



Funded by
the European Union
NextGenerationEU



Powered by



LUISS 

Research Center
for International
and Strategic Studies

OCTOBER.2026

La Dimensione Subacquea

Nuovi scenari di minaccia e reazione per il paese

In collaboration with



La Dimensione Subacquea

Nuovi scenari di minaccia e reazione per il paese

Contributori

Raffaele Marchetti, Alessandro Celestra, Manfredi Valeriani, Denise Danili, Antonio Leandro, Daniela Irrera, Carolina Polito, Gabriele Marchionna, Giacomo Leccese, Ivan Fraternali, Lorenzo di Stefano, Claudio Passalacqua

Sommario

<i>Executive Summary</i>	5
1. Mappatura delle infrastrutture subacquee strategiche italiane	6
1.1 Definizione di infrastruttura subacquea e criteri di strategicità.....	6
1.2 Tipologie e architettura delle infrastrutture critiche subacquee	7
1.3 Le principali reti e dorsali nazionali	9
1.4 Choke points e aree di maggiore vulnerabilità.....	14
2. Perimetro normativo e giurisdizionale della Dimensione subacquea	16
2.1 La sovranità e la giurisdizione dello Stato costiero	16
2.2 Le zone d'ombra dell'alto mare: limiti dei meccanismi di enforcement e vuoti normativi	17
2.3 Altri strumenti internazionali rilevanti e profili di responsabilità	19
2.4 Il quadro normativo italiano: la legge 9/2026 e le nuove competenze della Marina Militare	19
2.5 Spunti di cooperazione e proiezione strategica	21
3. Rischi e minacce alle infrastrutture sottomarine	23
3.1 Perimetro di analisi.....	23
3.2 Minacce non deliberate	25
3.3 Minacce deliberate e ibride	28
3.4 Vettori e modalità di azione	32
3.5 Mappatura dei rischi.....	37
4. Soluzioni di difesa e modelli di protezione	40
4.1 Misure di prevenzione, sorveglianza e deterrenza nel contesto subacqueo	40
4.2 Protezione passiva e resilienza delle infrastrutture.....	42
4.3 Risposta e ripristino a seguito dell'interruzione	44
4.4 Il processo di riparazione.....	45
5. Esperienze estere	47
5.1 Stati Uniti	47
5.2 Francia	47
5.3 Giappone	47
5.4 Australia.....	48
5.5 Svezia.....	48
5.6 Regno Unito	48

5.7 Irlanda.....	49
5.8 Israele	49
5.9 Cina.....	49
5.10 Egitto	50
5.11 Turchia.....	50
6. La dimensione subacquea al 2050: quattro futuri per l'Italia	51
6.1 Perché guardare al 2050, e come.	51
6.2 Ciò che accadrà comunque: gli elementi predeterminati.	51
6.3 Le due incertezze critiche.	52
6.4 Ciò che gli scenari insegnano: misure robuste e misure contingenti	56

Indice delle Figure

Figura 1. Sistema di cavi sottomarini per telecomunicazioni	8
Figura 2. Sistema di infrastrutture sottomarine per il trasporto di gas e idrocarburi....	9
Figura 3. Mappa dei Cavi Sottomarini.....	10
Figura 4. Sistema Gasiero Sottomarino.....	11
Figura 5. Ripartizione degli spazi marittimi secondo la CNUDM	17
Figura 6: Scenari futuri per l'Italia.....	53

Indice delle Tabelle

Tabella 1. Matrice di rischio per le infrastrutture sottomarine	38
Tabella 2. Matrice Rischio - Impatto	39

Executive Summary

La dimensione subacquea è divenuto uno dei fronti primari della sicurezza nazionale, e il Mediterraneo rappresenta oggi uno dei teatri più vulnerabili e strategici al mondo. L'Italia, per posizione geografica e concentrazione di landing points in Sicilia, Puglia e Liguria, è uno degli Stati più esposti a rischi accidentali e minacce ibride, con un profilo di dipendenza che rende la continuità operativa delle infrastrutture subacquee un asset strategico nazionale. Le minacce di oggi sono ridotte rispetto alle potenziali minacce future a motivo di almeno tre elementi fondamentali: 1) la proliferazione di armamenti a basso costo come i droni marini, 2) l'aumento delle tensioni internazionali; 3) la predisposizione di future minacce (mappatura delle infrastrutture, pre-posizionamento di strumenti latenti etc.) che potrebbero avere un impatto significativo in caso di conflitti futuri.

Le nuove responsabilità introdotte con la Legge 9/2026 assegnano alla Marina Militare un ruolo centrale nella sorveglianza, deterrenza ed enforcement nella dimensione subacquea, incluse le attività di controllo nelle acque interne, nel mare territoriale e sulla piattaforma continentale, nonché la prevenzione della navigazione subacquea ostile. A queste funzioni si aggiunge il compito di cooperazione con le Marine alleate e con l'Agenzia per la Sicurezza delle Attività Subacquee (ASAS).

Il rischio più frequente per le infrastrutture sottomarine italiane non è il sabotaggio diretto, ma gli incidenti accidentali (ancore, reti da pesca, instabilità dei fondali), spesso indistinguibili nelle prime fasi da potenziali attacchi ibridi. Questa ambiguità impone la capacità di attribuzione rapida, di messa in sicurezza dei nodi costieri e di controllo degli accessi alle aree sensibili subito dopo un'interruzione. La dimensione subacquea resta inoltre caratterizzata da una forte opacità fisica: ciò rende essenziale lo sviluppo di una *Underwater Domain Awareness* (UDA) avanzata basata su sonar attivi/passivi, sistemi MAD, AUV e ROV, integrati in un quadro di comando e controllo interagenzia che consenta una valutazione accurata delle anomalie e un'efficace *deterrence by detection*.

Inoltre, la possibilità che attori statuali o proxy colpiscano infrastrutture critiche in acque poco profonde, interferiscano con navi posacavi o conducano operazioni cyber di pre-posizionamento rende necessario lo sviluppo di una postura attiva anche nelle dimensioni logistiche, cyber e geoeconomiche. La protezione delle navi di riparazione, la gestione dei *choke point* marittimi e il coordinamento con operatori privati e autorità portuali diventano così componenti decisive della sicurezza subacquea nazionale.

Infine, la dimensione internazionale è parte integrante della missione: le infrastrutture che insistono nel Mediterraneo dipendono dalla stabilità di aree come il Mar Rosso, il Canale di Suez e il Mediterraneo orientale. Si renderà dunque necessario contribuire ad una architettura euro-atlantica di sicurezza subacquea che integri consapevolezza, resilienza e capacità di risposta con NATO, UE e partner regionali.

In questo quadro, la protezione della dimensione subacquea non è solo una sfida tecnica, ma un compito strategico che richiede una combinazione di superiorità operativa, cooperazione interistituzionale e capacità di anticipazione, affinché l'Italia preservi la propria funzione di hub critico della sicurezza energetica e digitale nel Mediterraneo.

1. Mappatura delle infrastrutture subacquee strategiche italiane

1.1 Definizione di infrastruttura subacquea e criteri di strategicità

Per infrastruttura subacquea si intende l'insieme delle strutture e dei sistemi essenziali situati sul fondale marino o al di sotto di esso, cruciali per una varietà di operazioni che comprendono le comunicazioni, la produzione e il trasporto di energia, i trasporti e la difesa. In questa categoria rientrano quindi i cavi sottomarini in fibra ottica, che oggi veicolano circa il 99% delle comunicazioni internazionali, i cavi elettrici per la trasmissione di energia tra regioni e Paesi, gli oleodotti e i gasdotti, gli impianti offshore per le energie rinnovabili, le strutture di ricerca e sorveglianza marina, nonché le infrastrutture di trasporto con fondazioni sommerse quali i tunnel subacquei. La strategicità di queste infrastrutture non è esclusivamente una proprietà tecnica intrinseca, è piuttosto il risultato di una valutazione politico-istituzionale che riflette priorità economiche, vulnerabilità percepite e obiettivi di sicurezza nazionale. Essa si articola lungo tre piani distinti: funzionale, sistemico e di sicurezza/geopolitico.

Sul piano funzionale, un'infrastruttura subacquea è strategica quando abilita o condiziona l'erogazione di servizi essenziali per il funzionamento dello Stato. La criticità non dipende dalla natura tecnica dell'asset in sé, ma dal suo ruolo abilitante rispetto a funzioni quali la continuità delle comunicazioni, o la sicurezza degli approvvigionamenti energetici. L'interruzione di tali funzioni comprometterebbe infatti la continuità operativa del Paese. Un cavo in fibra ottica che trasporta traffico internet commerciale, per esempio, può diventare strategico nel momento in cui abilita anche comunicazioni militari o sistemi di controllo di infrastrutture critiche terrestri. Dal punto di vista sistemico, la strategicità si misura invece in termini di sostituibilità, ridondanza ed effetti a cascata. Nella definizione di questa dimensione tre indicatori sono particolarmente rilevanti: la bassa sostituibilità, che si verifica quando i percorsi alternativi sono scarsi o quando la riallocazione del traffico richiederebbe tempi incompatibili con la continuità dei servizi essenziali; la bassa ridondanza, che si manifesta nella concentrazione di numerose tratte su medesimi corridoi marini o su un numero limitato di punti di approdo, ampliando la probabilità che un singolo evento produca impatti estesi; e l'elevata interdipendenza, per cui un'interruzione energetica può ripercuotersi a cascata su reti digitali e altri servizi critici, moltiplicando l'effetto del danno iniziale. Infine, sul piano securitario e geopolitico, rivestono particolare importanza le infrastrutture con valore dual-use, nonché quegli asset che contribuiscono a consolidare il ruolo del Paese quale hub mediterraneo di connettività e snodo delle reti globali di dati ed energia, proiettandola come ponte tra Europa, Africa, Medio Oriente e Asia.

Va precisato che, sebbene le infrastrutture sottomarine possano essere bersagli di azioni dolose, gli incidenti più frequenti restano di natura accidentale come attività di pesca commerciale e di navigazione o fenomeni naturali come terremoti e frane sottomarine¹. Tuttavia, gli eventi registrati negli ultimi anni, in particolare nell'area del Mar Baltico (Nordstream 1&2 - 2022, Baltconnector - 2023, BCS East-West Interlink

¹ European Commission Joint Research Center (2025), "Subsea cables: how vulnerable are they and can we protect them?"

data cable - 2024)², segnalano un'escalation di azioni ostili deliberate che impone di riconsiderare il profilo di rischio complessivo. A complicare ulteriormente il quadro, la riparazione di un cavo sottomarino o di una stazione di atterraggio è un'operazione complessa, lunga e dipendente da un numero estremamente ridotto di navi specializzate disponibili a livello mondiale: un attacco coordinato contro le principali infrastrutture sottomarine avrebbe quindi un potenziale impatto sistemico di rilievo sulla sicurezza nazionale.

1.2 Tipologie e architettura delle infrastrutture critiche subacquee

Partendo dalla definizione generale di infrastrutture subacquee è possibile identificare alcune tipologie specifiche³. Quelle di maggior rilievo strategico sono indubbiamente le infrastrutture di comunicazione e quelle energetiche. Della prima categoria fanno parte i cavi sottomarini per le telecomunicazioni. Il sistema di cavi sottomarini per le telecomunicazioni si compone di una parte sommersa (*wet plant*) e di una parte terrestre (*dry plant*), entrambe essenziali per la continuità della trasmissione⁴. La componente sommersa include il cavo in fibra ottica, i ripetitori che amplificano il segnale ad intervalli regolari di circa 100 km lungo i fondali oceanici, e in alcuni casi dispositivi di diramazione che consentono ramificazioni verso destinazioni multiple. La parte terrestre comprende invece il punto di approdo costiero (*beach manhole*) e le stazioni di atterraggio (*cable landing station*), che ospitano le apparecchiature terminali, i sistemi di alimentazione i dispositivi di raccordo con la rete terrestre. I cavi vengono posati da navi appositamente progettate, le posacavi, in un processo che può richiedere da uno a tre anni dalla pianificazione alla messa in esercizio. In acque profonde, i cavi vengono adagiati direttamente sul fondale. In prossimità della costa, vengono invece interrati in trincee mediante aratri specializzati e rivestiti quindi con armature in acciaio zincato a fini di protezione.

² Lindholm, R. (2025, March 24). Mapping undersea infrastructure attacks in the Baltic Sea. Wilson Center.

³ Cassetta, M. (2024). Le Minacce alle infrastrutture critiche subacquee nazionali. Rivista Marittima Settembre-Ottobre 2024

⁴ Swinhoe, D. (2021). What is a submarine cable? subsea fiber explained. Data Center Dynamics. Retrieved June, 25, 2023

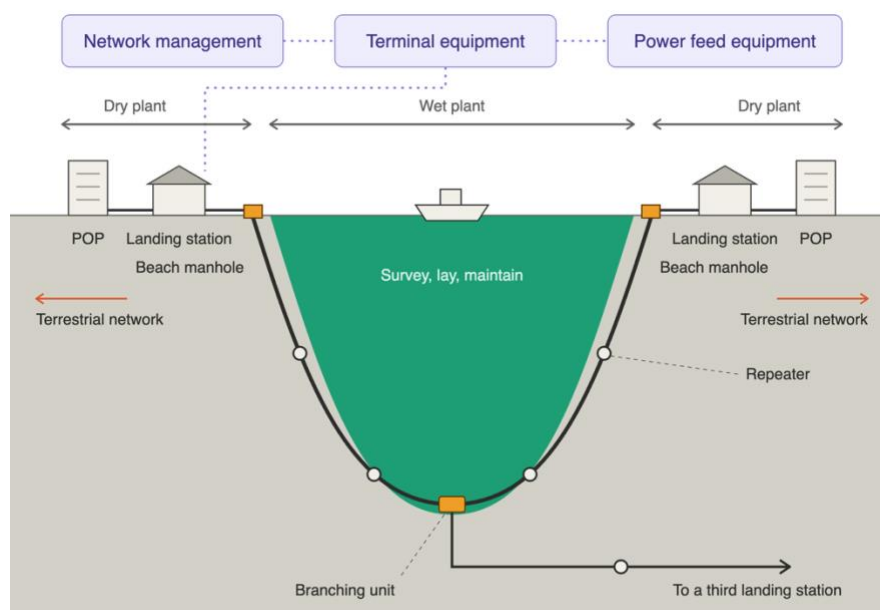


Figura 1. Sistema di cavi sottomarini per telecomunicazioni⁵

Un sistema di cavi sottomarini moderno si articola di solito su tre livelli sovrapposti: il livello fisico (il cavo e sue infrastrutture di supporto), il livello logico (i sistemi di gestione centralizzata Network Management System che monitorano e controllano da remoto la trasmissione dei dati) e il livello informativo (i pacchetti di dati veicolati lungo il sistema). L'intreccio di questi tre livelli determina la continuità delle comunicazioni globali e, al contempo, moltiplica le superfici di attacco potenzialmente sfruttabili da attori ostili.

