e dei punti sensibili; centralizzazione dei controlli e monitoraggio continuo dei sistemi di sicurezza; sorveglianza marittima e capacità di risposta rapida, incluse riparazioni e ridondanza di rete; collaborazione tra Stati, Ue e operatori privati (perché la protezione non è solo tecnica ma anche organizzativa e strategica). Per la difesa fisica dei cavi, invece, si va verso una sensoristica sofisticata, che si può aggregare in questo modo: sensori in fibra ottica distribuiti (utili per rilevare vibrazioni, deformazioni e disturbi lungo la tratta); sensori di tensione e *strain* (per intercettare trazioni anomale sul cavo); sensori acustici e vibrazionali nei punti critici (soprattutto vicino agli approdi); sensori perimetrali e Cctv nelle *landing station* (per rilevare accessi o manomissioni fisiche); e, per ultimo vista l'attualità del tema, veniamo a Hormuz e ai cavi che passano nello stretto, questa è davvero la bomba nucleare nelle mani degli iraniani: la vulnerabilità dei cavi sottomarini. Le fonti citano sistemi come Aae-1, Falcon, Gulf Bridge International, Sea-Me-We e Tgn-Gulf tra quelli potenzialmente esposti nell'area. Un danno a questi collegamenti potrebbe rallentare Internet, disturbare le transazioni bancarie, la logistica, la telemedicina e le comunicazioni d'emergenza. In pratica, la crisi di Hormuz sui cavi sottomarini significa una vulnerabilità da guerra ibrida: il danno più probabile non è il collasso totale di internet, ma una degradazione seria e localizzata delle reti con impatti economici e finanziari importanti, e questa è un'altra delle cose che non ci possiamo certo permettere di questi tempi.

GATEWAY SUBACQUEI Sono i nodi che raccolgono, elaborano e instradano i dati provenienti da sensori e sistemi underwater verso reti più ampie, comprese quelle terrestri, telco o satellitari. In pratica fanno da ponte tra il mondo sommerso e quello emerso. La loro importanza cresce perché senza questi punti di raccordo i sensori restano isole separate, utili solo localmente. Con i *gateway*, invece, il monitoraggio dei fondali diventa una capacità integrata, che può sostenere manutenzione, sorveglianza, risposta alle emergenze e persino operazioni multi-dominio.

CHECKPOINT CHARLIE

di Adriano Soi*

Il governo delle crisi
Cisr e Strategia di sicurezza nazionale

Poco più di dieci anni fa una legge ampliò le attribuzioni del Cisr – il Comitato interministeriale per la sicurezza della Repubblica che dal 2007 coadiuva il presidente del Consiglio dei ministri nell'esercizio delle sue responsabilità di vertice politico dell'Intelligence italiana – facendo dello stesso collegio anche la sede politico-istituzionale in cui il premier affronta e gestisce le situazioni di crisi che coinvolgono aspetti di sicurezza nazionale.
La stessa legge prevedeva anche un regolamento che disciplinasse il funzionamento del Cisr in questi casi, testo che però ha visto la luce solo il 6 maggio scorso con la pubblicazione sulla Gazzetta ufficiale. D'ora in avanti il presidente del Consiglio potrà dunque avvalersi del Cisr anche per gestire crisi che presentino profili di sicurezza nazionale.
In sintesi, a questo fine il Cisr ora può: formulare al presidente proposte di indirizzo sulle attività di gestione delle crisi; fornire valutazioni sul quadro informativo e sull'evoluzione della situazione, determinando di conseguenza il fabbisogno conoscitivo; proporre al presidente misure e provvedimenti nonché lo svolgimento di esercitazioni volte a incrementare le capacità operative per gestire situazioni di crisi.
Le disposizioni di dettaglio sono numerose e non è questa la sede per analizzarle diffusamente. Giova invece osservare che il Cisr per la gestione delle crisi è un collegio a geometria molto più variabile rispetto a quella del Cisr "generalista" che – lo ricordiamo – oltre al presidente del Consiglio e, se nominata, all'Autorità delegata, prevede dieci ministri: Esteri, Interno, Difesa, Giustizia, Economia, Imprese e Made in Italy, Ambiente e sicurezza energetica, Agricoltura e sovranità alimentare, Infrastrutture e trasporti, Università e ricerca, nonché il direttore generale del Dis con funzioni di segretario. In sede di gestione delle crisi, invece, questo organico è ora integrato dal titolare della Protezione civile e dal capo del relativo Dipartimento mentre il presidente può convocare anche altri ministri, il sottosegretario di Stato alla presidenza del Consiglio, segretario del Consiglio dei ministri, il consigliere diplomatico e quello militare, i direttori di Aise e Aisi nonché altre autorità civili e militari la cui presenza sia ritenuta utile in relazione alla natura della crisi. Si può così giungere a un numero di componenti davvero notevole, che nei casi di crisi di sicurezza cibernetica aumenta ancora per l'inserimento del ministro delegato all'Innovazione tecnologica e la transizione digitale e del direttore generale dell'Agenzia per la cybersicurezza nazionale.
D'altra parte, il regolamento consente al presidente del Consiglio di convocare il Cisr anche in una composizione ristretta "ad alcuni dei suoi componenti" e permette così di ridurre molto il collegio, cosa non consentita dalla legge 127 del 2004 sul Cisr "generalista", in cui il numero dei ministri non può essere ridotto.
Ma la novità più rilevante introdotta dal regolamento è l'istituzione della "Strategia di sicurezza nazionale", adottata almeno triennalmente dal presidente del Consiglio su proposta del Cisr, sentito il Copasir. Nel documento l'Esecutivo definirà, alla luce dei fattori di minaccia e di rischio, gli interessi fondamentali per la tutela della sicurezza nazionale. Si tratta, com'è evidente, del recepimento da parte del governo della proposta avanzata nel 2024 dall'onorevole Guerini, presidente del Copasir.
Sia il Cisr per la gestione delle crisi sia la Strategia di sicurezza nazionale sono, sulla carta, due importanti passi avanti per adeguare il Sistema di informazione per la sicurezza della Repubblica alle straordinarie condizioni di politica internazionale che ci troviamo oggi a dover fronteggiare. Il problema, come sempre, è passare dalle parole ai fatti.

STRATEGIA DI SICUREZZA NAZIONALE

È il documento con cui il governo dovrebbe fissare, in modo periodico, quali interessi considera essenziali per la sicurezza del Paese e quali minacce o rischi richiedano priorità politica e amministrativa. Non è un semplice testo programmatico. Se davvero applicata, una strategia di questo tipo serve a coordinare apparati diversi, orientare l'Intelligence, definire priorità operative e collegare crisi, prevenzione e decisione politica dentro una visione comune. Il punto decisivo, quindi, non è tanto scriverla, quanto farne uno strumento reale di indirizzo e non una formula di principio.

* docente di Intelligence e sicurezza nazionale presso la Scuola di Scienze politiche "Cesare Alfieri" di Firenze

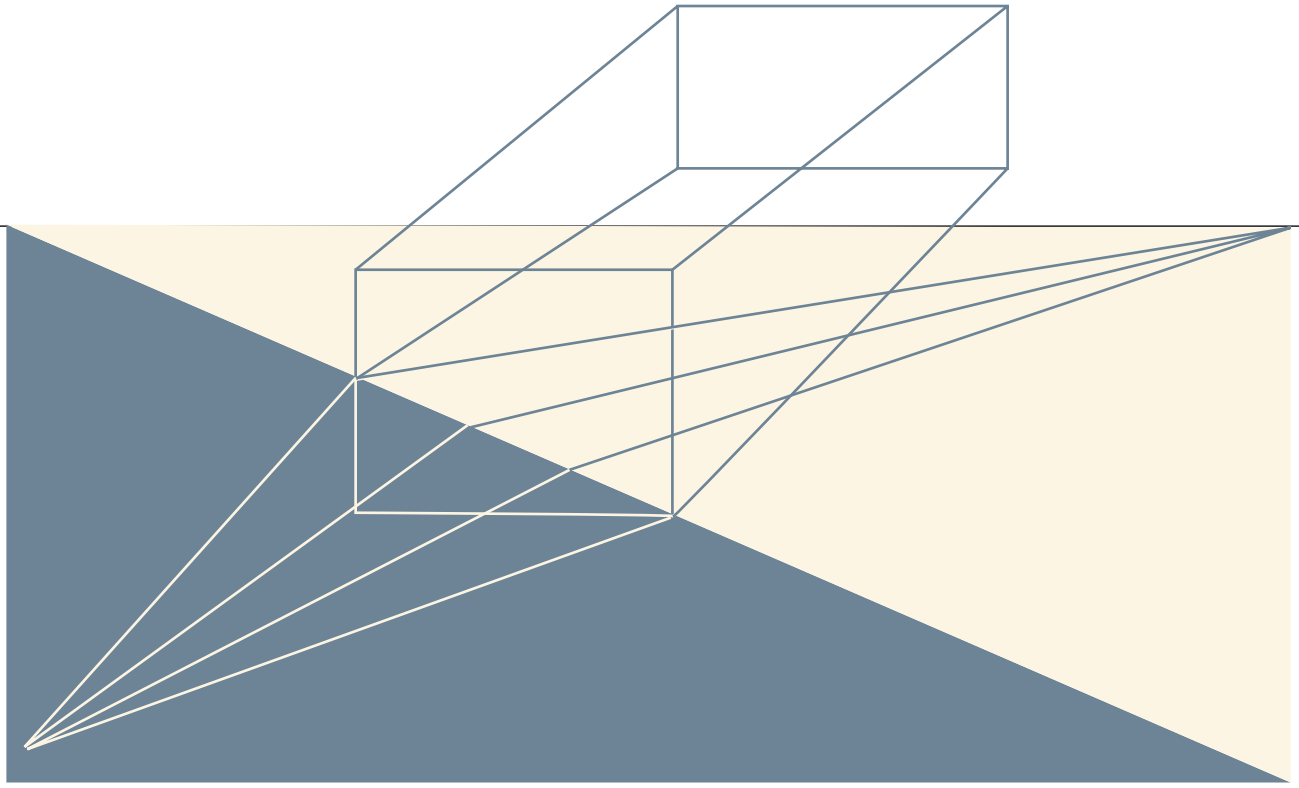
La sicurezza delle infrastrutture sottomarine dipende sempre più dalla capacità di costruire reti di comunicazione e monitoraggio permanenti. La protezione del dominio underwater richiede un'infrastruttura connessa, interoperabile e adattabile, in grado di trasformare il dato in consapevolezza operativa. Per l'Italia, questa trasformazione riguarda la tutela degli asset nel Mediterraneo e la possibilità di convertire competenze tecnologiche in capacità strategica

Il mare ora chiede reti intelligenti

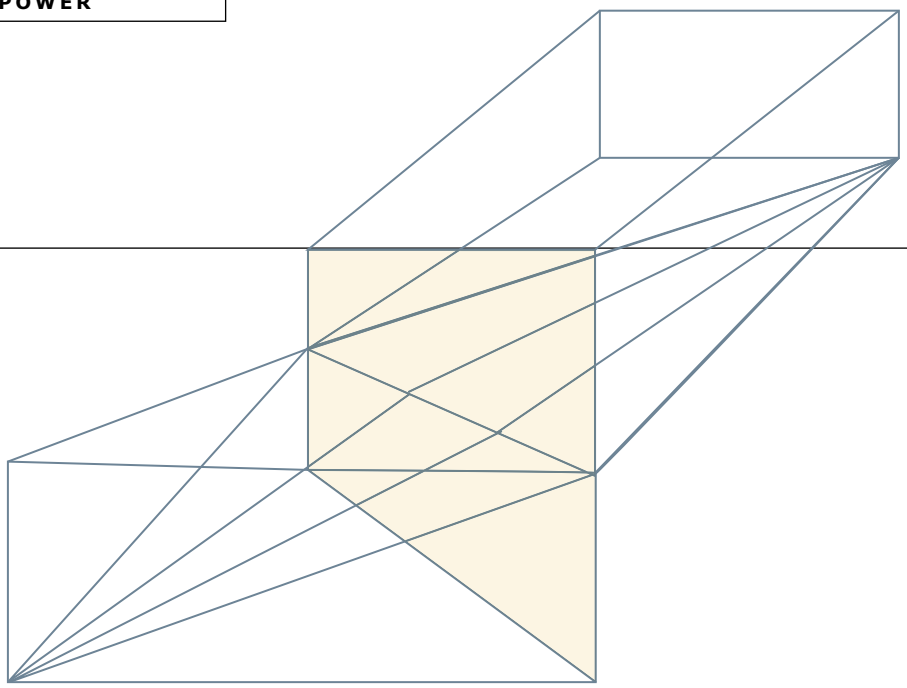
CHIARA PETRIOLI
fondatrice e ceo di WSense

Per decenni il dominio sottomarino è rimasto un ambiente sostanzialmente non connesso. Esistevano *modem* acustici, sistemi in grado di far comunicare due dispositivi tra loro, oppure collegamenti ottici ad altissima velocità, ma limitati da un range che non superava i pochi metri di distanza. Mancava ciò che sulla terra ha cambiato tutto: un'infrastruttura di rete. Non un semplice scambio sporadico di dati, ma una connettività continua, affidabile e interoperabile, capace di mettere in relazione sensori, piattaforme, droni e sistemi distribuiti.
È questo il vero salto tecnologico che oggi sta iniziando a prendere forma nel mondo *underwater*.
Anche il settore della robotica marina ha lavorato per anni senza una rete reale, ma impiegando asset che comunicavano in modo limitato, sistemi incapaci di cooperare su larga scala e piattaforme che parlavano linguaggi diversi. Senza *standard* comuni e senza infrastrutture, era impossibile immaginare un ecosistema intelligente e coordinato. Negli ultimi anni, però, molto è cambiato. La standardizzazione delle comunicazioni sottomarine (sia in ambito Nato sia nei grandi consorzi industriali dell'energia e delle telecomunicazioni) ha finalmente posto le basi per costruire vere reti *underwater*. È un passaggio fondamentale che permetterà di realizzare una vera interoperabilità tra dispositivi differenti e consentire la nascita di infrastrutture distribuite, sicure e scalabili. Oggi siamo nel momento in cui gli *standard* esistono, le capacità industriali anche, tra cui aziende *deep tech* quali WSense al cuore di questa rivoluzione, e si sta aprendo la fase della realizzazione su scala. È una situazione simile a quella che interessò i primi anni delle reti terrestri: la tecnologia è pronta, ma le infrastrutture devono ancora essere dispiegate.
È vero che oggi esistono cavi sottomarini che trasportano dati in tutto il mondo, ma si tratta ancora di *backbone* isolati, non di infrastrutture capaci di creare connettività diffusa nell'ambiente sottomarino circostante. Per questo oggi la sfida è integrare il mondo *wireless underwater* con le dorsali globali delle telecomunicazioni, creando *gateway* capaci di collega-

ADAPTABILITY BY DESIGN L'espressione indica un principio progettuale secondo cui una rete di sorveglianza non deve limitarsi a funzionare bene il giorno in cui viene installata, ma deve nascere già pronta a evolvere insieme alle minacce. Nel dominio *underwater* questo è cruciale, perché droni, sensori e tecniche di intrusione cambiano rapidamente e rendono obsolete le difese statiche. Progettare l'adattabilità significa quindi prevedere aggiornamenti, riconfigurazioni e capacità di apprendimento continuo come parte integrante del sistema, non come correzioni aggiunte in seguito.