Un'altra categoria di infrastruttura è rappresentata dai cavi elettrici sottomarini che hanno assunto un ruolo crescente nella configurazione del sistema energetico europeo, svolgendo funzioni essenziali per l'integrazione delle energie rinnovabili offshore, la realizzazione di interconnessione tra Paesi e la stabilizzazione dei mercati elettrici attraverso scambi transfrontalieri. Cavi di questo tipo possono trasmettere energia in corrente alternata (Alternate Current AC/ High Voltage Alternating Current - HVAC) o in corrente continua ad alta tensione (High Voltage Direct Current - HVDC). Per tratte brevi (inferiori agli 80km circa), la tecnologia AC risulta più economica, per tratte più lunghe diventa invece necessario ricorrere all'HDVC che consente di coprire centinaia di chilometri con minori perdite. Analogamente ai cavi di telecomunicazione, l'infrastruttura dei cavi elettrici sottomarini presenta un segmento sommerso (cavo, sistemi di protezione, eventuali armature) e un segmento terrestre con stazioni di conversione e trasformazione, che costituiscono nodi critici per l'interconnessione con la rete elettrica nazionale. L'installazione di questi cavi avviene preferibilmente mediante interrimento nel fondale tramite aratri sottomarine, al fine di ridurre il rischio di danneggiamento.

⁵ Adattato da: Jill C. Gallagher (2022), "Undersea Telecommunication Cables: Technology Overview and Issues for Congress", US Congressional Research Service, p. 5, <https://crsreports.congress.gov/product/pdf/R/R47237>.

Infine, l'ultima tipologia di infrastruttura subacquea da considerare è quella delle condutture per gas e idrocarburi. Nel settore energetico, le pipeline sottomarine per il trasporto di gas e idrocarburi rappresentano infrastrutture di primaria importanza per la sicurezza energetica nazionale. Per queste infrastrutture il segmento sommerso comprende la condotta principale, generalmente in acciaio ad alta resistenza, rivestita da strati protettivi anticorrosione, isolamento termico per prevenire la formazione di idrati e, frequentemente, armature metalliche per garantire la stabilità sul fondale. Lungo il tracciato possono poi essere presenti strutture sottomarine di raccolta (*manifold*) e *riser* verticali che collegano il fondale a piattaforme offshore o unità galleggianti di produzione. In acque profonde la condotta viene adagiata direttamente sul fondale. Nelle aree costiere invece è interrata tramite scavo di trincee. L'integrità del sistema è monitorata attraverso sensori di pressione flusso e piattaforme digitali di supervisione e controllo (SCADA), che consentono la gestione remota e l'individuazione di anomalie.

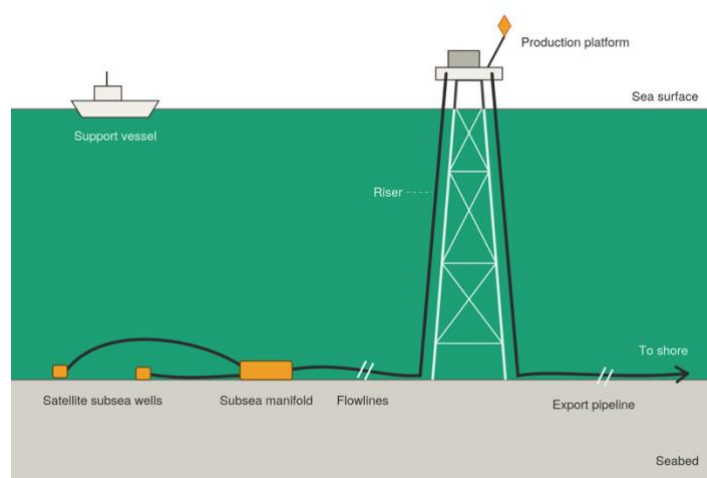


Figura 2. Sistema di infrastrutture sottomarine per il trasporto di gas e idrocarburi⁶

1.3 Le principali reti e dorsali nazionali

La rete di telecomunicazioni subacquee italiana è fortemente polarizzata attorno a tre nodi principali, ciascuno con una funzione geografica distinta nel sistema delle connettività internazionali. La Sicilia costituisce il principale hub nazionale, posizionandosi come punto di convergenza per le dorsali intercontinentali che collegano l'Europa al Medio Oriente, all'Asia e all'Africa subsahariana. Attraverso la Sicilia transitano o approdano sistemi di rilievo globale AAE-1 (Asia Africa Europe 1), che collega Hong Kong all'Europa attraverso il Mar Rosso e il Mediterraneo orientale, e 2Africa, il cavo perimetrale africano di nuova generazione co-finanziato da Meta e altri *hyperscaler* (Google, Amazon, Microsoft)⁷, destinato a diventare uno dei sistemi a più alta capacità al mondo.

La posizione della Sicilia nel bacino centrale del Mediterraneo la trasforma in un nodo di transito obbligato per i flussi di dati tra Europa e le regioni orientali e meridionali del

⁶ Adattato da: Control Solutions for Multiphase Flow: Linear and nonlinear approaches to anti-slug control - Scientific Figure on ResearchGate. Available from:

⁷ Salgado, R. (2024), Undersea Cables, Hyperscalers, and National Security, Hoover Institution, Stanford University, Aegis Series Paper No. 2304

globo. Sempre nel meridione del paese troviamo un altro importante snodo, quello di Bari che svolge la funzione di principale punto di ingresso adriatico, con un ruolo strategico per le connessioni verso i Balcani, il Medio Oriente e il Mar Nero, contribuendo a posizionare l'Italia come *gateway* digitale sull'asse adriatico-ionico. Genova e Savona costituiscono invece i principali hub tirrenici settentrionali, con collegamenti verso la Francia, la Spagna e il Nord Africa attraverso il sistema BlueMed e altri cavi che transitano nel Mar Ligure.

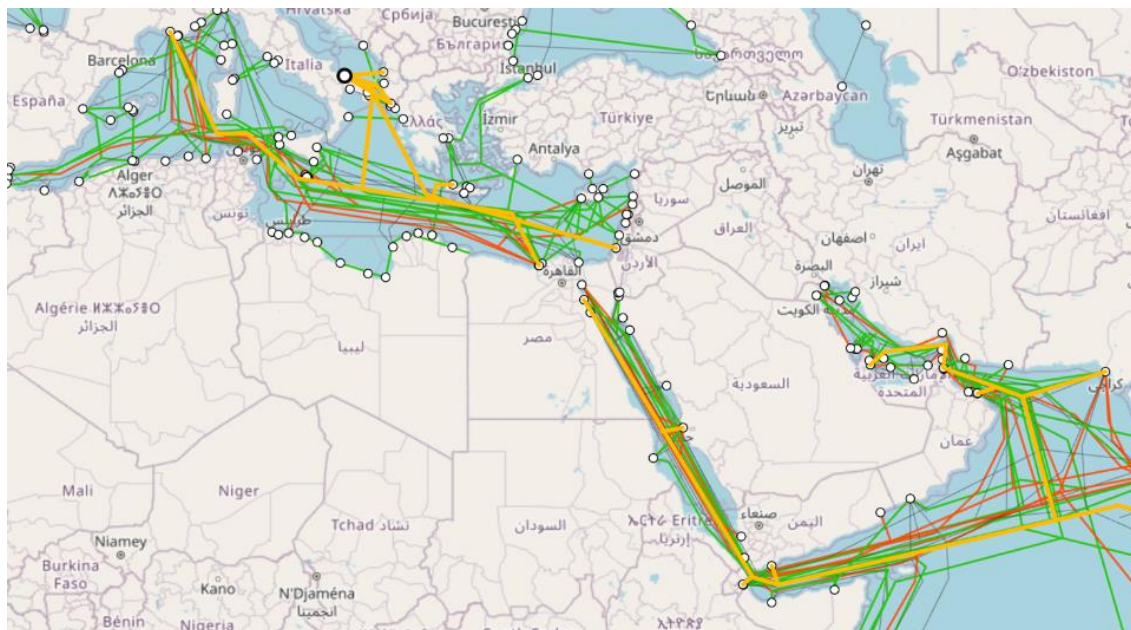


Figura 3. Mappa dei Cavi Sottomarini⁸

La struttura risulta quindi fortemente polarizzata con importanti implicazioni dirette sul profilo di rischio del sistema. La concentrazione dei landing points in poche aree geografiche, Sicilia e Puglia in primo luogo, determina l'esistenza di *single points of failure* territoriali; un danno o un'interruzione in una di queste aree avrebbe effetti immediati e difficilmente mitigabili sull'intera connettività internazionale del Paese.

Per quanto riguarda il sistema gasiero, il sistema energetico mediterraneo si sviluppa prevalentemente lungo asse nord-sud, con l'Italia che riveste un duplice ruolo, quello di mercato finale degli approvvigionamenti provenienti dall'Africa e dal Medio Oriente e quello di potenziale piattaforma di transito verso l'Europa centro-settentrionale.

Le principali infrastrutture gassiere che riguardano la dimensione subacquea italiana sono:

2. **Transmed (Trans-Mediterranean pipeline):** asse storico dell'importazione di gas algerino attraverso la Tunisia e il Canale di Sicilia, con punto di approdo proprio sull'Isola. Transmed ha rappresentato per decenni la principale arteria di approvvigionamento del Paese e continua a mantenere un ruolo strutturale nel sistema energetico nazionale accentuato anche dalla crescente centralità dell'Algeria come fornitore di gas a seguito della Guerra in Ucraina e della conseguente cessazione delle importazioni dalla Russia.

⁸ Telegeography (2026), Submarine Cable Map

3. **Greenstream;** gasdotto sottomarino che collega la Libia all'Italia attraverso il Canale di Sicilia, portando gas dal campo di Wafa e dalle installazioni costiere libiche sino alla Sicilia meridionale. La sua operatività è condizionata dalla stabilità politica libica, rendendolo un asset ad elevata vulnerabilità geopolitica.
4. **TAP (Trans Adriatic Pipeline):** infrastruttura di più recente realizzazione che porta il gas azeri dall'Azerbaijan attraverso la Georgia, la Turchia e la Grecia sino all'approdo in Puglia. Il TAP rappresenta il segmento terminale del Corridoio Meridionale del Gas (SGC) e costituisce uno degli assi strategici della diversificazione delle forniture italiane ed europee.

Complessivamente, la geografia del sistema gasiero italiano evidenzia una duplice dipendenza, sia da infrastrutture fisiche che attraversano zone marittime con elevato grado di instabilità o sotto sovranità di paesi terzi, sia da corridoi marittimi, in primo luogo i Canali di Sicilia e Otranto, che costituiscono colli di bottiglia geografici per l'intera catena di approvvigionamento.



Figura 4. Sistema Gasiero Sottomarino⁹

Il peso del vettore GNL nel mix nazionale rende questa esposizione tutt'altro che marginale. Nel 2024 il GNL ha rappresentato circa il 25% delle importazioni di gas dell'Italia, pari a circa 14,6 miliardi di metri cubi, quota salita a circa il 30% nel primo semestre 2025¹⁰. I flussi provengono da un numero ristretto di bacini di liquefazione: nel 2024 il Qatar ha fornito circa il 45% del GNL importato ($\approx 6,6$ mld mc), gli Stati Uniti circa il 35% ($\approx 5,2$ mld mc) e l'Algeria circa il 14% (≈ 2 mld mc); nel corso del 2025 gli Stati Uniti hanno superato il Qatar come primo fornitore, attestandosi intorno al 45%

⁹ Adattato da: Agenzia Nova (2022), Energia: ecco la nuova mappa dei flussi del gas in Italia

¹⁰ U.S. Department of Commerce, International Trade Administration, *Italy Energy – Liquefied Natural Gas (LNG)*, Market Intelligence, 2025, <https://www.trade.gov/market-intelligence/italy-energy-liquefied-natural-gas-lng>

delle consegne¹¹. Questi flussi convergono su cinque rigassificatori la cui geografia non è neutrale rispetto ai colli di bottiglia mediterranei: tre impianti gravitano sul bacino tirrenico-ligure (Panigaglia, OLT Livorno, FSRU Piombino), due sull'Adriatico settentrionale (Adriatic LNG/Porto Levante e l'FSRU di Ravenna, operativo da aprile 2025). Su una capacità nazionale di rigassificazione dell'ordine di 28 miliardi di metri cubi annui, i due terminali adriatici ne rappresentano oltre la metà, e il solo Porto Levante copre circa il 15% della domanda nazionale di gas¹².