re reti subacquee e infrastrutture terrestri. L'obiettivo, in altri termini, è quello di trasformare il mare da ambiente opaco e intermittente a dominio costantemente monitorato e connesso.
Il sabotaggio del Nord Stream ha mostrato in modo evidente quanto siano vulnerabili le infrastrutture sottomarine e quanto il mondo dipenda da ciò che passa sul fondo del mare, dai cavi di telecomunicazione alle pipeline energetiche, passando per le infrastrutture strategiche. Ma soprattutto ha reso chiaro che oggi esistono tecnologie relativamente accessibili (come i droni sottomarini) capaci di operare a profondità sempre maggiori e di rappresentare una minaccia concreta. E questo non è un aspetto secondario. Parliamo di infrastrutture strategiche per i paesi che valgono miliardi, che possono essere minacciate da sistemi dal costo infinitamente inferiore. E mentre le capacità offensive evolvono rapidamente, le infrastrutture di sorveglianza *underwater* sono ancora largamente assenti.
Per questo la priorità non è più soltanto raccogliere dati, ma trasformarli in consapevolezza operativa. Monitorare il fondale non basta, bisogna distinguere un'anomalia naturale da una minaccia reale, riconoscere un drone in avvicinamento e identificare comportamenti sospetti prima che raggiungano un'infrastruttura critica.
Qui entra in gioco l'intelligenza artificiale. I sistemi di nuova generazione devono essere capaci di elaborare localmente le informazioni, apprendere e adattarsi continuamente, un po' come accade nella *cybersecurity*. Non esiste una soluzione definitiva, dal momento che le minacce evolvono costantemente, le infrastrutture di sorveglianza devono essere progettate per evolvere insieme a loro. Un punto fondamentale è che la sicurezza *underwater* non può più essere pensata come un sistema statico. Le minacce stanno cambiando rapidamente: droni sempre più piccoli, autonomi, difficili da rilevare, capaci di operare a profondità e distanze che fino a pochi anni fa erano proibitive. Per questo le infrastrutture di sorveglianza devono nascere già con una logica di adattabilità integrata, una vera *adaptability by design*.
I sistemi del futuro dovranno essere capaci di aggior-



b

narsi e riconfigurarsi nel tempo, imparando a riconoscere nuove tipologie di comportamento e nuove minacce. Non basterà installare sensori sul fondale, ma serviranno reti intelligenti, distribuite, capaci di fondere informazioni provenienti da tecnologie diverse e trasformare il dato grezzo in consapevolezza operativa.
L'evoluzione tecnologica sta andando esattamente in questa direzione. Da una parte cresce l'intelligenza a bordo dei sistemi di monitoraggio; dall'altra stanno migliorando radicalmente le soluzioni per abbattere i consumi energetici, le batterie e le tecnologie per la produzione di energia. Questo consente di immaginare infrastrutture permanenti, droni capaci di operare per lunghi periodi e reti distribuite su larga scala.
Il Mediterraneo può diventare un laboratorio strategico di questa trasformazione. Non solo perché è un mare centrale per le connessioni energetiche e digitali tra Europa, Africa e Medio Oriente, ma perché concentra *asset* industriali, infrastrutture critiche e competenze tecnologiche avanzate. L'Italia, in particolare, dispone di grandi aziende industriali e di un ecosistema *deep tech* che negli ultimi anni ha lavorato sulla frontiera delle comunicazioni e della sensoristica *underwater*.

La sfida, ora, è trasformare questo vantaggio tecnologico in una capacità infrastrutturale reale. Vale a dire, essere tra i primi a costruire reti di monitoraggio e protezione su scala, sviluppando soluzioni che possano poi essere esportate a livello internazionale. Perché sia possibile, serviranno investimenti pubblico-privati per realizzare infrastrutture permanenti di sorveglianza e connettività, esattamente come è avvenuto in passato per le reti terrestri o satellitari. Il punto centrale è che fare attività in mare è estremamente costoso e continuare a operare senza infrastrutture significa ripetere ogni volta lo stesso sforzo senza lasciare capacità permanenti sul territorio. Costruire reti intelligenti *underwater*, invece, vuol dire creare un patrimonio strategico stabile e duraturo.
Per un Paese come l'Italia, al centro del Mediterraneo, questa non è soltanto una questione tecnologica, ma una scelta che riguarda il posizionamento strategico del sistema Paese nel mondo e la capacità di proteggere quella centralità marittima da cui dipendono la nostra connettività e la nostra sicurezza.

GATEWAY UNDERWATER Sono i punti di raccordo che permettono a una rete sottomarina di uscire dal proprio isolamento e collegarsi alle dorsali terrestri o satellitari. Senza questi nodi, i sensori e i droni *underwater* restano confinati in un circuito locale, utile ma incapace di generare vera continuità operativa. Il *gateway* ha quindi una funzione strategica, perché trasforma un insieme di dispositivi dispersi in una infrastruttura capace di scambiare dati, ricevere comandi e alimentare una consapevolezza situazionale più ampia. È il passaggio che rende il mare un dominio realmente connesso.

HACKER

di RANIERI RAZZANTE*

La sicurezza invisibile delle e-mail *tra autenticazione e difesa multilivello*

La posta elettronica costituisce oggi uno dei servizi digitali più critici per la comunicazione tra pubbliche amministrazioni, imprese e cittadini. Attraverso questo canale transitano informazioni operative, documenti sensibili e comunicazioni ufficiali capaci di incidere sulla continuità dei processi. L'*email* rappresenta oggi uno dei principali vettori di attacco, come evidenziato dalle linee-guida dell'Acn dedicate alla configurazione dei sistemi di posta elettronica per l'autenticazione del mittente.
Il funzionamento della posta elettronica si basa sul protocollo Smtp, progettato come meccanismo *store-and-forward* per l'instradamento dei messaggi tra *server*. Il sistema prevede l'interazione tra il Mail user agent (Mua), utilizzato dall'utente per comporre e leggere le *email*, e il Mail transfer agent (Mta), che si occupa della trasmissione dei messaggi tra mittente e destinatario. Tuttavia, la struttura originaria del protocollo non include a oggi meccanismi automatici di autenticazione del mittente né sistemi di protezione del contenuto durante il transito. Questa assenza ha reso possibile l'evoluzione di diverse tecniche di attacco che sfruttano la fiducia implicita nel sistema *email*.
Tra le minacce più diffuse vi è lo *spoofing*, che consiste nella falsificazione dell'indirizzo *email* per far apparire un messaggio come proveniente da una fonte legittima. Il formato dei messaggi *email* distingue infatti tra *envelope-from*, utilizzato per l'instradamento del messaggio tra *server*, e *message-from*, visibile all'utente finale nell'intestazione dell'*email*. Questa separazione consente a un attaccante di manipolare l'indirizzo visualizzato dal destinatario, inducendolo a ritenere autentico un messaggio fraudolento. Il risultato è un aumento del rischio che l'utente compia azioni dannose, come l'apertura di allegati malevoli o la comunicazione di credenziali riservate.
A questa minaccia si affianca il *phishing*, una tecnica di attacco basata sull'invio di messaggi ingannevoli finalizzati ad acquisire dati sensibili. Le *email* di *phishing* sono spesso costruite per generare urgenza, paura o opportunità economiche, inducendo il destinatario a cliccare su *link* malevoli o a inserire informazioni personali. Nelle varianti più avanzate, come lo *spear phishing*, gli attaccanti personalizzano il messaggio sulla base del profilo della vittima, aumentando l'efficacia dell'attacco. Ad oggi è unanime l'analisi sull'enorme diffusione di questa tecnica nel mondo del *cyber-crime*.

SPEAR PHISHING

È una forma di *phishing* molto più mirata rispetto ai messaggi fraudolenti inviati in massa. L'attaccante costruisce l'email partendo da informazioni reali sulla vittima o sulla sua organizzazione, come ruolo, colleghi, fornitori, abitudini operative o contesto lavorativo. Proprio questa personalizzazione rende il messaggio più credibile e quindi più pericoloso. Non si punta solo a ingannare un utente distratto, ma a colpire una persona precisa con un'esca plausibile. È questo salto di qualità che lo rende uno degli strumenti preferiti per furto di credenziali, accessi iniziali e compromissione delle reti aziendali.

Per rispondere, le linee guida Acn promuovono l'adozione congiunta di tre protocolli fondamentali: Spf, Dkim e Dmarc. Il Sender policy framework (Spf) consente al proprietario di un dominio di specificare quali indirizzi Ip sono autorizzati a inviare *email* per suo conto, permettendo al *server* destinatario di verificare la legittimità del mittente attraverso il Dns. Il Domainkeys identified mail (Dkim) introduce invece un meccanismo di firma digitale, generata tramite chiavi crittografiche e verificabile attraverso un *record* pubblico Dns. Questo consente di garantire sia l'autenticità del dominio mittente sia l'integrità del contenuto del messaggio.
Il terzo protocollo, Dmarc (Domain-based message authentication, reporting and conformance), integra Spf e Dkim definendo, come ricorda Acn, politiche di gestione dei messaggi che non superano le verifiche di autenticazione. Dmar introduce inoltre il concetto di allineamento tra il dominio verificato dai controlli Spf/Dkim e il dominio presente nel campo *message-from*, che rappresenta l'identità visibile all'utente. L'allineamento può essere di tipo *strict*, con corrispondenza esatta tra i domini, oppure *relaxed*, con corrispondenza a livello di dominio principale. Questo meccanismo consente di individuare incongruenze che potrebbero indicare tentativi di impersonificazione al di là dei tecnicismi.
Le linee-guida Acn evidenziano che tali misure, pur fondamentali, non esauriscono il quadro della sicurezza *email*. A esse si affiancano ulteriori tecnologie come Tls, per cifrare il canale di comunicazione e protocolli di crittografia *end-to-end* come (S/Mmime e OpenPgp) che garantiscono riservatezza e autenticità del contenuto.
L'insieme di questi strumenti delinea un approccio multilivello alla sicurezza della posta elettronica, in cui la protezione dell'identità del mittente rappresenta il primo e indispensabile livello di difesa.

* docente cybercrime & homeland security dell'Università di Perugia

ITA AIRWAYS APRE IL VOLO DIRETTO ROMA-HOUSTON

ITA Airways ha inaugurato il primo collegamento diretto tra Roma Fiumicino e Houston, rafforzando la presenza negli Stati Uniti, primo mercato internazionale della compagnia dopo l'Italia. La rotta parte con 3 frequenze settimanali, che saliranno a 5, e porta a 9 le destinazioni nordamericane servite dal vettore. Il volo punta su domanda business e leisure e amplia la connettività tra Italia, Texas e area del Golfo del Messico.

ENAC E CONFETRA FIRMANO UN PROTOCOLLO

Enac e Confetra hanno firmato un protocollo per rafforzare il cargo aereo in Italia con interventi su qualità dei servizi, digitalizzazione, infrastrutture e sostenibilità. Tra le priorità figurano la Carta dei servizi merci per gli scali oltre 100.000 tonnellate annue, lo sviluppo dell'Airport cargo community system e il potenziamento dei poli logistici, per ridurre la dipendenza dagli *hub* esteri e sostenere l'*export*.

AVIO LANCIA IL SATELLITE SMILE CON VEGA C

Avio ha lanciato con successo il satellite scientifico Smile con Vega C dallo spazioporto europeo della Guyana Francese, portandolo in un'orbita iniziale a circa 700 km dopo un volo di 57 minuti. La missione, sviluppata per Esa e Accademia cinese delle scienze, studierà l'interazione tra vento solare e magnetosfera terrestre. Il lancio segna anche il debutto di Avio come Launch service operator per Vega C.

FINCANTIERI PREMIATA NEGLI USA

Tre cantieri statunitensi di Fincantieri hanno ricevuto riconoscimenti nazionali dallo Shipbuilders council of America per sicurezza, prevenzione degli incidenti e miglioramento continuo. Ace Marine, Marine Repair e Bay Shipbuilding si sono distinti per risultati sul Trir, con premi per eccellenza e miglioramento, mentre Ace Marine è tra soli 3 cantieri Usa con un indice inferiore a 1,0, rafforzando il profilo operativo del gruppo negli Stati Uniti.

AFFIDATA A OHB ITALIA LA MISSIONE RAMSES

Esa e JAXA hanno firmato gli accordi per la missione Ramses verso l'asteroide Apophis, con OHB Italia scelta come *prime contractor* per progettazione, integrazione e consegna della sonda. La missione prevede lancio nel 2028, rendezvous nel 2029 e osservazioni da circa 1 km per studiare come il passaggio ravvicinato con la Terra cambi forma, rotazione e orbita dell'asteroide, rafforzando la difesa planetaria europea.

QANTAS AUMENTA I VOLI TRA ROMA E PERTH

Qantas rafforza il collegamento diretto tra Roma Fiumicino e Perth estendendo l'operativo giornaliero fino al termine della stagione estiva. La capacità complessiva sulla rotta da Roma risulterà triplicata rispetto alla *summer* precedente, in risposta alla forte domanda tra Italia e Australia e al contesto geopolitico sui collegamenti verso l'Europa. La mossa rafforza il ruolo di Fiumicino come *hub* intercontinentale.

AIAD E ADS FIRMANO UN ACCORDO TRA ITALIA E REGNO UNITO

Aaid e Ads hanno firmato un Memorandum of understanding per rafforzare la cooperazione tra le industrie di difesa, sicurezza e aerospazio di Italia e Regno Unito. L'intesa prevede missioni commerciali, delegazioni, partecipazione coordinata a fiere ed eventi e un gruppo di lavoro congiunto per individuare aree prioritarie di collaborazione e nuove opportunità industriali nei mercati internazionali.

ENAC AVVIA UN CONFRONTO CON LA LIBIA

Enac ha ricevuto una delegazione libica guidata dai vertici di Lanco e del fondo Llidf per valutare future collaborazioni tra Italia e Libia nel trasporto aereo. Il confronto punta a sostenere la ripartenza del sistema aeroportuale libico con competenze tecniche, relazioni con gestori, vettori, *handler* e operatori cargo. L'iniziativa rafforza il dialogo tra le due sponde del Mediterraneo su connettività e scambi economici.

THALES ALENIA SPACE FIRMA CON ESA

Thales Alenia Space ha firmato con Esa un contratto da 26,1 milioni di euro per la fase 1 dello sviluppo dei telescopi della missione Lisa, il futuro osservatorio spaziale europeo per lo studio delle onde gravitazionali. Il gruppo guiderà progettazione, assemblaggio e test con Thales SESO, puntando su 6 telescopi ad altissima precisione. Il programma rafforza il ruolo industriale europeo in una missione con lancio previsto nel 2035.

Riportiamo in queste pagine le notizie più interessanti del panorama italiano di difesa, spazio e aviazione. Una selezione che offre uno sguardo rapido ed efficace sulle evoluzioni tecnologiche e strategiche che stanno definendo il futuro del nostro Paese

LEONARDO CONSEGNERÀ AL PERÙ IL QUINTO SPARTAN

Leonardo ha ottenuto dal Perù un ordine per un quinto C-27J Spartan destinato alla Fuerza Aérea del Perú, con consegna prevista nel 2027. Il velivolo sarà il primo del Paese nella versione Next Generation, con nuova avionica e migliori prestazioni. La commessa porta a 100 i C-27J ordinati nel mondo da 21 operatori e rafforza le capacità peruviane in trasporto tattico, evacuazione medica e protezione civile.

GRECIA APPROVA L'ACQUISTO DI 2 FREMM ITALIANE

La Grecia ha approvato l'acquisizione di 2 fregate FREMM usate della Marina militare italiana, la Bergamini e la Fasan, che saranno sostituite in Italia da 2 FREMM EVO. L'intesa conferma lo schema 2+2, con opzione per altre 2 unità, e apre ora alla fase contrattuale. La decisione rafforza il programma di ammodernamento navale di Atene.

FINCANTIERI E TEIJIN FIRMANO UN ACCORDO

Fincantieri e Teijin Automotive Technologies hanno firmato un accordo per sviluppare paratie non strutturali in materiali compositi avanzati per unità navali civili e militari. Le soluzioni, basate su un composito brevettato da Aeronautical service già certificato come non combustibile, puntano a ridurre i pesi e aumentare l'integrazione funzionale, aprendo nuove possibilità progettuali per efficienza, sicurezza e sostenibilità.

LEONARDO FORNIRÀ SISTEMI NAVALI PER IL KUWAIT

Leonardo ha firmato con ADSB, divisione navale di EDGE Group, un contratto da circa 320 milioni di euro per fornire sistemi di combattimento navali di nuova generazione destinati al programma Al Dorra della Marina del Kuwait. L'accordo rafforza una collaborazione che ha già portato alla consegna di oltre 25 navi e consolida il ruolo del gruppo nei sistemi integrati per piattaforme militari sui mercati internazionali.