È la combinazione tra direzione di provenienza e bacino di sbarco a determinare quale *choke point* risulti vincolante. I carichi in ingresso da Gibilterra (Stati Uniti e, più in generale, bacino atlantico) raggiungono i terminali tirrenici senza transitare né per il Canale di Sicilia né per quello di Otranto; per servire i terminali adriatici sono invece obbligati ad attraversare entrambi. I carichi di origine mediterranea occidentale (Algeria) servono i terminali tirrenici senza vincoli, ma incontrano il Canale di Sicilia se diretti in Adriatico. I carichi di origine mediorientale o levantina (Qatar, Egitto) entrano da Suez e devono attraversare il Canale di Sicilia per servire i rigassificatori tirrenici, o il Canale di Otranto per quelli adriatici. Ne discende un'asimmetria operativa rilevante: il Canale di Otranto in quanto l'unica via di accesso marittimo all'Adriatico settentrionale, vincola dunque in modo incondizionato, qualunque sia la provenienza del carico, l'intera capacità di rigassificazione adriatica, mentre la criticità del Canale di Sicilia è funzione del mix di approvvigionamento e cresce in proporzione alla quota di GNL in arrivo via Suez. La progressiva sostituzione della molecola qatarina con quella statunitense, accelerata dalle crisi del Mar Rosso e di Hormuz, attenua quindi la pressione sul Canale di Sicilia come corridoio di sbocco dei flussi suezini, ma non allenta in alcun modo il vincolo del Canale di Otranto sui terminali adriatici.

A questa dipendenza interna si sovrappone una dipendenza "a monte" da *choke point* extra-mediterranei sui medesimi flussi: un carico qatarino diretto a Porto Levante attraversa in serie lo Stretto di Hormuz, il Bab el-Mandeb, il Canale di Suez, e il Canale di Otranto con prossimità anche verso il canale di Sicilia. Cinque strozzature consecutive. Le prime tre sono interamente esterne al controllo nazionale ed europeo; le ultime due, pur prossime al territorio nazionale, restano corridoi di navigazione internazionale il cui regime giuridico limita gli strumenti di controllo unilaterale dello Stato costiero. La fragilità di questa catena seriale si è manifestata in due episodi recenti. La crisi del Mar Rosso ha di fatto chiuso il Bab el-Mandeb al traffico GNL dalla fine del 2023, comprimendo i transiti di metaniere via Suez da circa 32 milioni di tonnellate nel 2023 a circa 4 nel 2024, con i volumi qatarini via canale crollati a livelli trascurabili e dirottati intorno al Capo di Buona Speranza¹³. La crisi dello Stretto di Hormuz del 2026, con la chiusura dichiarata dalle forze iraniane a marzo, forse majeure di QatarEnergy a seguito degli attacchi al complesso di Ras Laffan, riapertura graduale avviata a giugno, ha temporaneamente sottratto al mercato europeo una quota significativa dell'offerta qatarina, che copre il 12-14% del GNL importato dall'Unione

¹¹ S&P Global Commodity Insights, *Italy's LNG regasification capacity growth central to Russian gas displacement: Snam*, 17 dicembre 2024, <https://www.spglobal.com/energy/en/news-research/latest-news/natural-gas/121724>

¹² Adriatic LNG, *Adriatic LNG launches Open Season 2025*, comunicato stampa, 1 settembre 2025, <https://www.adriaticlng.it/en/media/press-releases/corporate/open-season-2025-en>

¹³ Kpler, *US-Houthi truce may spur LNG flows via Red Sea and Suez Canal; gradual recovery expected*, 8 maggio 2025, <https://www.kpler.com/blog/us-houthi-truce-may-spur-lng-flows-via-red-sea-and-suez-canal-gradual-recovery-expected>

Europa¹⁴ ¹⁵. Il dato strategico per il sistema italiano è che ciascuna di queste interruzioni a monte ridistribuisce i flussi tra i terminali e, con essi, il carico sui due canali nazionali: ogni spostamento verso l'origine atlantica intensifica i transiti attraverso il Canale di Sicilia per i carichi diretti all'Adriatico, rendendo il binomio Sicilia-Otranto non un vincolo statico ma una variabile dipendente dalla geografia mutevole dell'offerta.

Il Canale di Otranto merita in questo quadro una qualificazione ulteriore: esso è al tempo stesso corridoio di transito obbligato per le metaniere dirette ai terminali adriatici e sede di infrastruttura fissa sul fondale, con il tratto offshore del TAP che vi transita per approdare a Melendugno. Nel medesimo spazio ristretto convergono dunque entrambe le dimensioni della dipendenza energetica subacquea, il flusso mobile e l'asset posato, rendendo il canale il caso più compiuto, nel perimetro nazionale, di sovrapposizione tra vulnerabilità di corridoio e vulnerabilità di infrastruttura.

Per quanto riguarda la realizzazione e la gestione delle infrastrutture elettriche sottomarine di trasmissione ad alta e altissima tensione ricadono principalmente sotto la responsabilità di Terna, in qualità di gestore della Rete di Trasmissione Nazionale (RTN). In questo caso, il portafogli di asset sottomarini di Terna comprende alcune delle infrastrutture tecnologicamente più avanzate del bacino mediterraneo.

I collegamenti di maggiore rilevanza sistemica si trovano nel bacino tirrenico ed includono:

5. **SA.PE.I. (Sardinia-Peninsula Interconnection):** collegamento HVDC a 500 kV con capacità di 1.000 MW e sviluppo complessivo di circa 435 km, di cui oltre 420 km in tratto sottomarino. Il cavo raggiunge profondità dell'ordine di 1.600 metri, collocandosi tra le infrastrutture HVDC più profonde al mondo al momento della sua realizzazione, nonché il cavo sottomarino da 1.000 MW più lungo al mondo.
6. **Sa.Co.I.3 (Sardinia-Corsica-Italy 3):** nuova infrastruttura in tecnologia HVDC destinata a sostituire e potenziare il collegamento esistente, migliorando le capacità di scambio energetico tra Sardegna, Corsica e Toscana.
7. **Tyrrhenian Link:** progetto di salto di scala infrastrutturale che prevede un doppio collegamento HVDC a 500 kV articolato in due rami - uno tra Sicilia e Campania (ramo est) e uno tra Sicilia e Sardegna (ramo ovest) - per uno sviluppo complessivo di circa 970 km e una capacità di trasmissione di 1.000 MW per ciascun ramo. Concepito come corridoio strategico nel Mediterraneo centrale, è finalizzato a incrementare la capacità di scambio tra macro-zone di mercato e a facilitare l'integrazione delle energie rinnovabili nel Mezzogiorno

Sul versante adriatico, l'infrastruttura di maggiore rilievo è l'interconnessione Italia-Montenegro: collegamento HVDC di circa 445km (di cui oltre 420km in mare) con una capacità di 600 MW, che consente lo scambio bidirezionale tra la rete italiana e quella balcanica. In parallelo, si sviluppa il progetto GRITA 2 con il gestore greco IPTO (Independent Power Transmission Operator), che prevede un nuovo elettrodotto

¹⁴ Congressional Research Service, *Iran Conflict and the Strait of Hormuz: Impacts on Oil, Gas, and Other Commodities*, R45281, Washington D.C., 2026, <https://www.congress.gov/crs-product/R45281>

¹⁵ Bloomberg, *Qatar plans quick LNG output recovery as Hormuz reopening nears*, 16 giugno 2026, <https://www.bloomberg.com/news/articles/2026-06-16/qatar-plans-to-rapidly-restart-lng-production-after-hormuz-opens>

sottomarino fino a 1.000 MW per una lunghezza complessiva di circa 300km (di cui circa 240 km in mare), finalizzato a rafforzare l'integrazione del mercato elettrico dell'Europa sud-orientale. Anche per quanto riguarda le infrastrutture elettriche sottomarine, il Canale di Sicilia rimane rilevante con l'interconnessione Italia-Tunisia (ELMED). ELMED, con capacità prevista di 600 MW e lunghezza stimata tra i 200 e i 220 km, è sviluppata da Terna in collaborazione con STEG (*Société Tunisienne d'Electricité et du Gaz*) con l'obiettivo di connettere direttamente i sistemi elettrici europeo e nordafricano, favorendo l'integrazione di nuova capacità rinnovabile e rafforzando la sicurezza energetica nel bacino centrale del Mediterraneo.

A queste infrastrutture si aggiungono infine quelle sul fronte della generazione eolica offshore: l'Italia si trova in una fase di rapida espansione progettuale che avrà riflessi diretti sull'estensione del sistema di cavi elettrici sottomarini. Ad oggi, risultano depositati 93 progetti di impianti eolici offshore distribuiti nelle acque di dieci regioni costiere, per una potenza aggregata nell'ordine di decine di gigawatt. La quasi totalità delle proposte (88 su 93) riguarda impianti a tecnologia galleggiante, con distanza media dalla costa superiore ai 30 chilometri. Le Regioni con il maggior numero di iniziative sono Puglia (26 progetti), Sicilia (25) e Sardegna (24), delineando un asse meridionale quale principale area di sviluppo del settore. L'espansione attesa dell'eolico *offshore* aumenterà significativamente la superficie di esposizione dell'Italia nella dimensione subacquea, aggiungendo nuovi cavi di connessione alla rete continentale, nuovi nodi logistici costieri e nuove interdipendenze sistemiche tra produzione offshore e rete di trasmissione.

1.4 Choke points e aree di maggiore vulnerabilità

L'analisi congiunta della distribuzione delle infrastrutture di telecomunicazione, del sistema gasiero e della rete elettrica sottomarina rileva una struttura geografica caratterizzata da forte concentrazione spaziale, interdipendenza settoriale e connessione a *choke point* di rilevanza sia regionale che globale. Questa configurazione determina un profilo di rischio che non è semplicemente la somma dei rischi di ciascuna infrastruttura considerata singolarmente, ma un rischio sistemico emergente dalla loro sovrapposizione in spazi geografici ristretti. Complessivamente, anche la mappa dei punti di approdo conferma una dinamica di forte concentrazione. Una quota rilevante dei landing point dei cavi per telecomunicazioni, una parte significativa degli approdi dei gasdotti e degli elettrodotti transnazionali si concentra in poche regioni, configurando potenziali *single points of failure* di natura territoriale.

Il Canale di Sicilia e il Mediterraneo centrale costituiscono l'area di maggiore sensibilità strategica per l'Italia. In questo corridoio si sovrappongono in modo particolarmente evidente le principali rotte di comunicazione ed energetiche: dorsali internet intercontinentali, gasdotti provenienti dal Nord Africa e cavi elettrici transnazionali di nuova generazione convergono verso i medesimi approdi siciliani nel medesimo spazio marittimo. La Sicilia è al contempo punto di atterraggio e transito per dorsali internet che collegano Europa, Medio Oriente e Asia, e concentra approdi e infrastrutture energetiche dal continente africano. Questa convergenza aumenta la resilienza soltanto se accompagnata da ridondanza e capacità di ripristino: in assenza di tali condizioni, trasforma invece il territorio in un moltiplicatore di rischio, in cui un incidente o un atto ostile in un'area geograficamente ristretta può generare effetti a cascata sia sul traffico dati che sui flussi energetici. Il quadrante adriatico-ionico, e in particolare il Canale di Otranto, costituisce poi un secondo corridoio di elevata rilevanza strategica.

In questo spazio convergono il gasdotto TAP, i cavi elettrici transnazionali verso la Grecia e i Balcani, e direttrici digitali di crescente importanza. La vicinanza geografica con aree di instabilità nel Mediterraneo orientale amplifica la valenza strategica di questo corridoio.

Se estendiamo poi l'analisi oltre il perimetro nazionale, emerge un ulteriore vulnerabilità: i *choke point* globali condizionano l'integrità delle infrastrutture italiane pur trovandosi al di fuori della sovranità, della giurisdizione o comunque della prossimità geografica dello Stato. Il caso più evidente è il Canale di Suez, che costituisce un *choke point* globale per i flussi di dati tra Europa e Asia: La concentrazione di dorsali internet che transitano per questo canale, e la loro esposizione a dinamiche di instabilità regionale, rende l'Italia indirettamente vulnerabile a eventi che si verificano a migliaia di chilometri dalle sue coste.¹⁶

Il profilo di rischio più rilevante non è esclusivamente quello dell'attacco deliberato. La fragilità sistemica prodotta da incidenti accidentali, da eventi naturali e dall'effetto domino tra danni a reti energetiche e digitali rappresenta una minaccia altrettanto concreta la cui gestione richiede un approccio integrato che le successive sezioni si propongono di analizzare e sviluppare a partire dal contesto normativo per la realizzazione, la gestione e la protezione delle infrastrutture, per poi analizzare rischi specifici e possibili soluzioni di difesa.

¹⁶ Come spiegato nei paragrafi successivi, anche azioni cinetiche in superficie non direttamente rivolte verso le condutture subacquee, come attacchi alle navi mercantili o alle navi di riparazioni, possono avere ripercussioni sulla resilienza delle infrastrutture sui fondali.

8. Perimetro normativo e giurisdizionale della Dimensione subacquea

Tra le principali questioni giuridiche che riguardano le infrastrutture critiche sottomarine, due sono oggetto di crescente attenzione: l'ambito delle competenze degli attori e la responsabilità degli stessi. Per quanto riguarda l'ambito delle competenze, il dibattito verte sull'effettivo spazio di manovra delle forze armate per il monitoraggio, la sorveglianza, la prevenzione e l'intervento in caso di azioni criminali avverso le infrastrutture avvenute in spazi marittimi internazionali. Per quanto riguarda la questione della responsabilità, è controverso sia se le aziende proprietarie delle infrastrutture che forniscono un bene pubblico siano responsabili dei danni subiti dalla società, sia se le forze armate siano responsabili della funzionalità delle aziende. In entrambi casi, si discute di omissione, di negligenza e di prontezza nel ripristino del servizio pubblico e dell'eventuale risarcimento dei danni sofferti e dei costi affrontati dalla società.

2.1 La sovranità e la giurisdizione dello Stato costiero

La Convenzione delle Nazioni Unite sul diritto del mare del 10 dicembre 1982 (CNUDM)¹⁷ costituisce il principale strumento di codificazione del diritto del mare e individua con chiarezza le prerogative dello Stato costiero negli spazi marittimi antistanti la costa.