ITALIA ACQUISTA SEI AEROCISTERNE DI AIRBUS

L'Italia acquisirà 6 aerocisterne Airbus A330 MRTT per l'Aeronautica militare con un contratto da 1,39 miliardi di euro che include circa 10 anni di supporto logistico. La gara si è chiusa con un'unica offerta di Airbus dopo un iter partito con il tentativo di acquistare KC-46A Boeing. Restano da definire versione finale della piattaforma, calendario di consegna e quota di partecipazione industriale italiana.

DELTA APRE IL VOLO DIRETTO ROMA-SEATTLE

Delta Air Lines ha avviato il nuovo collegamento diretto tra Roma Fiumicino e Seattle, operato 4 volte a settimana con Airbus A330-900neo. Seattle diventa la sesta destinazione Usa servita dalla compagnia dalla capitale e rafforza il ruolo di Fiumicino nei collegamenti transatlantici. Nel picco estivo Delta arriverà fino a 8 partenze giornaliere da Roma e fino a 19 voli al giorno tra Italia e Stati Uniti.

EDGE ACQUISISCE IL CONTROLLO DI CMD

EDGE Group ha firmato un accordo per acquisire una quota di controllo in Costruzioni Motori Diesel, azienda italiana specializzata in sistemi di propulsione per applicazioni automotive, navali e aeronautiche. L'operazione punta a espandere la presenza del gruppo nell'ingegneria avanzata, nell'Industria 4.0 e nelle soluzioni energetiche. La chiusura è attesa entro fine anno e prevede nuovi investimenti, sviluppo R&D e accesso a mercati internazionali.

ITA AIRWAYS E ITALO FIRMANO UN ACCORDO

ITA Airways e Italo hanno firmato un protocollo d'intesa per sviluppare un'offerta integrata aereo e treno con un unico biglietto acquistabile tramite Gds e sul sito della compagnia. Il progetto punta a ridurre i tempi di attesa e a rendere più fluido il viaggio, con soluzioni flessibili e coordinate. L'intesa rafforza la connettività sul territorio italiano e sostiene una mobilità più efficiente e sostenibile.

THALES E ARIANEGROUP TESTANO LA MUNIZIONE FLP-T 150

Thales e ArianeGroup hanno completato con successo il primo test di tiro della munizione balistica FLP-t 150, sviluppata per il futuro sistema terrestre X-Fire destinato a sostituire i lanciarazzi unitari francesi. Il vettore supera i 150 km di gittata e punta su precisione anche in ambienti con interferenze GNSS. Il programma rafforza una capacità sovrana francese per attacchi terrestri a lunga distanza.

AIRASIA ORDINA 150 AIRBUS A220

AirAsia ha ordinato 150 A220-300, firmando il più grande ordine singolo mai ricevuto dal programma e portando oltre 1.000 gli ordini fermi complessivi del velivolo. La compagnia sarà anche cliente di lancio della nuova cabina da 160 posti. L'A220 sosterrà l'espansione del *network* tra Asean e Asia centrale, con maggiore autonomia, consumi ridotti e più flessibilità nell'impiego della flotta.

LA POLONIA CREA UN CENTRO PER I MOTORI ABRAMS

La Polonia realizzerà a Deblin l'unico centro europeo autorizzato per manutenzione, riparazione e revisione dei motori AGT1500 dei carri Abrams, in base a un accordo tra WZL-1 e Honeywell. Il polo dovrebbe entrare in funzione entro il 2028 con investimenti per 70-80 milioni di euro. Il progetto rafforza l'autonomia logistica di Varsavia su una flotta di 366 Abrams e veicoli derivati.

LA SPACE FORCE AFFIDA A NORTHROP UN SATELLITE

La U.S. Space Force ha assegnato a Northrop Grumman un contratto da 398 milioni di dollari per sviluppare e costruire un prototipo di satellite per comunicazioni tattiche protette, l'Enhanced Protected Tactical SATCOM-Prototype. Il programma rientra nell'evoluzione del sistema NC3 americano e punta a rafforzare resilienza, sicurezza e continuità delle comunicazioni militari in scenari ad alta minaccia.

LA SVEZIA SCEGLIE LE FREGATE FDI FRANCESI

La Svezia ha selezionato la fregata FDI di Naval Group come piattaforma per il programma Lulea della Marina, che prevede 4 unità con prime consegne dal 2030 al 2033. Il programma vale tra 40 e 60 miliardi di corone svedesi, inclusi armamenti e supporto logistico. La scelta premia una piattaforma già matura e in produzione e segna il ritorno di Stoccolma nel segmento fregate dopo oltre 40 anni.

L'INDIA TESTA IL KIT TARA PER BOMBE PLANANTI

L'Aeronautica militare indiana ha completato il primo test in volo del *kit* TARA, sistema nazionale che trasforma bombe convenzionali in armi di precisione a lungo raggio. Il *kit* sarà integrato su Jaguar, Mirage 2000, Tejas e Su-30MKI e punta a colpire bersagli tra 150 e 180 km con precisione sotto i 5 metri. Il programma mira a ridurre la dipendenza da sistemi esteri e a valorizzare le scorte già disponibili.

LA REPUBBLICA CECA FA VOLARE IL PRIMO C-390

Il primo C-390 Millennium destinato alla Repubblica Ceca ha completato il volo tecnico presso lo stabilimento Embraer in Brasile, avvicinando l'avvio delle consegne. Il contratto per 2 velivoli vale circa 470 milioni di euro e include addestramento, supporto logistico, simulatori e ricambi. I nuovi aerei rafforzeranno trasporto tattico, evacuazione medica, rifornimento in volo e anche capacità antincendio.

IL GIAPPONE VALUTA L'INVIO DI MISSILI ALLE FILIPPINE

Il Giappone sta valutando il trasferimento alle Filippine del sistema missilistico antinave Type 88, dopo l'allentamento delle regole sulle esportazioni militari verso Paesi *partner*. Il sistema ha una gittata oltre 100 km e ogni batteria può lanciare fino a 24 missili. L'ipotesi rafforza la cooperazione tra Tokyo e Manila in risposta alle tensioni nel Mar Cinese Meridionale.

RHEINMETALL SVILUPPA UNO SCUDO ANTI-DRONE

Rheinmetall e Deutsche Telekom collaboreranno per sviluppare uno scudo di difesa contro droni e sabotaggi destinato a città e infrastrutture critiche in Germania. Il progetto unisce sensoristica, reti sicure, *cybersecurity* e protezione perimetrale, con soluzioni pensate anche per droni controllati via rete mobile. L'obiettivo è rafforzare la protezione civile in uno scenario di minacce ibride in crescita.

Riportiamo in queste pagine le notizie più interessanti del panorama mondiale di difesa, spazio e aviazione. Una selezione che offre uno sguardo rapido ed efficace sulle evoluzioni tecnologiche e strategiche che stanno definendo il futuro del nostro pianeta

L'INDIA CREA UN HUB PER I MISSILI DI MBDA

MBDA ha firmato con l'Indian Air Force un accordo per creare in India un centro dedicato a manutenzione, supporto logistico e aggiornamento dei missili aria-aria MICA usati da Rafale e Mirage 2000 modernizzati. Il polo punta a ridurre i tempi di ripristino delle scorte e ad aumentare la prontezza operativa, rafforzando anche la strategia indiana di autonomia industriale nella difesa.

IL BRASILE METTE IN SERVIZIO UNA NUOVA FREGATA

La Marina brasiliana ha ricevuto la fregata multiruolo Tamandaré, prima di 4 unità costruite dal consorzio Águas Azuis su progetto derivato dal MEKO A-100. La nave ha 3.500 tonnellate di dislocamento, radar AESA, missili Sea Ceptor, cannone Leonardo da 76 mm e capacità antisommergibile con elicottero e drone. L'ingresso in servizio rafforza il rinnovamento della flotta e apre alla possibile acquisizione di altre 4 unità.

IL REGNO UNITO ORDINA 72 SEMOVENTI RCH 155

Il Regno Unito acquisterà 72 semoventi RCH 155 su veicolo Boxer con un contratto vicino a 1 miliardo di sterline, prime consegne dal 2028. I sistemi possono sparare 8 colpi al minuto fino a 70 km e saranno prodotti con un forte coinvolgimento industriale britannico, da Telford a Stockport. Il programma colma il vuoto lasciato dagli AS90 ceduti all'Ucraina e rafforza la cooperazione con la Germania.

ANDURIL FORNIRÀ 3.000 MISSILI ALL'US ARMY

Anduril fornirà all'US Army almeno 3.000 missili da crociera Surface-Launched Barracuda-500M e 60 sistemi di lancio containerizzati, con prime consegne previste dal 2027. Il sistema può colpire bersagli terrestri e navali oltre 500 miglia nautiche e viene lanciato da *container* ISO *standard*. Il programma punta ad aumentare rapidamente la massa di fuoco a lungo raggio con un'arma modulare e a basso costo.

SPACEX LANCIA MISSIONE CARGO VERSO LA ISS

SpaceX ha lanciato la missione CRS-34 verso la Stazione spaziale internazionale con una capsula Dragon e un Falcon 9, trasportando circa 6.500 libbre di rifornimenti, hardware e esperimenti scientifici per Nasa. La missione segna il 34° volo cargo del programma commerciale per la Iss e il 6° impiego della stessa capsula Dragon. Il carico sostiene ricerca biomedica, osservazione della Terra e studi sulle condizioni di microgravità.

L'AUSTRALIA AVVIA L'ESTENSIONE DEI SOTTOMARINI COLLINS

L'Australia ha avviato un programma da 11 miliardi di dollari australiani, pari a 7,8 miliardi di dollari Usa, per estendere la vita operativa dei 6 sottomarini classe Collins fino agli anni 2040. Il piano partirà da HMAS Farncomb e prevede revisioni e aggiornamenti su propulsione, armi e sistemi. La misura serve a mantenere la capacità subacquea nazionale durante il passaggio ai sottomarini nucleari previsti dall'accordo AUKUS.

IL PENTAGONO FIRMA ACCORDI PER AUMENTARE LA CAPACITÀ

Il Dipartimento della Difesa statunitense ha firmato nuovi accordi quadro per accelerare la produzione su larga scala di munizioni cinetiche a basso costo destinate alla Joint Force. L'iniziativa punta a rafforzare rapidamente la capacità di attacco americana con sistemi più accessibili e producibili in volumi elevati, in risposta alla necessità di sostenere operazioni ad alta intensità e una maggiore disponibilità industriale.

L'INDONESIA METTE IN SERVIZIO NUOVI RAFALE E A400M

L'aeronautica indonesiana ha messo in servizio un nuovo lotto di mezzi che include 6 caccia Rafale, 4 Falcon 8X, 1 Airbus A400M e 1 radar Thales GM403, insieme a missili AASM Hammer e Meteor. La consegna completa il primo lotto dei 42 Rafale ordinati e rafforza superiorità aerea, trasporto strategico e sorveglianza radar, in un piano più ampio di modernizzazione della difesa aerea nazionale.

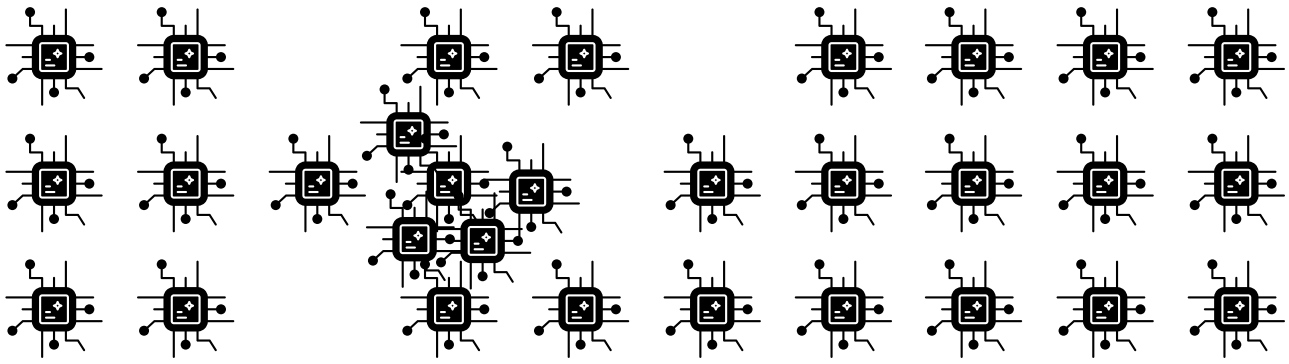
La minaccia più pericolosa per un satellite può venire non dallo spazio, ma da un chip difettoso (o malevolo) assemblato in una fabbrica dall'altra parte del mondo. È in questo modo che assetti e infrastrutture spaziali rischiano di essere compromessi direttamente dalla superficie terrestre

Quando un satellite va in panne per un chip

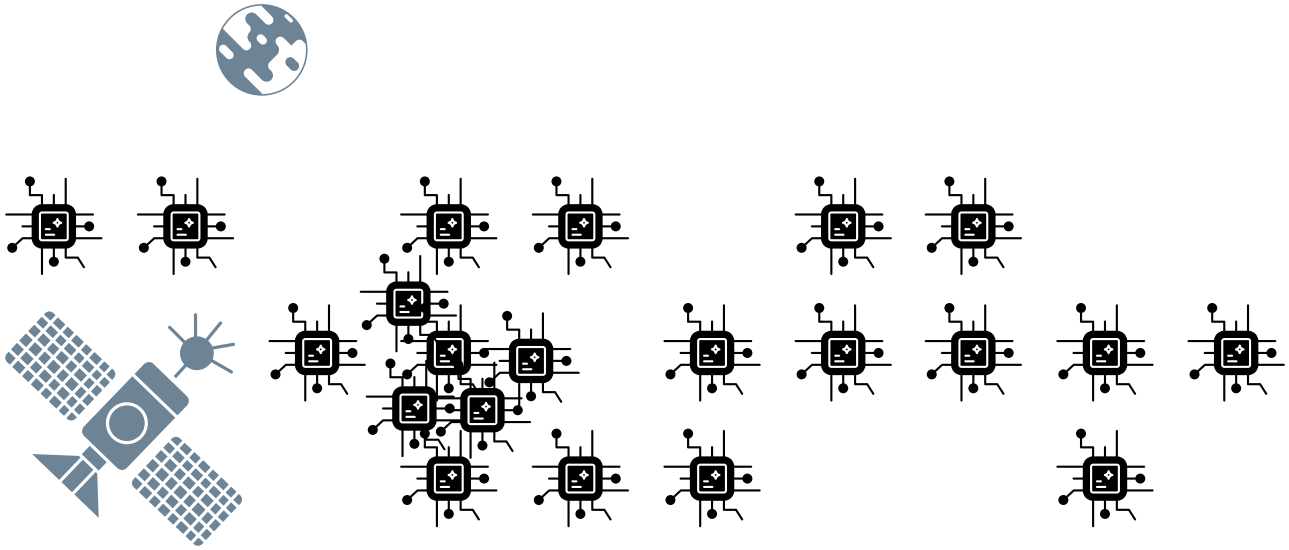
MARCO LISI
inviato speciale per lo spazio del Maeci e membro del board Asi