Nelle acque territoriali, lo Stato costiero esercita, in particolare, sovranità piena sul fondale, sul suolo e sul sottosuolo sottostanti, potendo disciplinare con leggi e regolamenti la posa e la protezione di cavi, condotte e infrastrutture, anche nel quadro della regolamentazione del passaggio inoffensivo (art. 21 CNUDM). Lo Stato costiero può proteggere cavi e condotte, fermo restando che le sue leggi non possono riguardare la progettazione, la costruzione, l'armamento e l'allestimento delle navi straniere a meno che diano attuazione a norme o regolamenti internazionali generalmente accettati (ad es., i regolamenti dell'International Maritime Organisation).

Nella zona contigua, la CNUDM riconosce allo Stato costiero poteri di *enforcement* preventivi o repressivi in caso di violazioni di leggi e regolamenti in materia doganale, fiscale, sanitaria e di immigrazione commesse sulla terraferma, nelle acque interne e nel mare territoriale (art. 33). Vige un generico regime di libertà di navigazione, anche in immersione. È altresì riconosciuta agli altri Stati la libertà di posare condotte e cavi sottomarini, nel rispetto del regime della piattaforma continentale o della Zona economica esclusiva (ZEE) eventualmente applicabile oltre i limiti esterni del mare territoriale. Con legge 7 maggio 2026 n. 70, l'Italia ha avviato l'iter di proclamazione della zona contigua con conseguente aggiornamento delle linee di base.

Nella ZEE, la CNUDM opera un bilanciamento tra i diritti sovrani dello Stato costiero in materia di esplorazione, sfruttamento e conservazione delle risorse e la libertà degli altri Stati di posare cavi e condotte. I diritti sovrani includono poteri coercitivi (art. 73 CNUDM) e concorrono con i poteri giurisdizionali nell'ambito di attività economiche relative alle acque, al fondo del mare, al suolo e al sottosuolo (art. 56 CNUDM). In questo spazio, lo Stato costiero può istituire "zone di sicurezza" di dimensioni

¹⁷ Convenzione delle Nazioni Unite sul diritto del mare, Montego Bay, 10 dicembre 1982, UNTS 1833. In vigore dal 16 novembre 1994.

ragionevoli intorno alle infrastrutture (art. 60 CNUDM), strumento potenzialmente funzionale alla protezione delle infrastrutture sottomarine critiche.

Per quanto riguarda la piattaforma continentale, l'art. 79 CNUDM riconosce il diritto di tutti gli Stati a posare cavi e condotte, ma conferisce allo Stato costiero il diritto di adottare misure e stabilire condizioni quando le infrastrutture siano connesse allo sfruttamento delle proprie risorse, al suo mare territoriale o al suo territorio. Tutti gli Stati devono tenere conto delle infrastrutture già in posizione, al fine di non pregiudicarne la riparazione.

Open point: La definizione e l'implementazione pratica delle "zone di sicurezza" ex art. 60 CNUDM attorno a infrastrutture sottomarine critiche italiane nella ZEE richiedono un'elaborazione operativa e normativa specifica, in coordinamento con l'Agenzia per la sicurezza delle attività subacquee (ASAS). L'assenza di perimetri formalmente delimitati riduce la capacità di deterrenza e di enforcement preventivo.

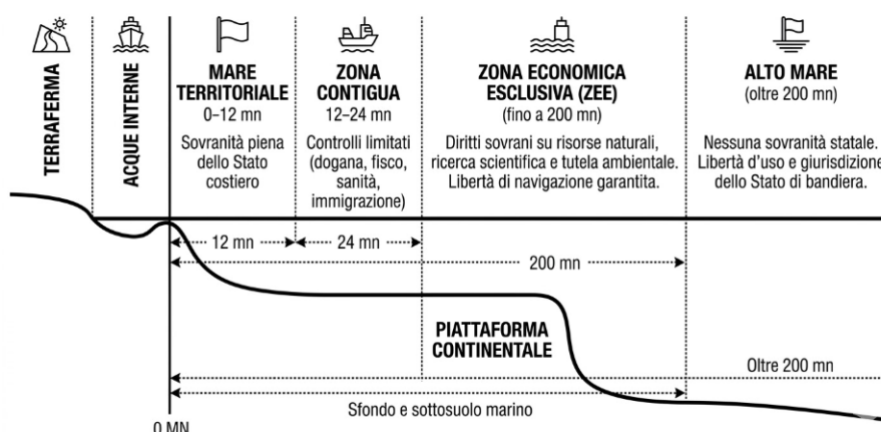


Figura 5. Ripartizione degli spazi marittimi secondo la CNUDM¹⁸

2.2 Le zone d'ombra dell'alto mare: limiti dei meccanismi di enforcement e vuoti normativi

È nell'alto mare e nei fondali al di là della piattaforma continentale che il quadro normativo rivela le proprie lacune più critiche. L'art. 87 CNUDM include la posa di cavi e condotte tra le libertà degli Stati, mentre l'art. 112 ne sancisce il diritto di posa oltre la piattaforma continentale. Tuttavia, i meccanismi di protezione e i poteri di enforcement restano gravemente insufficienti di fronte alle minacce contemporanee.

L'art. 113 CNUDM obbliga gli Stati a criminalizzare nei propri ordinamenti la rottura o il danneggiamento doloso o colposo di cavi e condotte in alto mare da parte di navi di bandiera o di persone soggette alla loro giurisdizione. Gli artt. 114 e 115 prevedono rispettivamente la responsabilità per i danni causati a infrastrutture altrui durante operazioni di posa e l'obbligo di indennizzare i proprietari di una nave che abbiano sacrificato attrezzature per evitare danni ai cavi. Questo corpus normativo, tuttavia, non è stato uniformemente attuato dagli Stati e si fonda interamente sulla

¹⁸ Elaborazione degli autori su CNUDM

cooperazione dello Stato di bandiera e sulla sua disponibilità ad attivare la propria giurisdizione penale, un presupposto che si rivela spesso illusorio.

Peraltro, il meccanismo di giurisdizione esclusiva dello Stato di bandiera crea una vulnerabilità strutturale in caso di navi appartenenti a "flotte ombra" o battenti bandiere di comodo che operano in alto mare danneggiando infrastrutture. In tali casi, non sussiste un controllo effettivo da parte dello Stato di bandiera e lo Stato costiero danneggiato non dispone, dalla visuale di queste disposizioni, di alcun titolo giuridico autonomo per intervenire, fermare o sequestrare tali navi.

La Convenzione di Parigi del 14 marzo 1884 sulla protezione dei cavi telegrafici sottomarini, la cui applicazione è salvaguardata dall'art. 311 CNUDM, è tuttora vigente nei rapporti tra i 36 Stati contraenti, tra cui l'Italia e gli Stati Uniti, ed attribuisce giurisdizione penale ai tribunali dello Stato di bandiera per i reati commessi a bordo di navi (art. VIII). Sebbene in via interpretativa la convenzione possa coprire i cavi elettrici, i cavi in fibra ottica e i cavi telefonici, essa resta inadeguata su più fronti: non copre i reati non commessi a bordo, è priva di effettività al cospetto di navi prive di bandiera o battenti bandiera ombra, e non prevede poteri di visita e ispezione senza il consenso dello Stato di bandiera.

Il diritto di visita e ispezione attribuito alle navi da guerra in alto mare è infatti limitato all'accertamento della nazionalità della nave e all'acquisizione di prove sui fatti controversi (art. 10 della Convenzione del 1884). In ogni caso, il *boarding* per sequestro o dirottamento rimane condizionato al consenso dello Stato di bandiera. Il diritto di visita di cui all'art. 110 CNUDM è più ampio, ma riguarda ipotesi tassativamente elencate nelle quali non rientra il danneggiamento di un cavo o di un'infrastruttura sottomarina.

Taluni commentatori hanno proposto di ricondurre gli attacchi a cavi e condotte sotto la fattispecie della pirateria (artt. 100-106 CNUDM), con ciò giustificando il diritto di visita ai sensi dell'art. 110 e la giurisdizione universale ai sensi dell'art. 105, ma tale interpretazione non convince: la pirateria richiede il perseguimento di fini privati, mentre gli attacchi più pericolosi alle infrastrutture subacquee sono generalmente motivati da ragioni politiche, strategiche o ibride.

Il diritto di inseguimento ex art. 111 CNUDM consente allo Stato costiero di estendere la giurisdizione in alto mare su navi straniere che abbiano commesso illeciti nelle acque soggette alla propria sovranità. Questo strumento è applicabile laddove il danneggiamento di un'infrastruttura abbia origine o effetti nelle acque territoriali o nella ZEE italiana in violazione delle leggi italiane, e costituisce una leva operativa rilevante per la Marina Militare, da attivare tempestivamente prima che la nave straniera raggiunga le acque territoriali di un altro Stato.

La figura dell'"incidente di navigazione" ex art. 97 CNUDM potrebbe coprire i danni a "*submarine telegraph, telephone or high-voltage power cable or to a pipeline*" secondo l'*International Law Commission* delle Nazioni Unite. La disposizione giustifica l'esercizio della giurisdizione penale sia dello Stato di bandiera che dello Stato di nazionalità del comandante o del membro dell'equipaggio responsabile. Tuttavia, solo lo Stato di bandiera conserva il potere di fermare e sequestrare la nave (art. 97, par. 3). Ne consegue che, anche in presenza di un incidente che coinvolga un'infrastruttura italiana in alto mare, la Marina Militare non può procedere all'arresto della nave senza il consenso dello Stato di bandiera.

In questo scenario, quando l'incidente in mare genera inquinamento, l'art. 221 CNUDM consente agli Stati costieri di adottare, al di là del mare territoriale, misure proporzionate al danno subito o prevedibile, al fine di proteggere le proprie coste dall'inquinamento o da una minaccia di inquinamento. Pur non riferendosi esplicitamente ai danni alle infrastrutture, la norma può essere invocata in via estensiva per legittimare interventi di emergenza anche in alto mare, qualora vi sia rischio di contaminazione o di danni ambientali connessi al danneggiamento di condotte.

2.3 Altri strumenti internazionali rilevanti e profili di responsabilità

Oltre alla CNUDM, alcuni strumenti internazionali possono giustificare l'esercizio della giurisdizione penale in base al collegamento territoriale degli effetti del reato, alla nazionalità dell'autore o della vittima, ovvero al principio di protezione di interessi comuni a più Stati. La Convenzione delle Nazioni Unite del 15 dicembre 2000 contro il crimine organizzato transnazionale (Convenzione di Palermo)¹⁹ offre in proposito una cornice applicabile quando i danneggiamenti alle infrastrutture assumano le caratteristiche di fattispecie criminose organizzate e transfrontaliere rientranti nella Convenzione.

La Convenzione di Roma del 10 marzo 1988 per la repressione degli atti illeciti contro la sicurezza della navigazione marittima²⁰ presenta invece limiti applicativi rispetto alle infrastrutture subacquee in alto mare: pur coprendo reati contro la navigazione, inclusi quelli che coinvolgono sottomarini, potenzialmente configurabili come reati-presupposto al danneggiamento di infrastrutture, essa non si estende agevolmente alle condotte lesive compiute direttamente contro cavi o condotte.

Sul piano degli investimenti internazionali, numerosi trattati bilaterali (BIT) includono le zone marittime nella nozione di "territorio" e possono classificare le infrastrutture sottomarine come "investimento estero diretto". La clausola di "*full protection and security*" prevista dalla maggioranza dei BIT impone allo Stato ospite obblighi positivi di protezione fisica, con potenziali implicazioni sulla responsabilità internazionale dello Stato costiero in caso di danneggiamento di infrastrutture di proprietà straniera operate nel proprio spazio marittimo.

Open point: La base giuridica della giurisdizione dello Stato di nazionalità del proprietario dell'infrastruttura subacquea in alto mare rimane incerta e non codificata. L'assenza di un titolo convenzionale chiaro espone gli interventi della Marina Militare a contestazioni di legalità in sede internazionale, richiedendo una valutazione caso per caso della sussistenza di basi giuridiche alternative, anche in combinazione con accordi bilaterali o multilaterali di cooperazione.

2.4 Il quadro normativo italiano: la legge 9/2026 e le nuove competenze della Marina Militare

¹⁹ Convenzione delle Nazioni Unite contro il crimine organizzato transnazionale (Convenzione di Palermo), 15 dicembre 2000, UNTS 2225.

²⁰ Convenzione per la repressione degli atti illeciti contro la sicurezza della navigazione marittima, Roma, 10 marzo 1988, UNTS 1678.

A livello nazionale, la legge 26 gennaio 2026 n. 9 (legge 9/2026)²¹ ha significativamente riformato il Codice dell'ordinamento militare (COM), introducendo disposizioni espressamente dedicate alla protezione delle infrastrutture subacquee di interesse nazionale. La definizione di tali infrastrutture, contenuta all'art. 2, par. 1, lett. n), copre, a determinate condizioni, sia le installazioni situate in spazi marittimi italiani sia quelle dislocate in alto mare, riflettendo la realtà operativa di una rete infrastrutturale che si estende ben al di là delle acque territoriali.

Sul piano delle prerogative della Marina Militare, la riforma è articolata su più livelli. L'art. 111, comma 1, lett. d-ter COM contempla ora la protezione dell'infrastruttura subacquea nazionale mediante l'uso della forza in caso di distruzione, danneggiamento o manomissione, nel rispetto del diritto internazionale applicabile. L'art. 111, comma 1, lett. d-quater attribuisce alla Marina il controllo nelle acque interne, nel mare territoriale e nella piattaforma continentale per fini di difesa militare, includendo espressamente la prevenzione della navigazione subacquea non autorizzata. L'art. 111, comma 1, lett. d-quinquies istituisce la competenza a cooperare con le Marine militari di Stati alleati o confinanti per la vigilanza delle infrastrutture subacquee.

La stessa legge 9/2026 ha istituito l'ASAS, chiamata a svolgere funzioni di coordinamento, rappresentanza internazionale e sviluppo di politiche di protezione delle infrastrutture subacquee, anche negli spazi privi di sovranità e di giurisdizione. L'ASAS è tenuta a operare in stretto raccordo con la Marina Militare, nonché con l'Agenzia per la Cybersicurezza Nazionale (ACN) in considerazione della natura duale — fisica e digitale — delle minacce alle infrastrutture sottomarine. Un analogo raccordo dovrebbe sussistere con l'Agenzia dell'UE per la Cybersicurezza (ENISA) al di là dei dettami della legge 9/2026.

Tema centrale rimane quello della responsabilità. Mentre le infrastrutture sottomarine critiche sono assoggettate al regime unionale di *compliance*, il comparto militare interviene nella gestione delle crisi connesse in un'ottica di sicurezza nazionale. In caso di omissioni o negligenza nell'esercizio delle attività di sorveglianza e protezione, la responsabilità è a carico dello Stato, in conseguenza dei comportamenti delle sue forze armate. D'altro canto, la Marina Militare può operare come stazione appaltante se si avvale di privati per organizzare al meglio le funzioni di sorveglianza e protezione. In tal caso, la responsabilità è a carico del soggetto titolare dei compiti di sorveglianza e protezione, ma azioni di regresso sono possibili ove il danno derivi da malfunzionamenti del servizio appaltato al player privato.

La Marina Militare svolge attività di sorveglianza, offre supporto tecnico-operativo e interviene in situazioni di emergenza. Conviene ricordare che la legge 9/2026 le assegna tali funzioni in raccordo con l'ampia nozione di «infrastrutture subacquee di interesse nazionale». I protocolli d'intesa tra la Marina Militare e i soggetti critici ripartiscono, in particolare, i compiti di sorveglianza e assistenza, affinché la tecnologia sviluppata dai secondi serva alle funzioni di sicurezza svolte dalla prima. In linea di principio, tali protocolli non alterano il quadro delle titolarità e delle responsabilità dei partner. Il soggetto critico mantiene la proprietà o comproprietà del cavo, il che comporta la responsabilità nell'ambito della manutenzione e della continuità del servizio tecnico. La Marina Militare assume funzioni e responsabilità in materia di sicurezza e protezione

²¹ Legge 26 gennaio 2026, n. 9, recante disposizioni in materia di sicurezza delle attività subacquee e modifica del Codice dell'ordinamento militare (d.lgs. 15 marzo 2010, n. 66).

da agenti esterni. Le due responsabilità sono collocate su piani differenti purché l'attività sia svolta in conformità ai protocolli di intesa o ad altro accordo.

La legge 9/2026 rende chiaro che la competenza della Marina si estende ben oltre i limiti spaziali della sovranità italiana in caso di «infrastrutture subacquee di interesse nazionale» dislocate in alto mare, con approdo o partenza dal territorio italiano. Di conseguenza, forme di negligenza o imperizia che causano o concorrono a causare il verificarsi di un «incidente» in alto mare sono imputabili alla Marina Militare in generale, qualora di stanza a presidio dell'infrastruttura di interesse nazionale e, nel quadro CER in particolare, se gli effetti dell'incidente si concretizzano anche (o soltanto) nel territorio italiano. Del pari, le responsabilità del soggetto critico si estendono all'intera struttura, per la parte di competenza del soggetto stesso, eventualmente definita in base ad accordi con partner stranieri. Qualunque fatto che incida sulla resilienza del cavo in territorio italiano, genera responsabilità a prescindere da dove esso sia accaduto (es. in alto mare) qualora, rispetto al fatto (es. difetto di manutenzione) tale responsabilità sia imputabile al soggetto critico.

Open point: Le direttive europee NIS 2²² e CER²³ non si applicano ai comparti dell'amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa (art. 1, par. 6 CER; art. 2, par. 7 NIS2). Tuttavia, i soggetti critici privati titolari o contitolari di cavi e infrastrutture vi sono soggetti. La Marina Militare è chiamata a interagire con tali soggetti attraverso protocolli d'intesa che ripartiscano in modo chiaro le responsabilità: i soggetti critici mantengono la responsabilità per la manutenzione e la continuità del servizio; la Marina assume le funzioni di sicurezza e protezione da minacce esterne. La Raccomandazione (UE) 2024/779²⁴ e l'EU Action Plan on Cable Security orientano verso un approccio olistico e integrato, cui la Marina è chiamata a contribuire attivamente.

2.5 Spunti di cooperazione e proiezione strategica

La cooperazione internazionale è lo strumento imprescindibile per colmare i vuoti normativi che caratterizzano la dimensione dell'alto mare. In assenza di meccanismi multilaterali coercitivi, la strada più efficace nel breve-medio termine è quella della cooperazione operativa e del *soft law*: elaborazione di principi condivisi, raccolte di buone pratiche, intese bilaterali e multilaterali per la sorveglianza congiunta e lo scambio di informazioni.

Un esempio rilevante, anche se di portata regionale, è rappresentato dalle iniziative di coordinamento avviate in ambito NATO per la protezione delle infrastrutture critiche sottomarine nel teatro nordatlantico²⁵, in risposta agli episodi di danneggiamento ai gasdotti Nord Stream nel settembre 2022, la cui attribuzione rimane tuttora controversa. Tali episodi hanno dimostrato che la vulnerabilità delle infrastrutture subacquee non è teorica, e che gli strumenti di risposta giuridica e operativa disponibili si sono rivelati insufficienti nella fase immediatamente successiva all'incidente. Un

²² Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio (NIS 2), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, GU L 333, 27.12.2022.

²³ Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio (CER), relativa alla resilienza dei soggetti critici, GU L 333, 27.12.2022.

²⁴ Raccomandazione (UE) 2024/779 del 26 febbraio 2024 della Commissione europea sulla sicurezza dei cavi sottomarini, GU L, 8 marzo 2024.

²⁵ NATO, "NATO steps up its support to protect critical undersea infrastructure," comunicato stampa, 2022. Disponibile su: <https://www.nato.int>

quadro più recente di cooperazione operativa è stato tracciato dai *Guiding Principles for Underwater Infrastructure Defence Exchanges (GUIDE)*²⁶.

La Marina Militare è ora espressamente abilitata dal COM, come novellato dalla legge 9/2026, a promuovere e partecipare a forme di cooperazione con le marine militari di Stati alleati o confinanti per la vigilanza delle infrastrutture subacquee. Tale competenza dovrebbe tradursi in accordi tecnico-operativi che prevedano sorveglianza coordinata, condivisione di dati d'intelligence, protocolli di risposta rapida e definizione di responsabilità condivise — anche nelle zone al di là della giurisdizione nazionale. Insieme all'ASAS, la Marina può candidarsi a svolgere un ruolo propulsore nella definizione di standard comuni a livello Euro-Atlantico, contribuendo a ridurre la frammentarietà normativa che oggi favorisce l'impunità degli attori ostili.

Open point: La classificazione delle infrastrutture subacquee come obiettivi militari in un conflitto armato è ammessa dal diritto dei conflitti armati quando tali infrastrutture siano funzionali alle operazioni delle forze armate nemiche o al loro sforzo bellico. La IV e la V Convenzione dell'Aia disciplinano le condizioni di liceità, tra cui il principio di "assoluta necessità", il rispetto delle acque neutrali e il divieto di distruggere cavi collegati a uno Stato neutrale. La Marina Militare deve integrare questi vincoli nella propria dottrina operativa, specialmente in scenari di crisi a intensità variabile.

²⁶ Lanciata nel maggio 2026 a margine del 23° Shangri-La Dialogue di Singapore, l'iniziativa coinvolge 17 Stati (tra cui l'Italia) e intende attuare un quadro di cooperazione internazionale in materia di difesa a supporto della sicurezza delle infrastrutture sottomarine critiche.

9. Rischi e minacce alle infrastrutture sottomarine

Le minacce di oggi sono ridotte rispetto alle potenziali minacce future a motivo di almeno tre elementi fondamentali: 1) la proliferazione di armamenti a basso costo come i droni marini, 2) l'aumento delle tensioni internazionali; 3) la predisposizione di future minacce (mappatura delle infrastrutture, pre-posizionamento di strumenti latenti etc.) che potrebbero avere un impatto significativo in caso di conflitti futuri.

3.1 Perimetro di analisi

Una delle acquisizioni concettuali più importanti dell'analisi del rischio nella dimensione subacquea è il superamento della visione riduzionistica che considera l'infrastruttura esclusivamente come oggetto fisico intesa come cavo, condotta, tubo di acciaio adagiato sul fondale. Le infrastrutture subacquee sono sistemi complessi, articolati in componenti fisiche, digitali e organizzative che interagiscono lungo un ciclo di vita esteso nel tempo e distribuito nello spazio. Ne consegue che la sicurezza dell'infrastruttura non è riducibile alla protezione del tratto sommerso (*wet plant*), ma dipende dall'affidabilità operativa dell'intero sistema²⁷.

Questo principio ha implicazioni operative dirette. Un'infrastruttura fisicamente intatta può essere compromessa da un attacco al suo sistema di gestione digitale, un cavo pienamente funzionale può diventare inutilizzabile se la stazione di atterraggio che lo collega alla rete terrestre è fuori uso. Un gasdotto perfettamente integro può essere reso inoperabile se la nave di manutenzione che dovrebbe intervenire in caso di guasto non riesce ad accedere alle acque territoriali dello stato costiero pertinente. In questo contesto, ogni analisi che si limitasse alla sola componente sommersa, mancherebbe la sostanza del problema.

Ne consegue che l'infrastruttura sottomarina va trattata come sistema socio-tecnico distribuito e non come semplice manufatto lineare posato sul fondale. Infatti, la vulnerabilità non coincide con la sola esposizione fisica del cavo o della pipeline, ma con la combinazione di: (i) concentrazione dei nodi terrestri e logistici; (ii) dipendenze industriali e di supply chain; (iii) dipendenze informative e digitali; (iv) capacità di intervento e riparazione; (v) cornici regolatorie e autorizzative che condizionano tempi di risposta e recovery. La superficie d'attacco e di guasto è quindi distribuita lungo una filiera di asset, attori e processi eterogenei. Questo ha implicazioni dirette per l'impostazione di qualsiasi piano di protezione e sorveglianza.

3.1.1 I cinque livelli del sistema infrastrutturale

Ai fini analitici, il ciclo di vita di un'infrastruttura subacquea si articola in cinque fasi distinte, ciascuna con specifiche vulnerabilità.

L'estensione di questo ciclo di vita e le diverse esposizioni al rischio che l'infrastruttura ha in ciascuna fase determinano la necessità di un approccio alla difesa con una visione ampia del problema e delle minacce, tale da non trascurare possibili punti ciechi o la difesa di un aspetto specifico.

²⁷ European Commission Expert Group, Report on the Security and Resilience of EU Submarine Cable Infrastructures, 2025.

Governance e pianificazione: Il primo livello riguarda gli attori e le dinamiche che influenzano l'assetto proprietario e la rotta dell'infrastruttura. Le pipeline sono prevalentemente di proprietà di compagnie energetiche interessate a collegare i propri giacimenti offshore ai mercati di sbocco; i cavi di comunicazione appartengono a big tech o consorzi di aziende di telecomunicazioni; i cavi elettrici appartengono per lo più ai gestori dei sistemi di trasmissione (TSO).

L'iniziativa tende a essere prevalentemente privata, anche se il ruolo dello Stato può assumere un peso significativo in presenza di imprese a partecipazione pubblica o operanti in settori strategici. La rotta delle infrastrutture è influenzata da esigenze commerciali, morfologia dei fondali, traffico marittimo e impatti ambientali sull'ecosistema marino²⁸.

Costruzione e supply chain. Il secondo livello riguarda la costruzione, l'assemblaggio e la supply chain dell'infrastruttura. Gli attori principali sono poche aziende altamente specializzate (suppliers) cui i proprietari affidano la realizzazione. La concentrazione di mercato tra un numero ristretto di produttori (Alcatel Submarine Networks, Subcom, NEC Corporation ed Elettra TLC) crea dipendenze strutturali difficilmente reversibili nel breve periodo²⁹.

Installazione. Il terzo livello riguarda la posa dell'infrastruttura sui fondali marini, affidata a navi altamente specializzate. Nel caso dei cavi di comunicazione ed elettrici l'installazione è svolta da un numero limitato di navi posacavi dotate di sistemi di posizionamento dinamico; per le pipeline energetiche si impiegano *Construction Service Vessels* (CSV) progettate per operazioni complesse di saldatura e posa. In fase di installazione, entrambe le tipologie di infrastruttura possono essere interrare per aumentare la protezione tramite aratri marini o ROV fino a circa 1.000–1.500 m di profondità. La batimetria incide sul diametro del cavo: nei primi metri la conduttura è più spessa, decrescendo in spessore all'aumentare della profondità.

Esercizio. Il quarto livello riguarda la gestione ordinaria dell'infrastruttura dopo l'installazione. Per i cavi di comunicazione, la messa in esercizio include il collaudo *end-to-end*, la configurazione degli apparati alle estremità (*terminal equipment*) e l'attivazione dei sistemi di monitoring OSS/NMS per il rilevamento di guasti, degradazioni e anomalie. Vengono inoltre allocate capacità commerciali (IRU, leasing) e configurati i meccanismi di protezione e ripristino (*rerouting, switching automatico*, soglie di allarme).

Per i cavi elettrici HVDC, la messa in esercizio richiede prove di isolamento, collaudi delle stazioni di conversione e integrazione con le funzioni di esercizio del gestore di rete. Per le pipeline offshore, la fase include attività di *pre-commissioning*, avvio controllato del flusso e calibrazione dei sistemi SCADA.

Riparazione e manutenzione. Il quinto livello riguarda la risposta a guasti e danneggiamenti. La riparazione è responsabilità delle aziende proprietarie ma viene affidata a soggetti privati con navi specializzate, spesso diverse da quelle impiegate per l'installazione. Per cavi elettrici e pipeline, i TSO stipulano framework agreement pluriennali con specifiche società di riparazione. Per i cavi di comunicazione esistono club agreement (con condivisione di risorse tra più proprietari) e *private maintenance*

²⁸ European Maritime Spatial Planning, Cables and pipelines & Marine protection and restoration.
²⁹ Submarine Telecoms Forum (2026), Industry Report 2025-2026.

agreement (con controllo diretto del proprietario). Il tempo medio globale tra individuazione del guasto e ripristino è di circa quaranta giorni, una finestra di esposizione strategicamente rilevante.