Quando immaginiamo la sicurezza di un sistema spaziale, l'istinto ci porta a guardare verso l'alto: satelliti in orbita, traiettorie balistiche, *jamming* delle frequenze radio. Eppure, la stragrande maggioranza degli attacchi reali e delle vulnerabilità strutturali nei sistemi spaziali moderni non si trova a seicento chilometri di quota, ma a zero metri sul livello del mare. Il segmento di terra (quell'insieme di antenne paraboliche, *server*, centri di controllo, *gateway* di telecomunicazione e stazioni di telemetria) è il vero sistema nervoso di qualsiasi infrastruttura spaziale. Ed è, per paradosso, la sua parte più esposta. Le stazioni Tt&c (Telemetry, tracking and command) ricevono la telemetria del satellite e inviano comandi per correggere la traiettoria, aggiornare il *software*, attivare sottosistemi. Una stazione Tt&c compromessa non è un punto di ascolto passivo: è un canale diretto per inviare comandi arbitrari a qualunque satellite raggiunga le sue antenne. I *gateway*, invece, interconnettono la rete spaziale con Internet e le reti aziendali: la loro compromissione può significare iniezione di traffico malevolo, degrado selettivo del servizio o attacchi laterali verso le infrastrutture connesse.
La narrativa dominante nella sicurezza spaziale tende a concentrarsi sulla protezione del *link* di comunicazione: cifratura dei segnali, protezione anti-*jamming*, tecniche di *frequency hopping*. Tutto necessario, ma non sufficiente. Perché se il nemico non attacca il canale radio ma il nodo che lo gestisce — la stazione a terra, il *gateway*, il sistema di comando — allora tutte le protezioni in orbita diventano inutili. Il 24 febbraio 2022, poche ore prima dell'invasione russa dell'Ucraina, decine di migliaia di modem connessi alla rete satellitare Ka-Sat di Viasat smisero di funzionare simultaneamente. L'interruzione colpì non solo terminali militari ucraini ma anche turbine eoliche in Germania e utenze private in tutta Europa.
L'indagine successiva attribuirà l'attacco, denominato AcidRain, a un *wiper malware* distribuito attraverso i sistemi di gestione del segmento di terra, non attraverso i satelliti stessi. Il vettore d'attacco era il sistema di gestione remota dei modem: un'infrastruttura a terra che aveva accesso diretto ai dispositivi finali.
Esiste una categoria di minacce ancora più insidiosa degli attacchi software: l'*hardware* malevolo (*malicious hardware*). Si tratta di componenti elettronici — *chip*, Fpga, moduli Rf, microcontrollori — che contengono funzionalità nascoste inserite intenzionalmente in fase di progettazione o produzione. Un *hardware trojan*, vero e proprio cavallo di Troia, è una modifica logica nel circuito integrato, attivabile da un comando specifico o da una combinazione di condizioni operative. Può rimanere dormiente per anni prima di attivarsi, rendendo quasi impossibile la sua individuazione con i test funzionali *standard*.
Un componente contraffatto, identico nell'aspetto a quello originale ma con specifiche degradate o modificate, può introdurre rotture selettive o comportamenti anomali

TRUSTED FOUNDRY Nel lessico della sicurezza tecnologica indica una fonderia o, più in generale, una filiera produttiva considerata affidabile per la realizzazione di componenti elettronici sensibili. Il punto non è solo la qualità industriale, ma la possibilità di controllare chi progetta, chi fabbrica, chi assembla e chi certifica ogni passaggio. In settori critici come quello spaziale questo conta enormemente, perché un *chip* alterato all'origine può introdurre vulnerabilità quasi impossibili da rilevare dopo l'integrazione. La fiducia, quindi, non riguarda il marchio del componente, ma l'intera catena che lo ha reso possibile.



in momenti critici. Nell'ambito delle stazioni Tt&c e dei *gateway*, questi componenti malevoli sono devastanti. Un chip con *trojan* integrato nel sistema di gestione dei comandi può intercettare e duplicare ogni sequenza di comando inviata a un satellite. Un modulo di cifratura compromesso può rendere vana qualunque protezione crittografica del *link*. Un Fpga modificato nel sistema di *tracking* può alterare sottilmente i dati orbitali, inducendo manovre errate. Nei sistemi spaziali l'impatto è amplificato da tre fattori: la longevità (un'infrastruttura di terra può restare attiva vent'anni), l'inaccessibilità (un satellite compromesso non si sostituisce), e la criticità sistemica (Gps, comunicazioni di emergenza, allerta precoce dipendono da questi sistemi). La detezione di questi agenti *hardware* è il problema centrale: i test funzionali verificano che un chip faccia quello che deve, non che non faccia nulla in più. Stiamo poi parlando di modifiche che coinvolgono poche centinaia di dispositivi miniaturizzati, in un circuito integrato che ne contiene milioni: difficile, se non impossibile, rivelarle con un'indagine visiva.
Il problema del *malicious hardware* è intrinsecamente legato alla complessità delle filiere produttive moderne. Un singolo satellite o una stazione di terra incorpora migliaia di componenti elettronici provenienti da decine di Paesi e centinaia di fornitori. La catena che porta da una cava di minerali rari in Congo a un chip montato su un *server* in un centro di controllo in Europa può passare per fonderie in Taiwan, assemblatori in Malesia, distributori in Singapore, integratori in Germania. In ognuno di questi passaggi esiste una finestra di vulnerabilità. La *supply chain attack*, un attacco che compromette la sicurezza non attaccando il bersaglio finale direttamente ma inserendo elementi malevoli lungo la catena di fornitura, è oggi considerata una delle minacce più sofisticate e difficili da contrastare. Costruire una filiera *trusted* richiede trasparenza documentale, preferenza per fornitori verificati in ambito nazionale o alleato (come previsto dal Trusted foundry program DoD e in parte dai programmi Esa) e verifica fisica dei componenti tramite analisi a raggi X, microscopia elettronica (Sem) e il confronto di impronte digitali dei circuiti integrati (Ic *fingerprinting*). L'intelligenza artificiale sta migliorando rapidamente la capacità di identificare *pattern* anomali nel *layout* dei circuiti, rendendo questo processo più scalabile.
Finora abbiamo parlato di vulnerabilità nei componenti e nelle filiere produttive. Esiste però uno scenario ancora più concreto e immediato: una *ground station* di fabbricazione straniera *untrusted* installata fisicamente all'interno di uno spazioporto, a fianco delle stazioni di altri operatori nazionali o alleati. Questo scenario non è teorico. Molti spazioporti commerciali ospitano stazioni di operatori internazionali diversi, condividendo infrastrutture fisiche e di rete. La presenza di un singolo nodo non fidato in questo ambiente trasforma l'intera struttura in un sistema a fidu-



cia degradata. Il punto critico è che il rischio non riguarda soltanto la missione gestita dalla stazione ostile: riguarda tutte le missioni del sito. Un attore malevolo con accesso fisico (reti elettriche, reti di trasmissione dati, condotte e *wireless*, radiofrequenza) a un ambiente condiviso ha una superficie di attacco enorme, spesso invisibile agli altri occupanti. Le possibili direttrici di attacco sono molteplici. Sul piano Rf, la prossimità fisica garantisce angoli di elevazione favorevoli: è possibile effettuare *jamming* selettivo dei *link* altrui, *spoofing* del segnale Gnss locale (degradando il *tracking* delle antenne vicine) o interferenza su canali adiacenti con effetti indistinguibili da guasti *hardware*. Anche senza azioni attive, la stazione è un sensore di Intelligence passivo: registra frequenze, *schedule* di contatto, dimensione dei pacchetti, costruendo nel tempo un profilo operativo completo di tutte le missioni del sito. In un ambiente condiviso attribuire un attacco è estremamente difficile. Questo abbassa la soglia di rischio percepita dall'attore ostile, che può agire con bassa probabilità di essere scoperto e quasi nessuna di essere incolpato con certezza. Le contromisure richiedono isolamento di rete completo, monitoraggio dello spettro perimetrale, separazione fisica delle zone operative e adozione di un modello *zero-trust* per l'intera infrastruttura del sito. Costi e complessità di queste necessarie misure sono difficili da affrontare. Lo spazio è diventato un'infrastruttura critica globale. Le costellazioni di satelliti in orbita bassa gestiscono connettività Internet per miliardi di persone, supportano la navigazione autonoma, abilitano le comunicazioni militari sicure, monitorano il cambiamento climatico in tempo reale. La loro integrità è una questione di sicurezza nazionale, ma anche di sicurezza quotidiana per chiunque dipenda, consciamente o no, da un segnale Gps o da una connessione *broadband*. Proteggere i sistemi satellitari richiede un cambio di paradigma: smettere di guardare solo verso l'alto e iniziare a guardare molto più criticamente verso il basso: verso i *data center*, le antenne, i *gateway*, i chip che li compongono e le fabbriche in cui sono stati costruiti. La *supply chain*, il segmento di terra e l'ambiente fisico in cui operano le stazioni sono i veri fronti della sicurezza spaziale moderna.

ZERO TRUST È un modello di sicurezza basato su un principio semplice e severo. Nessun dispositivo, utente o nodo di rete deve essere considerato affidabile per il solo fatto di trovarsi "dentro" il perimetro di un'infrastruttura. Ogni accesso va verificato, segmentato e limitato in modo continuo. In un ambiente come uno spazioporto condiviso, dove possono convivere operatori diversi, questo approccio è decisivo perché impedisce che la vicinanza fisica o logica si traduca automaticamente in fiducia. In pratica, è il contrario della vecchia idea per cui bastava proteggere il confine esterno per sentirsi al sicuro.

Multi-Domain EW Solutions

Mastering **Electromagnetic Spectrum** in:
Land, Air, Maritime, Underwater, Cyber and Space.

/ EuroAtlantica

di CESARE CIOCCA e RACHELE ROSSI*

D1

NATO

Presenza USA in Europa, una riduzione non converrebbe a nessuno

D2

UNIONE EUROPEA

Dal Caucaso il futuro concetto di Sicurezza-Difesa collettiva

* Comitato Atlantico Italiano

D1

Il disallineamento degli Stati Uniti dagli alleati europei non sembra destinato a convergere nel prossimo futuro. La proiezione strategica statunitense verso il Pacifico rende l'Europa periferica nella futura geografia politico-strategica. In tale contesto, si inserisce la polemica tra il presidente statunitense e il cancelliere tedesco a cui ha fatto seguito la dichiarazione da parte di Washington di voler ritirare cinquemila militari dalla Germania entro 6-12 mesi. Le truppe Usa sul territorio europeo sono 90mila, dislocate in 40 basi a cui il dipartimento della Difesa ha accesso: 66mila sono permanenti, mentre 13mila sono schierate a rotazione tra Romania e Polonia. Dopo la caduta dell'Urss, la presenza statunitense in Europa ha subìto una costante riduzione, salvo poi aumentare di nuovo a seguito dell'invasione della Crimea e dello scoppio della guerra russo-ucraina. Proprio nell'ottica di quest'ultima è stato approvato nel dicembre 2025 il National defence authorization act (Ndaa) che vieta al presidente Usa di ridurre il personale permanente di stanza in Europa al di sotto delle 76mila unità per più di 45 giorni consecutivi a garanzia di una continuità che non è fondamentale solo per il Vecchio continente, ma per gli stessi Usa. Un disimpegno statunitense dal continente europeo non solo comporterebbe ingenti spese per il trasferimento del personale e la sua ricollocazione in patria, ma indebolirebbe la deterrenza europea e atlantica qualora a essa si accompagni anche una limitazione degli assetti forniti da Washington. Degno di nota anche il mancato dispiegamento da parte di Washington di missili Tomahawk sul territorio tedesco, unica valida contromisura agli Iskander russi dispiegati nell'exclave di Kaliningrad. Una riduzione non coordinata della presenza e assetti Usa appare rischiosa e potenzialmente dannosa per ambo le parti. Per Washington, con la perdita di risorse e infrastrutture fondamentali al prosieguo del conflitto con l'Iran e alla proiezione della propria potenza a livello globale, e per l'Europa con l'ineludibile necessità di rafforzare il pilastro europeo dell'Alleanza.

D2

Il Summit di Yerevan apre la strada a un più ampio e condiviso concetto di sicurezza e difesa del continente europeo. La prospettiva non è solo un rafforzamento dell'Unione in senso stretto ma il coinvolgimento di tutti i Paesi del continente, incluso il Canada invitato al vertice. Le politiche intergovernative che si stanno profilando consentiranno di realizzare iniziative concrete in tempi adeguati e quindi efficaci per le esigenze e l'imprevedibilità degli attuali scenari internazionali.
Dall'imposizione del diritto internazionale agli interventi umanitari, gestione delle tecnologie dirompenti e dei conflitti urbani, alle guerre ibride e terrorismo, le sfide ai concetti tradizionali di sicurezza e difesa collettive diventano sempre più ardue e interconnesse, tali da imporre una risposta collettiva e una postura pro-attiva.
L'Ue in particolare ha davanti a sé la sua estensione verso il Caucaso, con il difficile processo di ammissione di Georgia e Armenia, e con tutte le difficoltà delle crisi ancora irrisolte in quell'area. Il rafforzamento della cooperazione con Azerbaijan e le Repubbliche centro-asiatiche è anch'esso un tema prioritario che, sulla spinta di Paesi membri come l'Italia, è fondamentale per la sicurezza energetica del continente. Una più sistematica presenza e sorveglianza nelle regioni critiche, come quella del mar Caspio, sarà inoltre determinante sia per poter esercitare un'adeguata deterrenza, sia per prevenire o gestire tempestivamente situazioni di crisi.
In una visione più ampia non si potrà rinunciare, infine, a più ferme e risolute iniziative in materia di sicurezza delle linee di comunicazione marittime e controllo della dimensione subacquea e dei fondali, che richiederanno ampi investimenti nelle capacità delle forze navali dei Paesi membri.
Starà alla collettività europea raccogliere le sfide e trasformarle in opportunità di integrazione e sviluppo, affermando concretamente i valori di democrazia e libertà e realizzando economie sostenibili.

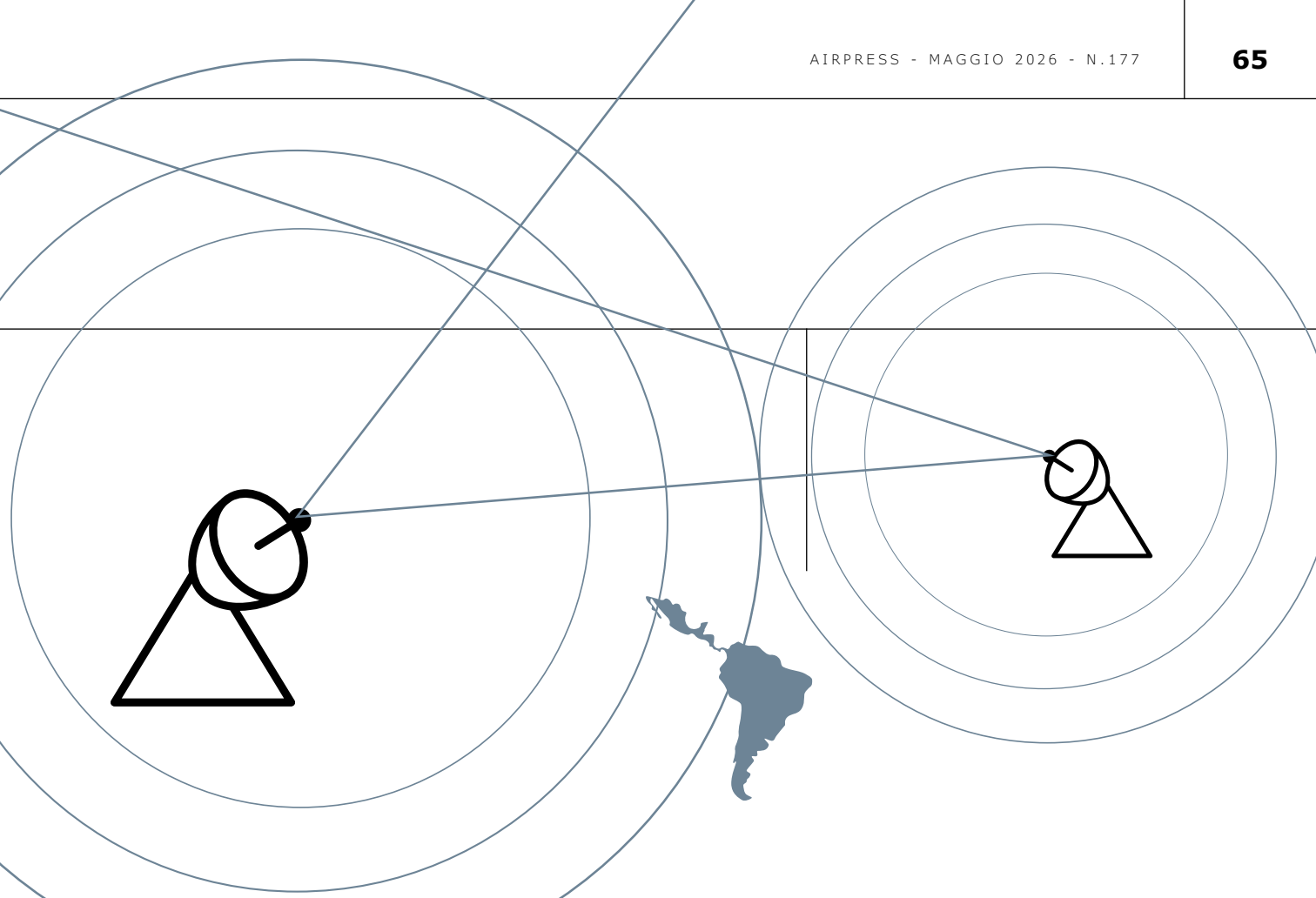
I conflitti orbitali non si combattono solo al di fuori dell'atmosfera terrestre ma anche sui territori più remoti del pianeta. È il caso del Sud America, dove gli Stati Uniti hanno bloccato delle infrastrutture cinesi di radioastronomia per timore di possibili usi militari