I moderni sistemi via cavo sono tutti progettati con funzionalità di ripristino automatico tramite network management software.

3.2 Minacce non deliberate

Un'analisi completa delle minacce alle infrastrutture subacquee richiede anzitutto di distinguere l'intenzionalità dell'azione. I danneggiamenti alle condutture sul fondale spesso avvengono per ragioni estranee ad azioni antropiche intenzionali. Pertanto, è necessario considerare adeguatamente il quadro delle minacce non intenzionali, che rappresentano la principale causa di danni alle infrastrutture subacquee a livello globale³⁰.

3.2.1 Minacce naturali

I rischi derivanti da fenomeni naturali costituiscono una minaccia significativa per la resilienza delle infrastrutture subacquee, sebbene spesso sottostimati nell'analisi di sicurezza convenzionale. Un recente studio guidato dal National Oceanography Centre (NOC) del Regno Unito ha evidenziato che circa il 25% dei danneggiamenti di cavi di comunicazione sottomarini tra il 1965 e il 2019 è attribuibile a cause naturali.³¹

Eventi estremi come tifoni, frane sottomarine, correnti ed eruzioni vulcaniche possono causare danni diffusi a più sistemi contemporaneamente. L'eruzione del vulcano Hunga del gennaio 2022 a Tonga ha distrutto l'unico cavo internazionale dell'arcipelago, isolando il Paese per settimane e ostacolando gravemente la risposta all'emergenza. Nel Golfo di Guinea, tra gennaio e marzo 2020, le correnti di torbidità nel Canyon del Congo hanno ripetutamente danneggiato i cavi, interrompendo i servizi Internet in tutta l'Africa occidentale.

Anche fenomeni di intensità inferiore, come tempeste continue, correnti marine persistenti, possono contribuire in modo significativo ai guasti: una nuova analisi di casi storici rivela infatti che una percentuale significativa di danneggiamenti precedentemente non attribuiti potrebbe essere correlata a tali impatti di bassa intensità ma prolungati nel tempo.³²

Il cambiamento climatico costituisce inoltre un fattore moltiplicatore di lungo periodo, poiché potrebbe incrementare sia l'entità che la frequenza di tali fenomeni, con

³⁰ Kordahi, M. E. et al. (2019), "Global Trends in Submarine Cable System Faults 2019 Update", *Proceedings of the SubOptic 2019*, New Orleans, USA; Clare, M. (2021), Submarine Cable Protection and the Environment, International Cable Protection Committee (ICPC), Issue 2

³¹ Bricheno, L. et al. (2024), "The diversity, frequency and severity of natural hazard impacts on subsea telecommunications networks", *Earth-Science Reviews*, Vol. 259, 104972 <https://doi.org/10.1016/j.earscirev.2024.104972>

³² Clare M., et al. (2023), "Climate change hotspots and implications for the global subsea telecommunications network", *Earth-Science Reviews*, Vol. 237, 104296, <https://doi.org/10.1016/j.earscirev.2022.104296>.

ricadute significative anche sulle pipeline, particolarmente esposte a ripercussioni idrodinamiche dovute alle correnti.³³

Sulle cause di queste minacce l'azione umana ha scarsa capacità di azione; tuttavia, rimane possibile adeguare le azioni di gestione e difesa per limitare gli effetti avversi.

3.2.2 Minacce antropiche accidentali

I danni derivanti da cause esclusivamente naturali costituiscono solo una minima parte dei guasti alle infrastrutture subacquee. Nella maggior parte dei casi, i danneggiamenti sono causati da attività umane accidentali. Il trascinamento di ancore e reti da pesca costituisce di gran lunga la principale causa di danneggiamento dei cavi sottomarini, con stime che variano dal 60% all'86% a seconda del campione analizzato³⁴.

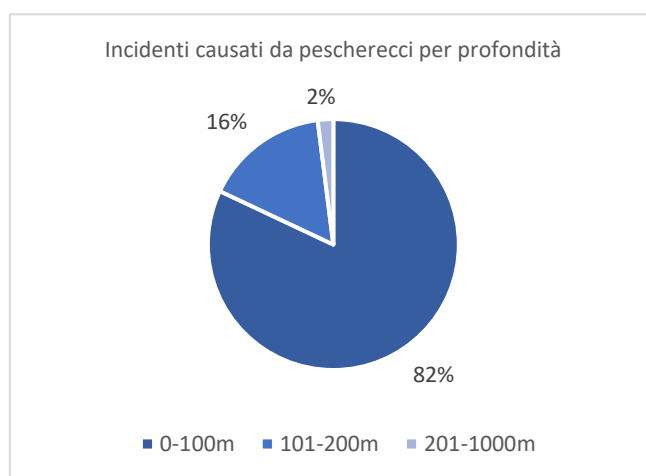


Fig. 2 — Principali categorie di guasto ai cavi sottomarini per causa

Pesca a strascico. Le porte a strascico (divergenti) e i pesi progettati per sollevare il sedimento marino rappresentano una minaccia concreta. Nel 90% dei casi un contatto tra reti e cavi non crea danni, ma l'impiego di rampini per recuperare le reti aumenta significativamente il rischio di aggancio, soprattutto nel caso di infrastrutture non insabbiate e prive di armatura.³⁵ In questo senso, il progressivo aumento della profondità di pesca, indotto dall'esaurimento degli stock ittici e dai cambiamenti climatici, costituisce un pericolo perché a batimetriche maggiori le condutture non vengono né insabbiate né dotate di armatura.

Trascinamento di ancore. Dal 2011, grazie a studi dell'ICPC, è stato dimostrato che le ancore rappresentano una causa di danni molto più significativa di quanto ritenuto in

³³ Durap, A. & Can, E. B. (2022), "Risk assessment of submarine pipelines: A case study in Turkey", *Ocean Engineering*, Vol. 261, 112079, <https://doi.org/10.1016/j.oceaneng.2022.112079>

³⁴ Kordahi, M. E. et al. (2019), "Global Trends in Submarine Cable System Faults 2019 Update", *Proceedings of the SubOptic 2019*, New Orleans, USA.; Clare, M. (2021), Submarine Cable Protection and the Environment, International Cable Protection Committee (ICPC), Issue 2,

³⁵ Clare, M. (2021), Submarine Cable Protection and the Environment, International Cable Protection Committee (ICPC), Issue 2, https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf

precedenza. I pericoli sono particolarmente rilevanti in acque inferiori ai 200 m, dove avviene pressoché la totalità di questo tipo di danneggiamento.³⁶ I danni possono verificarsi sia quando un'ancora viene calata direttamente su un cavo, sia quando è trascinata involontariamente per lunghe distanze.

Nel Mar Baltico, dal 2022 le ancore delle navi mercantili hanno causato danni a oltre dieci infrastrutture subacquee, tra cui il gasdotto Balticconnector tra Finlandia ed Estonia. Tutti questi casi presentano caratteristiche sospette che li pongono in una zona grigia tra danno accidentale e sabotaggio deliberato: infatti, l'equipaggio ha quasi sempre dichiarato di non essersi accorto dell'ancora in mare, trascinata per lunghi tratti colpendo diverse infrastrutture vicine.

Il problema è amplificato dal fatto che molte rotte di navigazione commerciale transitano nelle stesse aree geografiche dove si concentrano le infrastrutture sottomarine, e che le mappe di posizione dei cavi non sono sempre pienamente accessibili o aggiornate per tutti i soggetti naviganti.

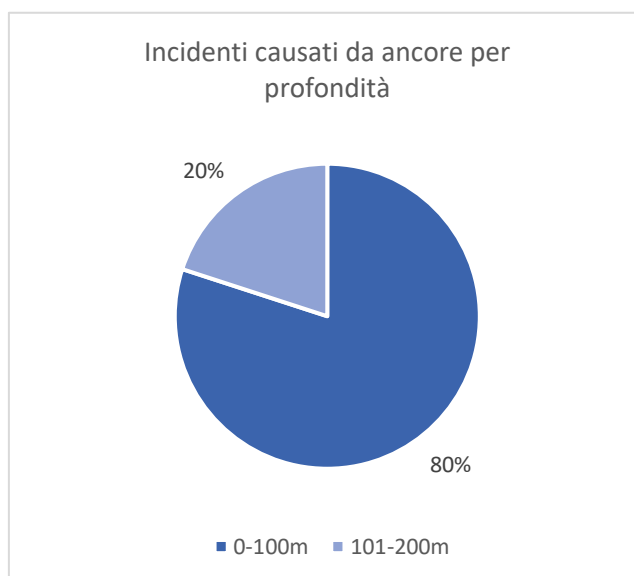


Fig. 3 — Modalità di danneggiamento da ancora su cavo sottomarino.

Conflitti e zone di guerra come rischio indiretto. Le azioni cinetiche in superficie possono incidere sulle infrastrutture subacquee in modo indiretto. Nel febbraio 2024, l'equipaggio della nave mercantile Rubymar (colpita da un missile balistico degli Houthi) ha calato l'ancora prima di abbandonare la nave e l'imbarcazione alla deriva ha danneggiato quattro cavi di comunicazione posati sui fondali del Mar Rosso.

La presenza di conflitti attivi rende inoltre impossibili le normali operazioni di installazione e riparazione, poiché le navi posacavi operano a velocità estremamente basse e devono rimanere ferme durante le riparazioni. Il costo per assicurare navi posacavi vicino allo Yemen è aumentato fino a 150.000 dollari al giorno, ostacolando la

³⁶ International Cable Protection Committee (2025), *Damage to Submarine Cables from Dragged Anchors*, <https://www.iscpc.org/publications/icpc-viewpoints/damage-to-submarine-cables-from-dragged-anchors/>

messa in servizio dei cavi Blue-Raman e 2Africa, con ripercussioni sulla ridondanza delle rotte e sulla connettività del continente africano.³⁷

3.3 Minacce deliberate e ibride

Le minacce derivanti da azioni antropiche deliberate si caratterizzano come minacce ibride, con azioni che combinano mezzi convenzionali e non convenzionali, fisici e digitali, statali e para-statali, per produrre effetti che rimangono deliberatamente al di sotto della soglia di risposta convenzionale.³⁸

La caratteristica essenziale della minaccia ibrida è la deliberata ambiguità rispetto all'identità dell'attore, alle intenzioni sottostanti e alla natura, ostile o accidentale, dell'evento. Questa ambiguità ritarda o impedisce una risposta immediata, poiché la vittima deve raccogliere prove di imputabilità prima di poter giustificare una misura coercitiva, ed erode nel lungo periodo la fiducia nella disponibilità e affidabilità delle infrastrutture.

Infatti, la logica operativa privilegia la produzione di incertezza decisionale e il prolungamento artificiale dei tempi di recovery (la media globale di circa quaranta giorni tra individuazione del guasto e ripristino rappresenta una finestra di sfruttabilità strategica), piuttosto che la distruzione dell'asset.

Questa logica è favorita da tre fattori strutturali: (i) la pluralità di attori, con linee di demarcazione deliberatamente sfumate tra attori statali, criminali, proxy e operatori privati; (ii) la frammentazione giuridico-spaziale, con un mosaico normativo che rende difficile l'attribuibilità degli atti ostili; (iii) la dipendenza da capacità limitate (navi di riparazione, componentistica specializzata, software EMS/NMS) la cui disponibilità può essere condizionata come atto di pressione ibrida.

3.3.1 Attori statuali

Per oltre un secolo, gli atti ostili contro le infrastrutture subacquee sono stati compiuti unicamente da attori statuali. Il primo caso noto risale al 1898, durante la guerra ispano-americana, quando gli Stati Uniti tagliarono diversi cavi telegrafici nelle Filippine e nei Caraibi per interrompere le comunicazioni spagnole.

Durante la Prima Guerra Mondiale la prima mossa britannica fu il taglio dei cavi telegrafici tedeschi; nella Seconda Guerra Mondiale l'Operazione Sabre vide gli Alleati tagliare due cavi giapponesi al largo di Saigon per costringere il nemico a utilizzare comunicazioni wireless intercettabili. Durante la Guerra Fredda, l'Operazione Ivy Bells (1971) portò all'installazione di un pod di induzione da parte del sottomarino

³⁷ Leccese, G. (2025), "Choke point Above and Below the Surface: The Red Sea's Emerging Infrastructure Challenge", *Istituto Affari Internazionali (IAI)*, Brief, no. 8, <https://www.iai.it/it/pubblicazioni/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge>

³⁸ European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), *Protecting Maritime Infrastructure from Hybrid Threats: Legal Options*, Hybrid CoE Research Report 14 (Helsinki: Hybrid CoE, 2025), pp. 8–12. Per la definizione operativa di "grey zone" nel contesto marittimo cfr. NATO, "Countering Hybrid Threats," NATO, aggiornato al 29 gennaio 2026.

specializzato statunitense USS *Halibut* per leggere messaggi sovietici via cavo nel Mare di Okhotsk.

Tali atti ostili verso le infrastrutture subacquee caratterizzano anche il nuovo millennio, come testimoniato dall'operazione, emersa nel 2013, con cui il GCHQ (Quartier Generale delle Comunicazioni del Governo) del Regno Unito si è collegato alla rete di cavi Internet per accedere a enormi quantità di comunicazioni di innocenti e sospettati per poi trasmettere le informazioni alla *National Security Agency* (NSA) statunitense. Oggi, gli attori statuali posseggono diverse capacità per interferire con cavi e pipeline sui fondali marini.