Guerra spaziale nei cieli del Sud America

MARCELLO SPAGNULO
ingegnere ed esperto aerospaziale

Ai piedi delle Ande argentine a Cesco nella provincia di San Juan, giace da diverse settimane la carcassa di un enorme radiotelescopio. Il luogo è uno dei migliori al mondo per osservare le stelle, circondato da catene montuose e sotto cieli incontaminati. Ma soprattutto, è sul lato opposto del pianeta rispetto alla Cina, una caratteristica che offre agli scienziati di Pechino la possibilità di osservare l'altra metà del cielo che altrimenti non potrebbero vedere. E infatti il radiotelescopio abbandonato era una collaborazione tra l'università nazionale di San Juan e l'Osservatorio astronomico nazionale cinese. In realtà più che una collaborazione era un investimento da 32 milioni di dollari avviato circa 15 anni fa, noto come China Argentina radio telescope, avviato dalle autorità cinesi con l'allora governo di Buenos Aires. Oggi però il radiotelescopio giace smontato, con la sua gigantesca antenna puntata verso il cielo, cieca. In un dettagliato rapporto il *New York Times* ci informa come il governo degli Stati Uniti abbia attuato fortissime pressioni sulle autorità argentine che alla fine hanno fermato la costruzione bloccando per mesi alla dogana dei componenti-chiave inviati da Pechino. Si rivela quindi una modalità per combattere le guerre spaziali anche sulla superficie del pianeta. Ma la questione del radiotelescopio di San Juan è solo l'ultimo di una serie di eventi iniziati oltre dieci anni fa quando a Buenos Aires Cristina Kirchner era presidente. Nel 2015 i cinesi realizzarono un primo radiotelescopio, un porto a Ushuaia e la base militare a Neuquén con una stazione di controllo satellitare da 50 milioni di dollari grazie a un accordo di locazione gratuita del terreno per cinquant'anni. Per Washington quella base in Patagonia con la sua antenna da 450 tonnellate, divenne la prova evidente dell'attrazione argentina nell'orbita di Pechino. E da quel momento ogni amministrazione della Casa Bianca ha intensificato la pressione politica su Buenos Aires. Nel 2024 il vicino dell'Argentina, il Cile, ha bloccato un progetto di osservatorio astronomico cinese da decine di telescopi nel deserto di Atacama a seguito di fortissime pressioni dell'ambasciatore statunitense. A febbraio scorso il segretario di Stato Marco Rubio ha discusso di "collaborazione spaziale"

ORBITA DI INFLUENZA L'espressione viene usata per descrivere la capacità di una grande potenza di attrarre un altro Paese dentro la propria sfera politica, economica e strategica. Nel caso argentino, il nodo non è solo il telescopio, ma la percezione americana che una presenza tecnologica cinese stabile in Sud America possa tradursi in accesso, leva diplomatica e capacità di raccolta informativa nell'emisfero occidentale. In questo senso le infrastrutture spaziali non sono viste come opere isolate, ma come tasselli di una proiezione di potenza più ampia e di lungo periodo.



con il ministro degli Esteri argentino Gerardo Werthein e subito dopo diversi esperti statunitensi si sono recati a Buenos Aires per informare le autorità argentine sui possibili rischi posti dal telescopio cinese. Sempre secondo il *New York Times*, alcuni scienziati dell'Università nazionale di San Juan sono stati persino convocati al laboratorio Sandia di Albuquerque, gestito dal dipartimento americano dell'Energia, per una riunione di tre giorni incentrata sul potenziale *dual-use* delle strutture di ricerca spaziale civile. Sembra che gli scienziati argentini fossero genuinamente interessati a beneficiare del contributo cinese per scopi scientifici e così la riunione ha sortito l'unico effetto di bloccare a tempo indeterminato la costruzione del telescopio che oggi giace come uno scheletro gigante. L'articolo del *New York Times* riporta singolari fotografie del seminterrato dell'edificio pieno di bacchette, lattine di salsa d'ostrica e scatole di tè verde lasciate dai tecnici cinesi sui tavoli, così come è ripreso un cartello in lingua cinese su un muro con istruzioni su come gestire incontri indesiderati con i puma. La lezione da trarre da questa storia è che gli ingenui astronomi argentini, che hanno trascorso gran parte della loro vita osservando le stelle, hanno ricevuto un corso accelerato di geopolitica terrestre. Avevano sperato di condividere il telescopio con la Cina e altre nazioni ma hanno scoperto che la rivalità tra le superpotenze li aveva raggiunti persino nei deserti del Sud America, fermando le loro ricerche scientifiche. Sono rimasti bloccati nel buco nero della geopolitica i cui conflitti spesso si celano dietro progetti di ricerca e scienza. Non è sempre così ovviamente, anzi talvolta sono proprio le comunità scientifiche a mantenere anche tra Paesi avversari quel canale di comunicazione che va oltre la conflittualità politica e militare. Ma nel caso dei radiotelescopi sudamericani la questione è di vitale importanza per Washington. Le preoccupazioni riguardano non tanto il loro uso scientifico quanto il possibile valore strategico delle infrastrutture spaziali. Strutture come la stazione in Patagonia sono ufficialmente dedicate all'osservazione astronomica ma la loro gestione da parte di enti collegati al programma spaziale cinese, che è piena-

SpaceX si prepara alla quotazione in Borsa

SpaceX ha presentato alla Securities and exchange commission il documento necessario per avviare la sua Ipo. È il passaggio formale che precede la quotazione e consente agli investitori di esaminare attività, conti, rischi e strategia della società prima dell'ingresso sul mercato azionario.
La documentazione non indica ancora numero di azioni e prezzo dell'offerta, definendo però il perimetro industriale che SpaceX intende proporre al mercato. La società organizza i risultati in spazio, connettività e IA.
La connettività satellitare è la parte più solida del quadro finanziario. Starlink ha prodotto 11,4 miliardi di dollari di ricavi nel 2025 e 3,3 miliardi nel primo trimestre 2026. L'Ebitda rettificato è stato rispettivamente di 7,2 miliardi e 2,1 miliardi. Gli abbonati erano 10,3 milioni alla fine del primo trimestre, più del doppio rispetto all'anno precedente.
Questo equilibrio descrive quindi la fase attuale di SpaceX, in cui la rete satellitare ha assunto un peso economico superiore alle attività di lancio, pur dipendendo dalla capacità del gruppo di mettere in orbita e rinnovare grandi costellazioni. Il segmento spazio conserva invece una funzione abilitante, pur avendo generato 4,1 miliardi di ricavi nel 2025 e 619 milioni nel primo trimestre 2026, con un Ebitda rettificato passato da un valore positivo di 653 milioni a una perdita rettificata di 351 milioni.
Starship resta il programma che può modificare la scala operativa di SpaceX, come indica anche il livello degli investimenti. La società ha speso 3 miliardi di dollari per il suo sviluppo nel 2025 e 930 milioni nel primo trimestre 2026. Il veicolo dovrebbe iniziare a lanciare satelliti nella seconda metà dell'anno, dopo una nuova prova suborbitale indicata nella documentazione.
La rilevanza di Starship va oltre i lanci, perché molte delle iniziative future descritte da SpaceX dipendono da una capacità di accesso allo spazio più ampia e industrializzata. A questo sviluppo la società collega anche i *data center* orbitali, previsti non prima del 2028, introducendo però una cautela importante quando riconosce che "resta un lavoro significativo".
L'acquisizione di xAI ha inserito l'intelligenza artificiale nel perimetro di SpaceX e ha aggiunto al gruppo un'area con ricavi già rilevanti, ma ancora in perdita. Il segmento IA ha generato 3,2 miliardi di dollari nel 2025 e 818 milioni nel primo trimestre 2026, con perdite Ebitda rettificate pari a 1,2 miliardi e 609 milioni. È anche l'area che assorbe la spesa più aggressiva in ricerca e sviluppo, con 12,7 miliardi nel 2025 e 7,7 miliardi nel primo trimestre 2026.
SpaceX presenta questa scelta come l'accesso a un mercato potenziale senza precedenti. La stima complessiva è di 28,5 trilioni di dollari, con la quota principale attribuita all'IA, soprattutto nelle applicazioni *enterprise*.
La proposta più distintiva riguarda i *data center* in orbita. SpaceX sostiene di essere "posizionata in modo unico per dispiegare e gestire *data center* in orbita" grazie alla propria integrazione verticale, che combina lancio, produzione satellitare, connettività e competenze sui data center terrestri.
La quotazione espone quindi una società con ricavi consistenti, margini concentrati nella connettività e una spesa orientata verso programmi ad alta incertezza. Per il mercato, la valutazione di SpaceX dipenderà dalla capacità di trasformare questa architettura in risultati misurabili, mantenendo l'ambizione dentro la prova dell'esecuzione.
•

mente integrato con l'esercito, e diversi limiti a una piena trasparenza alimentano i dubbi americani. Il nodo principale è quindi geopolitico perché la presenza di infrastrutture spaziali cinesi nell'emisfero occidentale è interpretata dagli Stati Uniti come parte di una più ampia competizione per l'influenza globale e per il controllo delle capacità di sorveglianza e comunicazione nello spazio. L'ambasciata cinese a Buenos Aires intervistata dai reporter del *New York Times* ha respinto le accuse, affermando che gli Stati Uniti stavano cercando scuse per contenere e reprimere la Cina, e ha definito il progetto del radiotelescopio un contributo al progresso scientifico dell'umanità. Di fatto, i funzionari cinesi accusano Washington di "pura e semplice manifestazione di egemonismo", sottolineando il fatto che in realtà anche gli Stati Uniti utilizzano dei telescopi in Cile. Sullo sfondo di questa disputa, una domanda rimane aperta: fino a dove arriverà la nuova guerra fredda dello spazio, a quale costo per la scienza internazionale, e soprattutto quanto è grande il rischio che da fredda diventi una guerra calda?

LOCAZIONE GRATUITA Quando uno Stato concede per decenni un terreno a un soggetto straniero senza corrispettivo economico diretto, non si tratta mai di un dettaglio puramente amministrativo. Una locazione così lunga e favorevole segnala che l'investimento ha un valore politico e strategico superiore a quello commerciale immediato. Nel caso delle infrastrutture spaziali, significa assicurare continuità operativa, stabilità giuridica e radicamento fisico in un territorio sensibile. È proprio questa durata a far percepire certi accordi non come semplici *partnership* scientifiche, ma come presenze strutturali difficili da ridiscutere.

OLTRE LA LUNA

di MARIAFELICIA DE LAURENTIS*

La cometa aliena dell'acqua *tra chimiche stellari e ghiacci estremi*

Un piccolo oggetto arrivato da oltre il Sistema solare potrebbe cambiare profondamente la nostra comprensione di come si formano i sistemi planetari nella Via Lattea. La protagonista è la cometa interstellare 3I/Atlas, soltanto il terzo visitatore proveniente da un altro sistema stellare mai osservato attraversare il nostro vicinato cosmico. E il suo contenuto chimico sta già mettendo in discussione molte delle idee consolidate sull'origine dell'acqua.

Le nuove osservazioni indicano infatti che questa cometa contiene una quantità straordinariamente elevata di "acqua pesante", una variante dell'acqua in cui l'idrogeno è sostituito dal deuterio, un isotopo più massiccio. Non si tratta di una differenza marginale: il rapporto tra deuterio e idrogeno rilevato è di gran lunga superiore a quello misurato sia negli oceani terrestri sia nelle comete del Sistema solare.

Questo parametro, apparentemente tecnico, è in realtà uno degli strumenti più potenti a disposizione degli astrofisici. Il rapporto deuterio/idrogeno funziona come una vera e propria "firma" delle condizioni ambientali in cui si sono formati i ghiacci. Ambienti più freddi e meno irradiati tendono a favorire l'incorporazione del deuterio nelle molecole d'acqua. Di conseguenza, misurare questa quantità permette di risalire, almeno in parte, alla storia fisica di un oggetto.

Nel caso di 3I/Atlas, il valore osservato è estremo: circa trenta volte più alto rispetto alle comete del Sistema solare e quasi quaranta volte superiore rispetto all'acqua presente sulla Terra. Un risultato che suggerisce un'origine in regioni della Galassia molto più fredde e isolate rispetto alla nube da cui è nato il Sole.

Questo dato ha implicazioni profonde. Per anni si è discusso se l'acqua terrestre potesse essere stata portata da comete simili a quelle che osserviamo oggi. Tuttavia, le misure effettuate nel nostro Sistema solare hanno già mostrato che molte comete hanno rapporti isotopici diversi da quelli degli oceani terrestri. Ora, con un oggetto interstellare che mostra valori ancora più estremi, emerge con forza l'idea che l'acqua possa avere origini molto diverse a seconda dell'ambiente di formazione.

In altre parole, non esiste un'unica "ricetta cosmica" per l'acqua. Ogni sistema planetario potrebbe sviluppare una propria chimica, legata alle condizioni locali della nube molecolare da cui nasce. Questo rende la nostra storia, e quella della Terra, ancora più specifica e meno facilmente generalizzabile.

Dal punto di vista osservativo, il risultato è altrettanto significativo. È la prima volta che si riesce a caratterizzare con questo livello di dettaglio la composizione isotopica dell'acqua in una cometa interstellare. Ciò è stato possibile grazie a radiotelescopi altamente sensibili, capaci di distinguere le sottili differenze spettrali tra molecole contenenti idrogeno e quelle contenenti deuterio.

La sfida principale in questi studi è il tempo. Oggetti come 3I/Atlast attraversano il Sistema solare a velocità elevate e rimangono osservabili solo per periodi relativamente brevi. Questo richiede una risposta rapida da parte della comunità scientifica, sia in termini di identificazione sia di coordinamento delle osservazioni. Ma proprio qui si intravede una prospettiva promettente. Con il miglioramento delle *survey* astronomiche e degli strumenti osservativi, il numero di oggetti interstellari individuati è destinato ad aumentare nei prossimi anni. Ogni nuova scoperta rappresenterà un'opportunità unica per sondare direttamente la chimica di altri sistemi planetari, senza doverli osservare a distanze proibitive.

In questo senso, le comete interstellari diventano vere e proprie sonde naturali della Galassia. Trasportano informazioni sulla composizione, sulla temperatura e sull'evoluzione delle regioni in cui si sono formate miliardi di anni fa. Studiarle significa aprire una finestra diretta su ambienti astrofisici altrimenti irraggiungibili.

Il passaggio di 3I/Atlas potrebbe quindi segnare un punto di svolta: non solo per ciò che rivela sulla diversità chimica dell'Universo, ma anche per il ruolo che questi visitatori cosmici potranno avere nella costruzione di una nuova astrofisica comparata dei sistemi planetari.

ACQUA PESANTE

L'espressione indica acqua in cui al posto del normale idrogeno compare il deuterio, un isotopo più pesante perché contiene anche un neutrone. Questa differenza minima nella struttura produce però un enorme valore scientifico, perché il rapporto tra deuterio e idrogeno conserva traccia dell'ambiente in cui il ghiaccio si è formato. Temperature molto basse e regioni poco irradiate tendono a favorire una maggiore incorporazione di deuterio. Per questo l'acqua pesante non è una curiosità chimica, ma una sorta di archivio naturale che permette di ricostruire la storia fisica di comete e sistemi planetari lontani.

* professoressa di Astronomia e astrofisica presso l'Università di Napoli Federico II, ricercatrice dell'Infn

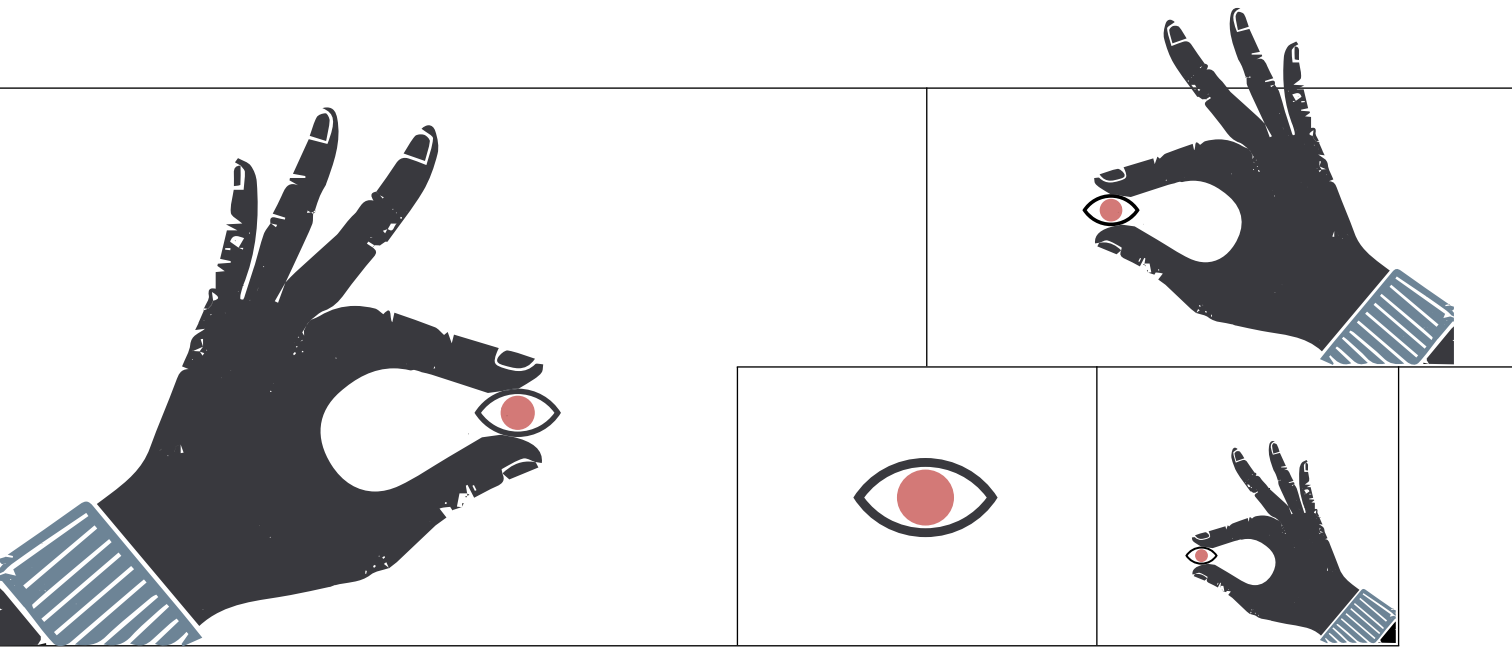
La protezione delle infrastrutture critiche non passa più solo dalla difesa dei sistemi informatici, ma dalla capacità di leggere insieme reti digitali, processi industriali e segnali fisici. In questo quadro, prende forma il modello del Soc multidominio, pensato per unificare monitoraggio, analisi e risposta operativa. La sfida è costruire una resilienza più integrata, capace di anticipare minacce che ormai si muovono senza soluzione di continuità tra cyber e mondo reale

Cos'è la resilienza integrata e come implementarla

CHIARA SPREAFICO
brand & communication specialist di Zenita Group

Nel nuovo scenario della sicurezza, le infrastrutture critiche funzionano grazie a una combinazione sempre più stretta di sistemi informatici e processi fisici. Le reti It (Information technology) gestiscono dati, comunicazioni e applicazioni. Le reti Ot (Operational technology) controllano macchinari, impianti, sensori e sistemi industriali. Quasi tutti i servizi dipendono ormai da entrambe le dimensioni. Per questo una vulnerabilità digitale può trasformarsi in un problema operativo concreto, con effetti sulla continuità dei servizi e sulla sicurezza delle attività essenziali.
È in questo spazio di interdipendenza che si colloca il Cyber-physical warfare (Cpw). Una forma di conflitto in cui l'attacco non resta confinato a computer, *server* o dati, ma punta a produrre conseguenze nel mondo fisico. Un'intrusione in una rete, un'anomalia in un sistema industriale o la compromissione di un nodo operativo possono generare effetti a cascata. Il risultato può essere il blocco di un servizio, l'alterazione di un processo, l'interruzione di una funzione critica o l'indebolimento della fiducia nelle istituzioni. È dentro questo cambio di paradigma che si inserisce il lavoro di Zenita Group sulla sicurezza integrata. La sicurezza informatica tradizionale resta indispensabile perché reti, server e dati continuano a essere bersagli centrali. Diventa però insufficiente quando l'attacco attraversa domini diversi. Un segnale anomalo su una rete industriale, un evento rilevato da un sensore fisico, un dato proveniente da un sistema Scada (Supervisory control and data acquisition), una telecamera intelligente, un asset Rf o una fonte aperta possono sembrare episodi separati. Letti insieme, possono indicare una manovra più ampia, già in corso o in fase di preparazione.
Il limite del Security operations center (Soc) tradizionale nasce da questa frammentazione. Il Soc classico monitora soprattutto il traffico It, rileva incidenti informatici e attiva procedure di risposta. È uno strumento utile, ma pensato per un ambiente in cui il perimetro digitale era più distinto dal resto dell'organizzazione. Nel Cpw quel perimetro si allarga. Le minacce possono combinare anomalie digitali, segnali fisici e contesto esterno. Se questi elementi restano in silos separati, chi deve decidere vede singoli allarmi, non la traiettoria dell'attacco. Il Soc multidominio risponde a questa esigenza con una cabina di regia unica.

CYBER-PHYSICAL WARFARE L'espressione indica un tipo di conflitto in cui l'obiettivo non è soltanto violare reti o sottrarre dati, ma produrre effetti concreti nel mondo fisico attraverso sistemi digitali compromessi. La particolarità sta proprio nel passaggio di soglia. Un'anomalia informatica può trasformarsi in fermo impianto, alterazione di un processo industriale, disservizio essenziale o perdita di sicurezza operativa. Non è quindi una semplice evoluzione della minaccia *cyber* tradizionale, ma un modello di attacco che sfrutta la saldatura crescente tra infrastrutture digitali e funzioni materiali critiche.



In questa direzione si muove l'approccio da noi sviluppato, che integra la sorveglianza degli ambienti It e Ot con la gestione delle minacce fisiche e l'Intelligence geopolitica. La sua funzione non è accumulare dati ma metterli in relazione. L'obiettivo è costruire una visione più completa per la detection e response, capace di individuare anomalie su reti eterogenee, correlare eventi distanti nel tempo e nello spazio e attivare risposte coordinate prima che l'attacco produca effetti più gravi.

La differenza operativa sta nella capacità di leggere il contesto. Un allarme informatico può avere un peso limitato se resta isolato. Può assumere un significato diverso se coincide con un malfunzionamento in un sistema industriale, con un'anomalia fisica o con segnali raccolti da fonti aperte. In un ambiente interconnesso, contenere un attacco significa riconoscere presto i collegamenti tra eventi diversi e trasformare quella lettura in azione.

Un modello multidominio richiede integrazione tecnica, continuità di monitoraggio, capacità analitica e una governance operativa chiara. Mettere insieme fonti diverse non garantisce automaticamente una risposta migliore. La complessità deve essere governata, perché un eccesso di segnali può aumentare il rumore invece di ridurlo. La catena decisionale deve essere definita e i tempi di reazione devono restare compatibili con la velocità degli incidenti.

Nella nostra esperienza, le soluzioni possono essere *on-premise* o basate su *cloud*, con pipeline di analisi proprietarie e controllate, soprattutto quando la protezione riguarda settori ad alta criticità. A questa dimensione si affianca la verifica continua della postura difensiva con *red teaming* e simulazioni di attacco che servono a testare la capacità dell'organizzazione di reagire a scenari realistici, prima che una crisi reale ne esponga le fragilità.

Il beneficio atteso è una difesa più coordinata, capace di anticipare l'evoluzione di un incidente e limitarne l'impatto sui servizi critici. Il limite informativo dei materiali disponibili sta nell'assenza di casi operativi e metriche di efficacia. La direzione resta definita. Quando infrastrutture digitali e fisiche funzionano come un unico ecosistema, la sicurezza deve collegare monitoraggio informatico, controllo operativo e lettura del contesto in un solo processo decisionale.

di LUISA FRANCHINA*

Il rischio dietro la filiera tech
quando la cyber-sicurezza diventa scelta strategica

Si sta affermando, nel contesto europeo, una crescente attenzione al ruolo dei fornitori tecnologici nella sicurezza delle infrastrutture critiche, con un progressivo spostamento del *focus* dalla sola protezione dei sistemi alla valutazione del rischio associato agli attori che li progettano, li gestiscono o ne garantiscono il funzionamento. In questo quadro, la nozione di "fornitore ad alto rischio" sta assumendo un rilievo sempre più centrale nelle politiche di *cyber*-sicurezza dell'Unione, riflettendo l'esigenza di considerare le implicazioni strategiche e geopolitiche delle scelte tecnologiche.
In questa traiettoria si inserisce il processo di revisione del Cybersecurity act, talvolta indicato come "Cybersecurity act 2", che segna un passaggio ulteriore rispetto all'impostazione originaria centrata su certificazione e standard tecnici. Si introduce infatti in modo esplicito una dimensione geopolitica nella valutazione della sicurezza: la proposta prevede infatti la possibilità di identificare fornitori, in particolare provenienti da Paesi terzi, considerati a rischio in relazione a componenti Ict critiche, sulla base non solo di elementi tecnici, ma anche del contesto giuridico e politico di appartenenza, inclusa l'esposizione a interferenze da parte di Paesi terzi, qualora approvata nel testo attuale.
L'approccio europeo si è sviluppato inizialmente nel settore delle telecomunicazioni, in particolare con riferimento alle reti 5G, dove gli Stati membri sono stati chiamati a valutare il profilo di rischio dei fornitori sulla base di criteri che includono elementi quali la trasparenza, l'affidabilità, il quadro normativo di riferimento e le possibili interferenze da parte di Paesi terzi. Tale impostazione si sta progressivamente estendendo ad altri ambiti, in linea con una visione più ampia della sicurezza digitale, che tiene conto della stretta interconnessione tra infrastrutture, servizi e catene di fornitura.
Si tratta di un'evoluzione potenzialmente vincolante, poiché la qualificazione come *high-risk supplier* può tradursi in limitazioni concrete come l'esclusione da *procurement* pubblico, restrizioni operative o, nei casi più critici, il *phase-out* o la rimozione di componenti critiche fornite da soggetti qualificati ad alto rischio, secondo tempi e ambiti definiti. Si configura così un cambio di paradigma in cui la *cyber*-sicurezza assume sempre più il ruolo di strumento di politica industriale e di sicurezza economica e la selezione dei fornitori diventa parte integrante delle strategie di autonomia strategica dell'Unione.
Il tema assume una dimensione particolarmente rilevante se si considera il livello di dipendenza tecnologica da fornitori esterni all'Unione, in settori-chiave come il *cloud*, l'*hardware* avanzato e alcune componenti *software* critiche. In questi ambiti, la concentrazione del mercato e la presenza di pochi attori dominanti pongono interrogativi non solo in termini di resilienza operativa, ma anche di autonomia strategica. La possibilità che vulnerabilità tecniche o pressioni di natura politico-istituzionale possano incidere sul funzionamento di servizi essenziali rappresenta un elemento di rischio che le istituzioni e le imprese europee stanno progressivamente mitigando, grazie all'adozione di *policy* mirate.
In questo contesto, le iniziative europee mirano a promuovere un ecosistema tecnologico più diversificato e affidabile, incoraggiando la riduzione delle dipendenze critiche e la valutazione sistematica dei fornitori lungo l'intero ciclo di vita dei prodotti e dei servizi Ict. Ciò si traduce, in termini operativi, nell'introduzione di criteri più stringenti nei processi di *procurement*, nel rafforzamento delle verifiche sui partner tecnologici e nella definizione di strategie di diversificazione che limitino l'esposizione a singoli attori.
Il tema dei fornitori ad alto rischio si inserisce in un quadro geopolitico più ampio, nel quale le scelte tecnologiche diventano parte integrante delle relazioni internazionali. Le misure adottate o in discussione a livello europeo possono generare reazioni da parte dei Paesi interessati, contribuendo a ridefinire gli equilibri nel mercato globale delle tecnologie digitali. In questo senso, la gestione del rischio *cyber* non può essere separata dalle dinamiche di competizione economica e politica.

HIGH-RISK SUPPLIER

L'espressione indica un fornitore considerato problematico non solo per eventuali vulnerabilità tecniche, ma per il contesto politico e giuridico in cui opera. Il punto decisivo è che la sicurezza non viene più valutata solo sul prodotto, ma anche sul soggetto che lo sviluppa, lo controlla o potrebbe subirne l'influenza da parte di uno Stato terzo. In questo modo la *cyber*-sicurezza esce dall'ambito puramente tecnico e diventa uno strumento di politica industriale e strategica. Scegliere un fornitore, quindi, non significa più soltanto comprare tecnologia, ma anche decidere quanto rischio geopolitico si è disposti ad accettare.

* presidente dell'Associazione italiana esperti in infrastrutture critiche

ITSM
Iccsai Transport and Sustainable Mobility Center
UNIVERSITÀ DEGLI STUDI DI BERGAMO

enac
Ente Nazionale per l'Aviazione Civile

Fact Book 2026

XX EDIZIONE

Tra un'epoca e l'altra: verso quale trasporto aereo?

Giovedì 4 giugno 2026

Saluti Istituzionali

Salvatore Deidda
Presidente Commissione Trasporti, Poste e Telecomunicazioni della Camera dei deputati

Relazione di presentazionedel Fact Book 2026

Renato Redondi
Centro ICCSAI-ITSM

Costantino Pandolfi
Vice Direttore Centrale Enac

Quali investimenti per non restare indietro

Stefano Paleari
Centro ICCSAI-ITSM

Alfonso Celotto
Presidente Aeroporti 2030

Presidenza del Consiglio dei Ministri

Carlo Borgomeo
Presidente Assaeroporti

Gaetano Intrieri
Chief Executive Officer Aeroitalia

Joerg Eberhart
Amministratore Delegato ITA Airways

Conclusioni

Pierluigi Di Palma
Presidente Enac

Edoardo Rixi
Viceministro delle Infrastrutture e dei Trasporti

Modera

Flavia Giacobbe
Direttore Formiche e Airpress

L'avvento del Regolamento 521/97 ha segnato un importante cambio di passo nel mondo aeroportuale, inserendosi nel processo europeo di liberalizzazione del trasporto aereo e spingendo verso una maggiore apertura al mercato e alla concorrenza. In accordo con la tendenza europea, la policy Enac in termini di concessioni aeroportuali caratterizzate da liberalizzazione e privatizzazione nella tutela degli interessi pubblicistici, ha incoraggiato importanti investimenti infrastrutturali.

Negli ultimi anni si sta intraprendendo un importante percorso volto a incrementare la capacità, la sostenibilità ambientale, la digitalizzazione e l'innovazione tecnologica, con una massima attenzione alla corretta programmazione e realizzazione delle opere e alle tempistiche di intervento in relazione alle previsioni di crescita del traffico. Ciò è di prioritaria importanza ai fini del costante mantenimento dei livelli di capacità, di sicurezza operativa e di qualità dei servizi, assicurando un uso corretto delle risorse impegnate.