La Russia ha sviluppato diverse piattaforme specializzate per operazioni sui fondali marini. La nave oceanografica *Yantar*, formalmente una nave di ricerca scientifica, è documentata per la sorveglianza ravvicinata delle infrastrutture subacquee NATO nell'Atlantico e nel Mediterraneo, con capacità di dispiegare mini-sommergibili e droni subacquei, sia a controllo remoto (Remotely Operated Vehicle, ROV) che autonomi (Autonomous Underwater Vehicle, AUV). L'arsenale russo comprende inoltre sottomarini a propulsione nucleare, come il *Paltus*, l'*X-Ray*, il *Kashalot* e il *Losharik*, appositamente modificati per interagire con il fondale a grandi profondità attraverso dei bracci meccanici.³⁹

La Cina agisce invece nella dimensione subacquea principalmente attraverso vettori complementari che rendono il suo profilo di minaccia multidimensionale. Sul piano cyber e di intelligence, dispone di capacità di compromissione dei sistemi di gestione (pre-positioning, accesso al management plane) e di sfruttamento della catena di fornitura. Sul piano fisico, il vettore osservato è il danneggiamento in acque poco profonde tramite naviglio mercantile e "flotte ombra" (casi Taiwan 2025), a cui sembra affiancarsi una capacità deep-sea emergente e a forte valenza segnaletica come mostra il dispositivo di taglio cavi fino a 4.000 metri rivelato nel 2025 e testato a 3.500 metri nel 2026, integrabile con i sommergibili *Fendouzhe* e *Haidou*⁴⁰. Sul piano industriale e geoeconomico, la proiezione avviene attraverso la Digital Silk Road e la presenza di operatori come HMN Technologies (già Huawei Marine Networks) nelle gare per nuove dorsali, con le conseguenti questioni di accesso fisico ai sistemi e potenziale compromissione delle componenti in fase di costruzione e riparazione.

Gli Stati Uniti vantano diversi possibili vettori di attacco verso le infrastrutture subacquee. Sul piano fisico, la US Navy nei decenni scorsi ha utilizzato il sottomarino specializzato USS *Halibut* per operazioni specifiche di interazione con il fondale e attualmente sembra possedere simili piattaforme con il sottomarino nucleare USS *Jimmy Carter*. I programmi di spionaggio rivelati da Snowden, in particolare TEMPORA e MUSCOLAR, condotti in collaborazione con il GCHQ britannico, hanno documentato la capacità di intercettare i dati veicolati da cavi sottomarini sia nell'Atlantico che nel Pacifico. La dottrina *Defend Forwards* (*Cyber Command*) prevede il dispiegamento di capacità offensive nelle infrastrutture avversarie a fini di deterrenza e risposta rapida. A tali capacità, si aggiunge il potenziale vantaggio dato dalla posizione privilegiata nel

³⁹ Kaushal, S. (2023), "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure", *Royal United Services Institute (RUSI)*.

⁴⁰ Silver, S. (2026), "China Just Proved It Can Cut Undersea Cables at 3,500 Meters Deep. Guam's 12 Fiber-Optic Lines Serve Google, the U.S. Military and the Entire Second Island Chain", 19FortyFive, April 19, 2026. <https://www.19fortyfive.com/2026/04/china-just-proved-it-can-cut-undersea-cables-at-3500-meters-deep-guams-12-fiber-optic-lines-serve-google-the-u-s-military-and-the-entire-second-island-chain/>

settore dei cavi di telecomunicazione degli hyperscalers statunitensi, come Meta, Google, Amazon e Microsoft, che potrebbero essere coinvolte in operazioni di spionaggio come già successo nel caso di PRISM.⁴¹

L'Iran rappresenta un attore di crescente rilevanza, sia per la capacità cyber sviluppate dai gruppi APT (Advanced Persistent Threat) denominati APT33, APT34 e APT35 (anche conosciuti come *Elfin*, *OilRig*, *Charming Kitten*), orientati alla raccolta di intelligence e alla disruption di sistemi industriali, sia per il controllo geografico sullo stretto di Hormuz, checkpoint globale per il traffico di gas liquefatto ma potenziale punto di vulnerabilità per i cavi di telecomunicazione posati su quei fondali. Tali infrastrutture potrebbero essere danneggiate indirettamente nel corso di operazioni militari in superficie, soprattutto considerando l'impiego iraniano di mine navali.

Una categoria distinta è quella degli attori la cui rilevanza per la dimensione subacquea è indiretta ma non trascurabile, in quanto fondata sulla trasferibilità delle capacità e sulla prossimità d'interesse. Pur priva di capacità subacquee documentate, la Corea del Nord ha maturato una postura cyber offensiva tra le più industrializzate a livello statale, orientata alla generazione di risorse in regime di *sanctions evasion* attraverso il targeting del sistema finanziario tradizionale (caso Bangladesh Bank/SWIFT, 2016⁴²) e il furto di criptovalute su scala miliardaria⁴³. Ciò che la rende rilevante non è la finalità predatoria in sé, quanto il modus operandi che la sostiene, fondato su compromissione di supply chain digitali e accesso persistente a sistemi critici, potenzialmente orientabile verso il settore delle telecomunicazioni e delle dorsali sottomarine qualora mutassero gli incentivi strategici di Pyongyang. Israele risponde alla stessa logica per un vettore diverso: la tradizione consolidata di operazioni cibernetiche di precisione contro sistemi industriali e di controllo (Stuxnet come caso paradigmatico⁴⁴) esprime una capacità OT/ICS direttamente trasferibile ai sistemi SCADA delle condotte e delle stazioni di conversione sottomarine, cui si somma un interesse geografico specifico per le infrastrutture del Mediterraneo orientale, teatro di dorsali dati ed energetiche di crescente sensibilità come EastMed. A questi si aggiunge, infine, un numero crescente di attori statali di media capacità che stanno investendo nella dimensione subacquea come asimmetria strategica a basso costo rispetto alle capacità navali convenzionali: per essi la barriera d'ingresso non è più la disponibilità di assetti navali sofisticati, ma l'accesso a tecnologie unmanned (ROV/AUV) commerciali e a competenze cyber di mercato, con un profilo di minaccia destinato a diffondersi in modo analogo a quanto osservato per i sistemi aeromobili a pilotaggio remoto.

⁴¹ Le rivelazioni di Snowden nel 2013 evidenziarono come la NSA statunitense, grazie al programma PRISM, avesse ottenuto la fornitura di dati (ad esempio email, file, notifiche di accesso, etc) da parte delle principali aziende tecnologiche USA che gestiscono informazioni, comunicazioni e dati-utente in formato digitale (Microsoft, Facebook e Google), spiando anche cittadini e istituzioni UE. Cosmi, S. (2014), "Nsa: "Google, Microsoft e Yahoo! sapevano tutto di Prism": il capo dell'ufficio legale accusa i giganti del web", *La Repubblica*, https://www.repubblica.it/tecnologia/2014/03/20/news/nsa_google_microsoft_e_yahoo_sapeva_no_tutto_di_prism_il_capo_dellufficio_legale_accusa_i_giganti_del_web-81428778/

⁴² United States Department of Justice. (2018). Criminal complaint: United States v. Park Jin Hyok (Case No. MJ18-1479). U.S. District Court, Central District of California. <https://www.justice.gov/opa/press-release/file/1092091/download> ; Si veda anche: BAE Systems Applied Intelligence. (2016). *Two bytes to \$951m*. BAE Systems Threat Research Blog. <https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html>

⁴³ Chainalysis. (2025). 2025 crypto crime report: Stolen funds. Chainalysis.

⁴⁴ Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), cap. 15-1.

3.3.2 Attori non statuali

A partire dal 2007 la tendenza a interferire con le infrastrutture sottomarine, per anni limitata agli attori statuali, si è estesa agli attori non statuali. Pescatori vietnamiti hanno tagliato più di 500 km di cavi sottomarini per estrarre materiali da rivendere, causando la perdita di più dell'80% della connettività del Vietnam. Nel 2015, tagli sospetti a dei cavi vicino alle coste californiane hanno spinto l'FBI a indagare per possibili atti di matrice terroristica. Nel 2016, pirati somali hanno attaccato una nave posacavi durante operazioni di installazione nel Mar Rosso.

Nel dominio cyber, la minaccia non statale converge sulle funzioni di sistema che rendono l'infrastruttura gestibile e ripristinabile. È utile quindi distinguere quattro profili principali:

Hacktivisti⁴⁵. Gruppi motivati da ragioni politiche o ideologiche, con capacità tecniche variabili ma generalmente inferiori a quelle dei gruppi statali. Tendono ad azioni dimostrative piuttosto che a operazioni con effetti sistemici profondi, ma possono causare disruption temporanee significative su sistemi di gestione accessibili via internet⁴⁶.

Cybercrime organizzato. Organizzazioni criminali transnazionali con crescente sofisticazione tecnica, motivate principalmente dal profitto economico. Possono rappresentare una minaccia per i sistemi di fatturazione e gestione operativa degli operatori di cavi, nonché per le catene di fornitura digitali⁴⁷.

Insider e contractor. Il personale con accesso privilegiato ai sistemi di gestione delle infrastrutture come dipendenti, manutentori, subappaltatori, rappresenta una superficie di rischio spesso sottovalutata. Casi di compromissione dall'interno hanno dimostrato come un singolo soggetto con accesso ai sistemi di controllo possa causare danni di entità comparabile a operazioni esterne complesse. Questo profilo è particolarmente rilevante nelle fasi di installazione e manutenzione, dove i perimetri di accesso sono per natura più permeabili⁴⁸.

Mercenari digitali. Gruppi di hacker professionisti che operano per conto terzi, tipicamente attori statali che vogliono mantenere la *plausibile deniability*, con capacità tecniche elevate e obiettivi definiti dal committente⁴⁹.

La distinzione tra attori statali e non statali è spesso artificiale. Infatti, molti attori non statali agiscono su commissione statale, ricevono capacità o copertura da governi, o operano in uno spazio grigio di tacita tolleranza da parte delle autorità nazionali. La categoria più pericolosa combina capacità tecniche di livello statale con l'organizzazione di soggetti privati, massimizzando l'ambiguità dell'attribuzione.

⁴⁵ Il termine “hacktivismo” deriva dalla combinazione tra le parole “hack” e “attivismo” e viene utilizzato per indicare quella tipologia di hacker che agiscono perché spinti dalla propria insoddisfazione politica o sociale nei confronti di determinati eventi.

⁴⁶ Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), cap. 18–20; Aanonsen, “Stuxnet, revisited (again): producing the strategic relevance of cyber operations,” pp. 72–74.

⁴⁷ ENISA, *ENISA Threat Landscape 2024*, pp. 42–60; Buchanan, *The Hacker and the State*, pp. 48–52.

⁴⁸ Canadian Centre for Cyber Security, “Cyber Threat Bulletin: Iranian Cyber Threat Response to US/Israel Strikes,” febbraio 2026.

⁴⁹ Buchanan, *The Hacker and the State*, pp. 70–85; Rid, *Active Measures*, pp. 400–420.

3.4 Vettori e modalità di azione

Una volta definiti gli attori, occorre definire i mezzi attraverso i quali le minacce trovano applicazione. In questo senso, occorre distinguere tra vettori fisici, cyber e geoeconomici.

3.4.1 Dimensione Fisica

Sabotaggio. Il fattore fondamentale che influenza le modalità di attacco fisico è la profondità di installazione dell'infrastruttura. In acque meno profonde, è possibile raggiungere e danneggiare cavi e pipeline anche con mezzi meno avanzati; operare a maggiori profondità richiede invece asset subacquei altamente specializzati.

Un primo vettore è l'impiego di sommozzatori per applicare cariche esplosive sulla condotta. Il limite batimetrico pratico per questa modalità è circa 90–100 m, stando agli attuali limiti dei sommozzatori militari specializzati.⁵⁰ Le differenze tra il tentativo di sabotaggio di un cavo al largo del porto di Alessandria nel 2013 (eseguito da tre subacquei con semplice respiratore) e il danneggiamento del gasdotto Nord Stream 2 nel 2022 (avvenuto a circa 84 m di profondità con miscele speciali di gas e circa 100 kg di attrezzatura) illustrano le diverse esigenze tecniche in funzione della profondità.⁵¹

Un'altra modalità è l'utilizzo deliberato di dispositivi di taglio meccanici, come le ancore. In questo caso, la stessa dinamica del danno accidentale è impiegata intenzionalmente, con la difficoltà aggiuntiva per il Paese target di distinguere la volontarietà dell'atto, come evidenziato dai casi del Mar Baltico, dove spegnimento dell' AIS e riduzione della velocità nei pressi dell'infrastruttura hanno alimentato sospetti senza consentire un'attribuzione definitiva.⁵² Nel contesto italiano sono soggetti a questi rischi i cavi che attraversano lo Stretto di Messina, i fondali del Canale di Sicilia in prossimità della costa o i tratti adriatici superficiali.

L'ultima casistica di sabotaggio fisico è rappresentata dall'impiego di avanzati mezzi subacquei per profondità superiori ai 200 m. Le capacità necessarie di sensing, mappatura e intervento sono a disposizione soltanto di un numero molto limitato di attori statuali. In questo senso, gli unici due attori probabilmente in grado di interferire con le infrastrutture sul fondale a tali profondità sembrano essere USA e Russia, con i sottomarini specializzati citati in precedenza.

Oltre a queste tecniche attualmente in uso, è bene poi prendere in considerazione metodologie di attacco che sono oggi in fase di sviluppo e che potrebbero avere in tempi ragionevolmente brevi un impatto importante. Tra queste tecniche innovative ricordiamo: il camuffamento bio-adattivo, le armi mimetizzate, i robot armati, gli animali armati, l'occultamento acustico contro la detezione sonar, la geo-ingegnerizzazione dell'ambiente, la manipolazione bio-tecnologica (inclusa la biologia sintetica), e l'aumento della capacità dei subacquei di operare in condizioni estreme

⁵⁰ N. A. (2025), "Eckernförde: Mine divers extend diving depth to 84 metres", *Marine Forum*, <https://marineforum.online/en/eckernfoerde-mine-divers-extend-diving-depth-to-84-metres/#:~:text=In%20response%20to%20the%20tense,Photo:%20U.S.%20Navy>

⁵¹ Per maggiori informazioni sulla ricostruzione del sabotaggio al Nord Stream, vedi: Struckmeier, L. (2024), "How did divers manage to blow up the Nord Stream pipeline? We went down to the spot to find out", *CBC News*, <https://www.cbc.ca/news/investigates/nord-stream-pipeline-explosion-ukraine-diver-1.7296527>

⁵² Kärmas (2024), "Balticconnector case more sabotage than an accident, experts say", *EER News*, <https://news.err.ee/1609255413/balticconnector-case-more-sabotage-than-an-accident-experts-say>

grazie a strumenti di miglioramento biologico. Tutte tecnologie che potrebbero aumentare notevolmente l'impatto di azioni di sabotaggio.