In prospettiva futura è interessante un'analisi finalizzata a comprendere l'andamento effettivo del traffico negli ultimi anni rispetto a quanto ipotizzato e come influiscono sulla capacità le tempistiche di realizzazione degli interventi, spesso procrastinate da procedure autorizzative ridondanti che finiscono per danneggiare la competitività del trasporto aereo italiano nel mercato globale, dove, oggi, il trasporto aereo rappresenta l'elemento fondamentale rispetto ad una filiera produttiva che determina la crescita economica del Paese.

Pierluigi Di Palma
Presidente Enac

Le consegne mondiali nell'Aviazione generale, escludendo i business jet, ammontano nel 2025 a 2376 velivoli di cui 641 prodotti in Europa, con una domanda degli Stati Uniti pari a due terzi di quella mondiale. È quanto emerso dal salone di Friedrichshafen. L'Italia si distingue per una presenza industriale competitiva soprattutto sui mercati esteri, nonostante i limiti che ancora frenano lo sviluppo interno del settore

Lo stato di salute del mercato dell'aviazione

FABRIZIO BRAGHINI
analista di politiche europee e di difesa

La seconda edizione di Aero2026, il salone internazionale della General aviation e Business aviation di Friedrichshafen, sede storica degli Zeppelin, è stata una *kermesse* in grande spolvero (860 espositori da 55 Paesi), diventata un *marketplace* per la domanda-offerta, dove si è fatto il punto sullo stato di un comparto tecnologico caratterizzato da continua evoluzione, adattamento tecnologico e progetti avanzati, innovativi e sostenibili. Il *focus* di quest'anno ha visto come nuove tematiche dominanti l'innovazione, la sostenibilità, la *safety*, la formazione con la diffusione delle Accademie, nonché la significativa partecipazione e il coordinamento di enti certificatori come Easa e di Paesi europei su aspetti quali semplificazione per la General aviation, *safety*, approvazioni e certificazioni di prodotto.
Il comparto Aviazione generale *business* fa segnare una crescita costante e robusta, con un +15% con ricavi di 36 miliardi di dollari e un +2% nel numero di consegne, con positive *performance* economiche e commerciali spinte dalla fascia alta dei velivoli *business*, come riporta preliminarmente l'Us Gama (General aviation manufacturers association che riunisce l'80% degli operatori e delle flotte mondiali), dove la domanda è assorbita per due terzi dal mercato statunitense. Al riguardo si deve tener conto che il comparto comprende un'ampia definizione che include *corporate, business jet* ed elicotteri, mono-bimotori a pistoni e *turboprop* e le fasce inferiori come alianti, velivoli sportivi e ala rotante.
Per avere un ordine di grandezza di dettaglio, le consegne mondiali nell'Aviazione generale, nei segmenti dei velivoli a pistoni e turbina escludendo i *business jet*, ammontano nel 2025 a 2376 velivoli di cui 641 prodotti in Europa, con una domanda degli Stati Uniti pari a due terzi di quella mondiale. Da notare a margine che, nonostante l'entrata sul mercato di velivoli evoluti, i monomotori (la categoria numericamente più ampia) più venduti sono sempre gli intramontabili e validi Cessna 172 Skyhawk e Piper PA28 Archer oggi in nuove versioni con avionica avanzata.
A Friedrichshafen sono state presentate alcune novità come il Cessna Ascend e SkyCourier , il Daher TBM 980 e Kodiak 900, Cirrus SF50 Vision Jet, l'addestrato-

AZEA La sigla indica la Eu Alliance for zero emission aviation, un'iniziativa europea nata per coordinare industria, regolatori e ricerca sul percorso verso un'aviazione a basse o zero emissioni. Non riguarda solo i grandi aerei di linea, ma anche la General aviation e la mobilità regionale, dove il tema è spesso più urgente perché i margini economici e tecnologici sono più stretti. Il suo valore sta nel provare a trasformare innovazione dispersa in una roadmap condivisa, mettendo al centro nodi molto concreti come batterie, propulsione ibrida e accesso al mercato.

Palazzo Chigi mette lo spazio tra le priorità

Il governo ha deciso di portare lo spazio pienamente all'interno della strategia nazionale, trasformando un settore a lungo percepito come frontiera tecnologica in un terreno di politica industriale, sicurezza e competitività. Il governo ha infatti deciso di stanziare 7,8 miliardi di euro fino al 2028, destinato a infrastrutture, tecnologie, ricerca e competenze. La scelta conferma il ruolo del finanziamento pubblico nei settori strategici, ma richiama anche la necessità di attrarre più capitale privato, rafforzare l'apertura internazionale e rendere più stretta la collaborazione tra imprese, ricerca e università.
Palazzo Chigi rivendica così un ruolo di coordinamento, con l'obiettivo di dare all'Italia una regia più solida in un ambito dove ricerca, impresa, difesa e servizi commerciali si intrecciano sempre di più. La posta in gioco non è solo la capacità di innovare, ma anche la possibilità di restare agganciati alle filiere più avanzate.
Intervenendo in occasione di una riunione del Comint, Giorgia Meloni ha indicato lo spazio come un ambito strategico per il presente e per il futuro del Paese. L'attenzione a questo dominio è stata presentata come una priorità nazionale, dentro una cornice che tiene insieme sicurezza, competitività e capacità industriale.
Il piano del governo si muove lungo tre direttrici. La prima è la *governance*: il Comint risponde all'esigenza di riunire le amministrazioni competenti e costruire una direzione comune. È un passaggio che segnala la volontà di superare frammentazioni e ritardi, perché nello spazio i confini tra civile e militare, ricerca e industria, infrastrutture pubbliche e servizi commerciali sono sempre più mobili.
La seconda direttrice riguarda le regole. Meloni ha richiamato alla legge nazionale sulla *space economy* del 2025, presentandola come il provvedimento che ha dato all'Italia una disciplina organica sullo spazio. Secondo la premier, la norma chiarisce le responsabilità, colma un vuoto regolatorio, offre una cornice stabile alle attività spaziali e rafforza la collaborazione tra pubblico e privato.
Il terzo pilastro è la filiera nazionale. Il discorso si sposta così sul tessuto produttivo e scientifico del Paese, fatto di grandi gruppi, Pmi innovative, *start-up*, università, centri di ricerca e distretti territoriali. A questo sistema si aggiunge poi il capitale umano, indicato come decisivo per mantenere competitivo il Paese.
•

re Tecnam P2008 JC NG, l'ultraleggero ad alta velocità TerrOne di Aeromecc Aerospace.
La presenza dell'Aviazione generale italiana al Salone con 37 espositori è rappresentativa di un piccolo ma dinamico numero di imprese, con un'offerta *Italian style* di aeromobili avanzati e originali ben inseriti in svariati mercati esteri come il Piaggio Aerospace P.180 Avanti Evo (ordinati due Avanti NX), la Tecnam con una gamma di velivoli mono e bimotori tra i quali P2008 JC NG, P2012 Vip, P2010, P2006T NG, Mentor, P92 con nuovo motore Rotax, che ha siglato ben 86 ordini al Salone, gli aerei sportivi e ultraleggeri Pioneer e l'elicottero Syton AH180 di Alpi Aviation, gli ultraleggeri avanzati Promecc Aerospace. Potremmo affermare che l'Italia dell'aviazione generale è più conosciuta all'estero che in patria, dove scarsa cultura aeronautica e problemi burocratici endemici non ne favoriscono la diffusione e la crescita, risultando in una flotta di aeromobili certificati in una scala inferiore alla media europea. Ne consegue una progressiva obsolescenza di queste macchine solo parzialmente compensata dai nuovi velivoli progettati e realizzati da Pmi aeronautiche italiane, e dalla diffusione nella fascia inferiore di nuovi ultraleggeri.
Se da una parte c'è una rinnovata collaborazione tra regolatori e operatori per snellire procedure e norme più in linea con l'approccio flessibile, lo stato apatico della flotta italiana nell'insieme presenta un rovescio della medaglia per il dinamismo industriale nelle fasce turismo e diporto, che progetta e realizza una gamma di velivoli apprezzati sui mercati internazionali. È il caso in particolare di Tecnam che offre una gamma in continua evoluzione e si posiziona (fonte Gama) tra i primi quattro produttori mondiali nei segmenti dei velivoli a pistoni e turbina. Il primo è Cirrus con 797 consegne, seguita da Piper con 291, Diamond con 235 e a ruota da Tecnam con 216 velivoli.
Il Salone si è anche caratterizzato per un costruttivo dialogo cliente-produttore-regolatore con iniziative di coordinamento europeo. Tra queste la Eu Alliance for zero emission aviation (Azea), *roadmap* che pone l'attenzione della General aviation, Regional mobility e CS-23 aircraft sull'aspetto critico dell'accesso al mercato

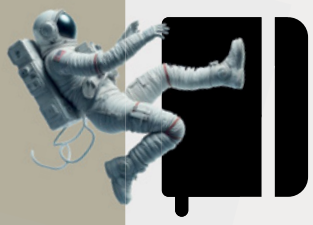
La Space Force chiama a raccolta gli alleati

Per Washington lo spazio non è più soltanto un'infrastruttura strategica di supporto alle operazioni terrestri, aeree e navali, ma un vero dominio operativo nel quale prepararsi a muovere, proteggere e coordinare assetti in caso di crisi o conflitto. In questa cornice lo United States Space Command sta lavorando con sei alleati occidentali alla definizione di un piano comune per la futura *orbital warfare*, cioè una dottrina condivisa per operare insieme nello spazio in un contesto segnato dalla crescita delle capacità spaziali di Cina e Russia. Il gruppo di lavoro coinvolgerà Australia, Canada, Francia, Germania, Nuova Zelanda e Regno Unito e dovrebbe arrivare a compimento entro la fine del 2026.
Il cambio di impostazione emerge già dal lessico adottato dai vertici militari americani. Non si parla più soltanto di sicurezza spaziale o di deterrenza, ma di manovrabilità orbitale, cioè della capacità di spostare rapidamente i satelliti, proteggerli, aggirare minacce e garantire continuità alle funzioni più sensibili. La Space Force e lo Space Command stanno infatti spingendo su sistemi in grado di manovrare e sostenere operazioni prolungate nonché, in prospettiva, ricevere e fornire supporto logistico in orbita. L'idea è superare il modello dei grandi satelliti statici, considerati più esposti in caso di confronto ad alta intensità, e puntare invece su architetture più mobili, distribuite e resilienti.
La spinta verso questa evoluzione nasce dalla percezione di una competizione sempre più serrata con i rivali sistemici. Pechino ha accelerato sullo sviluppo di capacità *dual use*, satelliti manovrabili, strumenti anti satellite e sistemi di guerra elettronica in grado di disturbare o neutralizzare assetti occidentali in orbita. Anche Mosca continua a investire in questo campo, mantenendo attivamente capacità di interferenza e di contrasto ai sistemi spaziali. Per gli Stati Uniti, una perdita di superiorità nello spazio avrebbe conseguenze che andrebbero ben oltre il piano militare, perché toccherebbe comunicazioni, navigazione, *targeting* e sistemi di allerta missilistica, cioè alcune delle infrastrutture più sensibili dell'intero dispositivo strategico occidentale.
La cooperazione con gli alleati serve quindi a costruire non solo coordinamento tecnico, ma una vera base dottrinale comune. Il progetto dovrebbe includere procedure condivise di *space control*, protocolli di risposta alle minacce anti satellite, scambio di informazioni orbitali e capacità integrate di comando e controllo. In questo quadro pesa anche la natura dei Paesi coinvolti. Alcuni appartengono già ai circuiti di Intelligence più stretti dell'Occidente, mentre altri hanno elaborato negli ultimi anni strategie nazionali di difesa spaziale, e tutti rappresentano partner con cui Washington vuole consolidare un nucleo altamente interoperabile in un settore destinato a diventare sempre più centrale.
Resta più sfumato il capitolo relativo agli impieghi offensivi. Ufficialmente la linea americana continua a richiamare deterrenza, protezione delle infrastrutture spaziali e capacità di risposta. Ma il concetto stesso di *orbital warfare* implica anche la possibilità di condurre operazioni contro assetti avversari, attraverso *jamming*, *cyber*-attacchi, interferenze elettroniche o sistemi co-orbitali capaci di alterare il comportamento dei satelliti nemici senza distruggerli fisicamente. Il senso dell'iniziativa sta proprio qui. Gli Stati Uniti stanno cercando di trasformare lo spazio da ambiente da proteggere a teatro in cui operare in modo coordinato con gli alleati, definendo in anticipo regole, capacità e linguaggio comune. Il passaggio segna così il tentativo di costruire una postura spaziale condivisa, nella quale interoperabilità, resilienza e capacità di manovra diventino elementi sempre più centrali della sicurezza occidentale.
•

delle batterie elettriche, la propulsione ibrido-elettrica e i sistemi *fuel cell* a idrogeno. Parallelamente è stato pubblicato il libro bianco *Wings of Change* dell'Associazione europea dei costruttori di General aviation che promuove una strategia sostenibile realizzabile con investimenti in innovazione come contributo all'attesa strategia Eu sostenibile per l'industria aeronautica civile. Si tratta di coordinamenti tra operatori e regolatori europei (come Eurocontrol, Sesar JU e Clean Sky Ju) e di certificazione nazionali, che accompagnano il *warning* lanciato dall'industria europea circa l'esigenza di una strategia specifica. L'obiettivo è mantenerne competitività, sovranità in sicurezza e *net-zero aviation*, focalizzandosi sulla spinta all'innovazione, decarbonizzazione, digitalizzazione e Atm, acquisendo competenze e talenti.
L'insieme delle iniziative che si spera si concretizzino e degli investimenti in nuove soluzioni tecnologiche dimostrano, come affermato ad Aero2026, che la General aviation di domani sta prendendo forma oggi, con aeromobili silenziosi a basse emissioni e affidabili.

CS-23 È la categoria regolatoria che disciplina una vasta parte degli aerei leggeri e di media complessità, compresi molti velivoli della General aviation. Più che una sigla tecnica, rappresenta un terreno decisivo per l'innovazione, perché da essa dipendono criteri di certificazione, margini di flessibilità progettuale e tempi di ingresso sul mercato. Quando si parla di elettrificazione, ibrido o nuove architetture per il volo leggero, il nodo non è solo inventare un velivolo migliore, ma farlo rientrare in un quadro normativo che ne permetta davvero la diffusione commerciale.

DIARI DI BORDO

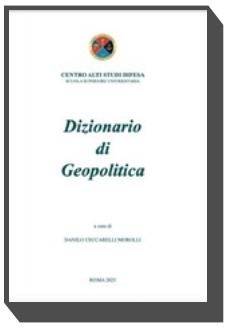


Oliver Barsanti
Tessitore di traiettorie
Cartabianca, 2026
Pp. 160. Euro 14

I controllori di volo svolgono un ruolo tanto importante quanto poco noto al grande pubblico, anche per la mancanza di lavori storici o biografici su questa materia. È con tale spirito che l'autore – che ha operato in quel ruolo prima in Aeronautica militare (1993-96) e poi, soprattutto, in Emav, fino a diventare presidente del sindacato Anacna – ha raccolto appunti ed episodi della propria esperienza professionale. Si va dalla prima mappatura GPS degli aeroporti ai messaggi formali trasmessi dai velivoli impegnati in missioni di Stato, dalla priorità all'Air Force One presidenziale alle diverse sale di controllo, molte delle quali non sono neppure in aeroporto. Benché esposto in tono molto divulgativo e senza una struttura organica, il libro aiuta il lettore non specialista a farsi una prima idea del lavoro del controllore.

Danilo Ceccarelli Morolli (a cura di)
Dizionario di geopolitica
CASD, 2025
Pp. 1039+LVI. S.i.p.

In un momento in cui la parola geopolitica è ovunque, il Centro alti studi difesa, da poco trasformatosi in Scuola superiore universitaria, affianca al periodico *Strategic Leadership Journal* un dizionario che ne definisce i principali termini. Al di là della scelta dei lemmi, croce e delizia di ogni curatore, non vi è dubbio che le circa 600 voci (da "Accra initiative" a "Zhou Enlai, dottrina" redatte da oltre 170 collaboratori costituiscono il primo importante tentativo di mappatura della disciplina in lingua italiana, proponendosi al tempo stesso come strumento di lavoro e confine contro gli abusi. A ulteriore conferma del suo lodevole obbiettivo, il volume è consultabile – oltre che nella sua forma cartacea – anche online sul sito del Casd. Un buon augurio per la collana "Spectator" che il dizionario inaugura.



Leonardo Tricarico e Gregory Alegi (a cura di)
Quale difesa per l'Europa
Rubettino, 2026
Pp. 128. Euro 15

La situazione internazionale ha messo la difesa europea al centro del dibattito politico, senza che a ciò corrispondessero in pari misura concretezza ed esattezza. Partendo dalla necessità di una difesa comune (e non solo di un "esercito europeo"!), è proprio attorno a questi due aspetti che ruota la ricerca condotta dal gruppo di lavoro Difesa della Fondazione Icsa. Sotto il profilo strutturale, la proposta è quella di creare un Alto rappresentante per la Difesa separato da quello per le Relazioni esterne, riproducendo la dicotomia presente nell'ordinamento di tutti gli stati. Segue poi un'analisi dei punti cruciali, dalla dottrina all'industria, passando per la necessità di porre l'etica (ovvero il diritto internazionale umanitario) al centro della costruzione europea. Tutto questo con il metodo della Pesco, in modo da superare il problema dell'unanimismo che finora ha bloccato i tentativi di procedere su una strada indispensabile.

La ripresa d'interesse per il mare riporta in primo piano la componente pilotata del pattugliamento marittimo e della lotta antisommergibile. Questa capacità, essenziale durante la Guerra Fredda, negli ultimi anni si era andata gradualmente riducendo, Ora, il possibile interesse italiano per il Kawasaki P-1 giapponese apre a nuove prospettive strategiche e industriali

Pattugliatori, per l'Italia è tempo di scegliere

GREGORY ALEGI
storico e giornalista

Fin dalla nascita dell'aeroplano, le forze di superficie ne hanno apprezzata la capacità di guardare e trasmettere oltre l'orizzonte. Sul mare, poi, fu subito chiaro come per le flotte la possibilità di esplorare e pattugliare ampi spazi a velocità impossibili per le navi fosse un moltiplicatore capacitivo essenziale. È dunque inevitabile che la ritrovata importanza del mare si accompagni a una rivisitazione della componente aerea, nelle sue più diverse declinazioni, anche non pilotate.
Come in ambito terrestre, anche sul mare l'uso dei droni è ormai una realtà. La guerra in Ucraina ha visto operare nella dimensione strategica gli RQ-4, ormai una presenza stabile sul mar Nero, ma esiste già una completa gamma di prodotti che vanno dall'Aw Hero italiano al Boeing ScanEagle. è facile prevedere che tali strumenti andranno diffondendosi, anche grazie al loro indubbio valore tattico. Altrettanto vale per i caccia imbarcati, categoria nella quale al momento non vi è alcun concorrente in vista per gli F-35B e F-35C, entrambi i quali richiedono portaerei di varia taglia, e per gli elicotteri, preziosi per la lotta antisommergibili, le forze speciali e il trasporto.
La ripresa d'interesse per il mare riporta in primo piano la componente pilotata del pattugliamento marittimo e della lotta antisom. Questa capacità, essenziale durante la Guerra Fredda, si andata gradualmente riducendo, in particolare con l'uscita dal servizio del Bréguet Atlantique alla metà dello scorso decennio. Scelto nel 1968 ed entrato in linea quattro anni dopo, l'Atlantique offriva un'ampia gamma di capacità alle quali nel clima *post*-Muro fu impossibile dare continuità. A questo contribuì anche l'elevato costo della soluzione tecnologicamente più avanzata, basata sulla cellula del bireattore civile Boeing 737NG. Il costruttore statunitense proponeva addirittura un pacchetto noto come Joint surveillance & command program che copriva sia le esigenze della Marina (con il Multi-mission maritime aircraft, Mma, poi evolutosi nel P-8A Poseidon) sia quelle dell'Aeronautica militare (l'Airborne Early warning and control, acquistato dall'Australia come Wedgetail e divenuto E-7 per l'Usaf con l'obiettivo di sostituire il glorioso E-3 Awacs), con tutte le

JOINT SURVEILLANCE PROGRAM L'idea del Joint surveillance & command program era costruire una famiglia coerente di velivoli su base comune, capace di coprire due esigenze diverse ma complementari. Da una parte il pattugliamento marittimo e la lotta antisommergibili, dall'altra l'allerta aerea e il comando in volo. Il vantaggio non era solo operativo ma industriale e logistico, perché avrebbe significato addestramento, manutenzione e filiere più integrate.

Kawasaki P1

E-7 Wedgetail

E-3 Awacs

P-8A Poseidon

sinergie relative. Il programma congiunto avrebbe offerto un grande salto capacitivo ma, per una serie di motivi, non ultimo l'alto costo a fronte di ricadute industriali basse o nulle, si fermò quasi subito.
Ciò portò ad affidare il ruolo antisom ai soli elicotteri EH.101 della Marina militare ed a ridurre la capacità marittima ad ala fissa al solo pattugliamento. Questo fu affidato agli Atr 72 MP, i cui vantaggi andavano dalla comunanza con gli Atr.42 utilizzati da Guardia di finanza e Capitanerie di porto fino all'origine nazionale. Nel nuovo quadro internazionale, con tutte le sue sfide marittime, questo schema – che in verità non aveva mai davvero convinto – ha mostrato tutti i propri limiti. Iniziava così la ricerca di un possibile successore, attorno al quale ricostruire la specialità. La scelta, secondo voci tanto diffuse da non poter essere derubricate a indiscrezioni, sarebbe caduta sul quadrireattore giapponese Kawasaki P-1, una macchina da 80 tonnellate sinora costruita in 36 esemplari, tutti dal Giappone, pari a circa la metà del fabbisogno complessivo previsto.

Rispetto a Boeing, Atr e alla proposta francese su base Airbus A321, il P-1 si distingue per essere stato progettato sin dall'inizio per uso militare, con tutto ciò che ne consegue. Dal lato opposto, l'aereo è stato sinora offerto senza successo a Francia (che optò piuttosto per l'A321 Mpa), Germania, Nuova Zelanda e Regno Unito (tutti poi orientatesi verso il P-8A), Thailandia e persino Vietnam. La mancanza di clienti internazionali si traduce peraltro nella mancanza di riferimenti sul supporto logistico, soprattutto per le dotazioni giapponesi, come i motori IHI F-7 da 60 tonnellate di spinta ciascuno. Giapponese è anche il radar a scansione elettronica Hps-1, in grado di cercare bersagli in terra, mare e cielo in ben sei modalità diverse. Sotto il profilo industriale, un anno fa Leonardo confermò l'avvio di discussioni con Kawasaki. Come testimonia la loro partecipazione al programma Gcap, il rapporto tra l'industria italiana e giapponese è peraltro già forte, con tutto ciò che questo comporta. Altre opportunità sono legate alla possibilità di compensare l'eventuale scelta dell'addestratore italiano

La Difesa apre una piattaforma online per le imprese

LIl ministero della Difesa ha inaugurato una nuova piattaforma digitale pensata per aziende, Pmi, *start up* e altri soggetti interessati a collaborare con il dicastero, con l'obiettivo di rendere più trasparente e tracciabile il rapporto tra amministrazione e sistema produttivo. Presentata a Roma alla biblioteca centrale dell'Esercito, alla presenza del ministro Guido Crosetto, dei vertici militari e di rappresentanti istituzionali, la piattaforma nasce come strumento destinato a regolare in modo uniforme le interlocuzioni con i portatori di interesse, in una fase in cui il ministero è chiamato a gestire *dossier* sempre più rilevanti anche sul piano degli appalti e dell'innovazione tecnologica.
Crosetto ha collegato il progetto all'esigenza di rendere più chiaro il perimetro dei rapporti tra il personale della Difesa e i soggetti esterni, spiegando che il sistema è stato costruito per offrire garanzie sia all'amministrazione sia a chi vi lavora. La logica non sarebbe quella di introdurre un controllo aggiuntivo, ma di dotare il dicastero di una cornice stabile entro cui registrare contatti, richieste, incontri e proposte. In questo modo ogni interlocuzione potrà essere ricostruita e inserita in un quadro verificabile, con l'intento di rafforzare legalità, parità di trattamento e tutela del personale coinvolto.
Uno dei punti centrali dell'iniziativa riguarda l'accesso all'innovazione. Accanto ai grandi gruppi già presenti nel comparto, la piattaforma punta infatti ad aprire il confronto anche a realtà più piccole e a soggetti che non hanno rapporti consolidati con il ministero, ma possono offrire competenze e soluzioni nuove. L'obiettivo è rendere più ordinato l'accesso e allo stesso tempo ampliare la platea degli interlocutori. Sul piano operativo, i soggetti esterni potranno accreditarsi tramite Spid o carta d'identità elettronica, indicando azienda, referenti autorizzati e requisiti richiesti. Il personale della Difesa utilizzerà invece un'applicazione per registrare incontri, partecipanti, oggetto e modalità del contatto. Il sistema riconosce soltanto soggetti già accreditati e conserva uno storico delle interlocuzioni. La piattaforma si presenta così come un'infrastruttura amministrativa costruita per rendere più accessibile, ordinato e verificabile il dialogo tra Difesa, industria e innovazione.
•

M-346J per sostituire gli ormai anziani Kawasaki T-4, alla quale è collegata la presenza di allievi giapponesi presso l'International flight training school di Decimomannu sin dal 2022.
Prima di abbandonarsi ai facili entusiasmi, bisogna comunque ricordare la concorrenza di Mitsubishi, che ha proposto il progetto T-X, ancora sulla carta, e degli Usa, il cui Boeing T-7A Red Hawk vola già. A rendere quest'ultimo concorrente particolarmente minaccioso è lo storico rapporto tra Giappone e Stati Uniti, che già premono per un'uscita dal Gcap a favore dell'F-47. Se si pensa che quarant'anni fa era il Giappone a chiedere di acquistare i caccia F-22A Raptor, che gli americani preferirono lasciare andare fuori produzione anziché esportarne le tecnologie sensibili, si tratta di un ribaltamento di prospettive molto eloquente.
Così come il mare, anche le scelte industriali scoprono dunque il proprio versante geopolitico. Da una parte la conferma della relazione-cardine della politica estera giapponese *post*-bellica; dall'altro il rafforzamento di un asse politico-industriale sempre più ampio, in grado di costituire un tassello chiave della sicurezza giapponese a fronte di una Cina le cui ambizioni investono ormai l'intera regione asiatica. L'acquisizione del nuovo pattugliatore marittimo diventa così una cartina di tornasole per la volontà giapponese di autodifesa ma anche la capacità europea di compiere scelte strategiche. Di certo una media potenza regionale, come disse a suo tempo il professor Carlo M. Santoro, non può più pensare di affidare il pattugliamento marittimo a un biturboelica di piccole dimensioni com'è avvenuto nell'ultimo decennio.

KAWASAKI P-1 Questo pattugliatore si distingue dagli altri perché non nasce dall'adattamento di un aereo civile, ma come piattaforma militare progettata fin dall'inizio per il pattugliamento marittimo. Questa scelta comporta vantaggi importanti in termini di autonomia, disposizione dei sensori, resistenza strutturale e integrazione della missione antisom. Ma porta con sé anche un rovescio della medaglia. Senza una base di clienti internazionali ampia, ogni decisione su supporto logistico, pezzi di ricambio e sostenibilità nel lungo periodo diventa più delicata.

GEOPOLITICAL INSIGHTS FROM ITALY

جيوسياسية
تحليلات
من إيطاليا

IL SITO DI INSIGHTS GEOPOLITICI DALL'ITALIA.
IN INGLESE E IN ARABO

decode39.com

savethedate

3_6 GIUGNO 26

La sicurezza in Bulgaria

La fondazione Hemus-95 organizzerà a Plovdiv, in Bulgaria, la 17sima edizione di Hemus, il salone internazionale dedicato alla difesa, l'antiterrorismo e la sicurezza. L'evento, promosso con il patrocinio dei ministeri bulgari della Difesa, dell'Economia e dell'Innovazione, approfondirà temi come *cybersecurity*, sistemi autonomi, intelligence, controllo delle frontiere e tecnologie per la sicurezza civile, con dimostrazioni dinamiche e conferenze

8_10 GIUGNO 26

A Dublino il quantum dell'Esa

Sarà Las Vegas a ospitare la Future force capabilities conference 2026, organizzata dalla National defense industrial association (Ndia). L'evento riunirà rappresentanti di forze armate, industria e ricerca per discutere l'evoluzione delle capacità militari ngli scenari operativi odierni. Focus su sistemi autonomi, armamenti avanzati, robotica e munizionamento, con sessioni tecniche, area espositiva e dimostrazioni operative dal vivo.

10_14 GIUGNO 26

L'aviazione di oggi e di domani a Berlino

L'associazione tedesca dell'industria aerospaziale e Messe Berlin organizzeranno a Berlino Ila Berlin, una delle principali fiere mondiali dedicate all'aerospazio. L'evento riunirà aziende, istituzioni, forze armate e centri di ricerca nei settori aviazione, spazio e difesa, con focus su sostenibilità, mobilità aerea avanzata, digitalizzazione e sovranità tecnologica. L'edizione 2026 prevede oltre 750 espositori da 37 Paesi e più di 95mila visitatori.

15_19 GIUGNO 26

La Difesa europea a Parigi

Torna il salone internazionale Eurosatory, che si svolgerà a Parigi, nel centro espositivo Paris Nord Villepinte. L'evento è uno dei principali appuntamenti mondiali dedicati a difesa e sicurezza, con la partecipazione di oltre 2mila espositori e decine di migliaia di professionisti. L'edizione 2026 approfondirà innovazione tecnologica, sistemi multi-dominio, cybersecurity e gestione delle crisi globali.

23_25 GIUGNO 26

La formazione militare a Bristol

Si terrà a Londra la conferenza internazionale Full spectrum air defence week, che riunirà rappresentanti militari, industria e istituzioni per affrontare le nuove sfide della difesa aerea integrata. Tra i temi principali: sistemi multilivello, difesa contro droni e missili ipersonici, radar di nuova generazione e reti C2 avanzate.

23_25 GIUGNO 26

La difesa aerea a Londra

Si terrà a Londra, presso l'Hilton Syon Park, la Full spectrum air defence week. La conferenza rappresenta un punto di riferimento per la comunità internazionale della difesa aerea e missilistica, con la partecipazione di oltre venti delegazioni militari provenienti da tutto il mondo. In programma, una giornata introduttiva sulle armi a energia diretta, seguita da sessioni dedicate alle minacce emergenti, all'interoperabilità e allo sviluppo di sistemi integrati.


ALA
SCP SINTERSA
ALA Group
Delivering what
OUR CUSTOMERS need,
where
they need it and
when
they need it
ALA is a GLOBAL DIVERSIFIED SUPPLY CHAIN INTEGRATOR
to the Aerospace, Defense, and High-Tech Industries.
With over 35 years of experience, ALA and its wholly owned SCP Sintersa Group build their success on the talent of 750+ people, offering a one-stop shop range of products, services, and high-performance engineered solutions truly capable of simplifying and optimizing its customers' supply chain operations across Europe, Israel, and North America.
www.alacorporation.com
a-l-a--spa

THE NEW ERA OF INTELLIGENT SHIPBUILDING ON BOARD

Stiamo plasmando la nuova era dello shipbuilding, portando a bordo un cervello digitale che consente alle nostre navi di pensare, evolvere e anticipare la complessità. Integriamo automazione avanzata, cyber defence, tecnologie di propulsione pionieristiche e intelligenza dei dati in tempo reale per ridefinire gli standard di performance, sostenibilità e innovazione.
Dai sistemi di nuova generazione alle tecnologie a zero emissioni, ogni soluzione esprime il nostro impegno verso l'eccellenza industriale.
Leader globali, trasformiamo la visione in realtà per guidare il cambiamento.

È COSÌ CHE PORTIAMO IL FUTURO A BORDO.

FINCANTIERI
FUTURE ON BOARD