Intercettazione. L'intercettazione dei dati tramite *tapping* riguarda specificatamente i cavi di comunicazione. Contrariamente a quanto generalmente ritenuto, anche la trasmissione in fibra ottica può essere soggetta a *eavesdropping* (intercettazione), attraverso tecniche di manipolazione della fibra, quali fibre bending, accoppiamento evanescente, taglio a V e scattering tramite reticolo di Bragg.⁵³ L'obiettivo è captare una porzione del flusso ottico senza interrompere visibilmente la comunicazione.

Queste procedure sono più facili da eseguire sul *dry plant*, dove un attore ostile può accedere al cavo senza particolari difficoltà fisiche. Il caso documentato della CLS sulle coste britanniche, intercettata dal GCHQ, ne è l'esempio più noto. Nel *wet plant*, le capacità tecniche richieste aumentano considerevolmente: i sottomarini specializzati russi del GUGI e il sottomarino statunitense USS Jimmy Carter sembrano essere le uniche piattaforme subacquee in grado di effettuare simili operazioni. Anche le navi di riparazione, che ospitano camere in cui può essere introdotta una porzione di cavo, sono considerate possibili minacce per l'intercettazione dei dati, al punto che Washington ha segnalato alle proprie big tech i pericoli derivanti dall'affidarsi ad aziende di riparazione cinesi.⁵⁴

Attacco alle navi posacavi. Le navi di riparazione e installazione costituiscono un altro potenziale punto di esposizione: il loro numero estremamente limitato fa sì che il danneggiamento di anche solo alcune di esse riduca drasticamente la capacità di risposta dell'intero sistema. Ad esempio, tutta l'area del Mediterraneo, del Mar Rosso e del Mar Nero è coperta soltanto da due navi di riparazioni.⁵⁵

Le navi posacavi possono essere colpite sia in porto sia durante le operazioni, quando sono costrette a rimanere ferme. Il caso somalo del 2016, in cui una nave posacavi fu attaccata da pirati nel Mar Rosso, riuscendo a respingere il tentativo di abbordaggio solo grazie al personale di sicurezza a bordo, dimostra la concretezza di questa minaccia.⁵⁶

3.4.2 Dimensione cyber

Il modo più efficace per compromettere una rete sottomarina non è tagliare il cavo: è impedire a chi lo gestisce di capire cosa sta succedendo e di intervenire in tempo. L'obiettivo operativo non è quasi mai la distruzione immediata, ma il *recovery drag* (l'allungamento del tempo tra l'insorgenza di un guasto e il suo ripristino) ottenuto degradando la *situational awareness* degli operatori, alterando la telemetria, saturando i canali di coordinamento o compromettendo gli strumenti del ripristino stesso.

Recorded Future, nel suo State of Security Report 2026, individua nella disruption reversibile di cavi, satelliti e telco lo strumento coercitivo di elezione per gli attori

⁵³ Per una spiegazione di tali tecniche, vedi: Iqbal M. Z., Fathallah H., and Belhadj N. (2011), "Optical fiber tapping: Methods and precautions." *8th International Conference on High-capacity Optical Networks and Emerging Technologies*, pp. 164-168.

⁵⁴ Voltz, D. et al. (2025), "U.S. Fears Undersea Cables Are Vulnerable to Espionage From Chinese Repair Ships", *The Wall Street Journal*, <https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320>

⁵⁵ MECMA, <https://www.mecmamc.org/public/index.html>

⁵⁶ Morel, C. (2016), "Threats beneath the seas: Vulnerabilities in the global cable network", *Hérodote*, Vol. 163, No. 4, pp. 33-43

statuali: abbastanza visibile da segnalare capacità, abbastanza ambiguo da restare sottosoglia di risposta formale⁵⁷.

I vettori di attacco cyber più rilevanti per le infrastrutture sottomarine includono quindi i seguenti scenari.

Compromissione della supply chain digitale. La supply chain digitale è una struttura di fiducia: ogni nodo della catena (fornitore di firmware, provider di strumenti di gestione, MSP con accessi ricorrenti) è per definizione autorizzato a interagire con i sistemi dell'operatore. Compromettere un nodo upstream significa ereditare quella fiducia, trasformando un singolo punto di compromissione in un vettore multi-target.

Il Cable Security Toolbox della Commissione europea (gennaio 2026) tratta esplicitamente la backdoor tramite componenti EMS/NMS come minaccia prioritaria, con il rischio specifico di *malicious system shut down* attraverso firmware compromesso in fase di fornitura. Il caso SolarWinds Orion rimane il paradigma documentato: l'effetto più rilevante non è stata la singola intrusione, ma l'incertezza generalizzata sulla fiducia negli strumenti di gestione, che ha imposto spegnimenti preventivi e sospensione degli accessi remoti in decine di organizzazioni.

Pre-posizionamento e accesso persistente. In questa modalità, l'attaccante non ha interesse a produrre alcun effetto visibile nell'immediato. L'obiettivo è costruire accessi persistenti e silenti su segmenti strategici dell'infrastruttura, così da disporre di opzioni attivabili in caso di crisi, una postura che vale come leva coercitiva anche se quelle opzioni non vengono mai esercitate: l'avversario sa che esistono e deve spendere risorse di mitigazione senza poter attribuire una minaccia concreta.

Il caso Volt Typhoon⁵⁸ documenta accessi mantenuti nel tempo su infrastrutture critiche statunitensi, incluso il settore delle comunicazioni, con una lettura istituzionale del rischio come «opzioni attivabili in uno scenario di crisi Taiwan». Nel contesto mediorientale, MuddyWater (gruppo MOIS) ha condotto attraverso Operation Olampo (marzo 2026), una campagna con TTP che indicano infrastruttura condivisa tra attori iraniani.

Routing manipulation. La manipolazione di annunci BGP (*Border Gateway Protocol*, governa il *routing* del traffico internet a livello globale) può essere condotta senza accesso fisico all'infrastruttura sottomarina e deviare il traffico attraverso rotte controllate dall'attaccante, consentendo intercettazione massiva, inserimento di payload malevoli o semplicemente degrado della connettività. L'effetto può essere deliberatamente «grigio»: le rotte rimangono annunciate, il servizio resta formalmente attivo, ma latenza, perdita di pacchetti e instabilità degradano in modo significativo.

Casi di BGP *hijacking*⁵⁹ (o anche dirottamento del *Border Gateway Protocol*, protocollo di routing di Internet) associabili a operazioni di intelligence statale sono stati

⁵⁷ Martti Lehto, Petro Julkunen e Hans Hartikainen, "Cyber Security in the Subsea Telecommunication Cable Networks," in ICCWS 2026, pp. 212–221.

⁵⁸ CISA (2023). The Attack on Colonial Pipeline: What We've Learned. Disponibile su: <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned>.

⁵⁹ Il termine hijacking (dal termine inglese hijack, "dirottare") indica una tecnica di attacco che consiste nel modificare opportunamente determinati attributi di una comunicazione Client-Server volta a indirizzare la vittima verso risorse malevole o, viceversa, per veicolare verso l'attaccante il flusso di comunicazione legittimo tra risorsa e vittima. Si veda:

documentati ripetutamente nell'ultimo decennio. L'analisi tecnica di RIPE Labs sui tagli di cavi nel Mar Baltico (dicembre 2024) documenta questa dinamica con dati empirici: a seguito di tagli fisici multipli, la resilienza del *routing* ha reagito in modo asimmetrico, rivelando dipendenze e colli di bottiglia logici non noti ex ante, confermando che la resilienza non è solo fisica ma anche logica.

Compromissione del landing hub. La *Cable Landing Station* (CLS) è il punto in cui la tratta sottomarina diventa operabile. Ospita la terminazione del cavo e il *Submarine Line Terminal Equipment* (SLTE), alimenta i *repeater* lungo il percorso, concentra il backhaul terrestre ed espone un Remote Network Management System (RNMS) accessibile via Internet per la manutenzione remota.

L'accesso malevolo avviene tipicamente attraverso i vettori più ordinari del panorama di minaccia: exploitation di sistemi esposti o non aggiornati, abuso di credenziali di servizio condivise tra vendor, pivot dalla rete IT verso ambienti di gestione, compromissione degli accessi remoti di terze parti. Nel 2022, Homeland Security Investigations ha interrotto un accesso non autorizzato ai sistemi di una società privata operante su un cavo critico per la connettività nel Pacifico, confermando che i punti di approdo sono superfici di azione appetibili anche in assenza di escalation cinetica.

Compromissione del management plane. Il caso Kyivstar illustra cosa significa compromettere il sistema nervoso di un'infrastruttura di telecomunicazione. Nel dicembre 2023, Sandworm (GRU 74455) ha attivato un accesso mantenuto per almeno sei mesi all'interno dei sistemi del più grande operatore mobile ucraino, cancellando migliaia di server virtuali e PC e interrompendo i servizi per 24 milioni di utenti⁶⁰.

Per i cavi sottomarini, la struttura del rischio è analoga. NOC, piattaforme OSS/NMS, sistemi di telemetria e strumenti di orchestrazione sono il livello da cui si governa la *fault detection*, la *shunt fault localization* e il *dispatch* delle navi di riparazione: se questo livello è compromesso, un guasto fisico si trasforma in crisi prolungata. Il caso SolarWinds Orion (*supply chain compromise* di una piattaforma di network management che ha garantito accesso persistente su migliaia di organizzazioni) rimane il riferimento più documentato di come colpire gli strumenti di gestione produca effetti sistemici e duraturi⁶¹.

Harvest now, decrypt later. Come in molti altri settori, è necessario considerare un rischio futuro che ha già ripercussioni nel presente: l'attacco quantistico. Si tratta attualmente di uno dei rischi più sottovalutati. Non tanto come minaccia immediata, poiché la tecnologia per decrittare comunicazioni cifrate in tempo reale tramite computer quantistici non è ancora disponibile, quanto piuttosto come strategia di raccolta sistematica di dati cifrati da decifrare in un secondo momento, quando la crittografia post-quantistica sarà accessibile agli attaccanti.

Questo approccio è adottato da attori statali dotati delle necessarie capacità di archiviazione e rende urgente la migrazione delle infrastrutture critiche verso algoritmi

<https://www.sicurezzanazionale.gov.it/cosa-facciamo/innovazione-consapevolezza-digitale/tipologie-di-attacco/hijacking>

⁶⁰ SentinelOne (2024). Sandworm/GRU 74455 – Kyivstar attack timeline. Disponibile su: <https://www.sentinelone.com/blog/sandworm-kyivstar/>.

⁶¹ GAO, GAO-22-104746 (2022). SolarWinds Orion supply chain compromise — impact on critical infrastructure. Disponibile su: <https://www.gao.gov/products/gao-22-104746>.

post-quantum, nonché lo sviluppo di capacità di *crypto-agility*, ossia la possibilità di aggiornare rapidamente gli algoritmi crittografici in uso⁶².

3.4.3 Dimensione geoeconomica

Accanto ai rischi descritti, emerge un'ulteriore tipologia di minaccia legata alla dimensione geoeconomica. Le infrastrutture sottomarine si collocano all'intersezione tra fattori economici, geografici e politico-strategici. Il quadro interpretativo della «*weaponized interdependence*» elaborato da Farrell e Newman descrive come le reti globali altamente interconnesse possano essere sfruttate dagli Stati come strumenti di potere. Farrell e Newman individuano due meccanismi principali: l'effetto *panopticon* e l'effetto *choke point*⁶³.

Effetto *Panopticon*⁶⁴. Questo effetto deriva dalla capacità di sorveglianza e intercettazione che può essere esercitata attraverso il controllo delle infrastrutture di telecomunicazione. Un operatore che possiede o gestisce un cavo subacqueo ha potenzialmente accesso a tutto il traffico che lo attraversa.

Questa capacità di sorveglianza spiega la competizione per il controllo delle dorsali globali. Nell'ultimo decennio, la concentrazione del mercato dei cavi subacquei è passata nelle mani di poche grandi aziende, principalmente *hyperscaler* americani come Google, Meta, Microsoft e Amazon (che controllano complessivamente circa il 69% della capacità globale).⁶⁵ Queste aziende si sono trasformate da semplici clienti a principali investitori e proprietari delle infrastrutture, riducendo il ruolo delle telco nazionali. È attualmente difficile progettare una nuova infrastruttura sottomarina senza la loro partecipazione.

Come anticipato, il pericolo dell'intercettazione dei dati non proviene soltanto dalle aziende operatrici, ma anche da quelle incaricate della costruzione e installazione: in tali fasi potrebbero infatti essere installati dispositivi per intercettare i dati in transito.

L'esclusione progressiva di operatori cinesi dai progetti di nuovi cavi nelle rotte atlantiche e nel corridoio indo-pacifico deriva proprio dal potenziale pericolo di un effetto *panopticon*: la cinese HMN Tech ha costruito e installato diverse infrastrutture, sollevando preoccupazioni sulla sicurezza dei dati, analoghe a quelle già emerse per Huawei nel caso del 5G.

Per l'Italia, che è nodo di transito per cavi che connettono Europa, Medio Oriente e Africa, questa dimensione ha implicazioni dirette sulla sovranità digitale nazionale.

⁶² NIST (2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards, 13 agosto 2024.

⁶³ Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79.

⁶⁴ Il concetto trae origine dal *Panopticon*, un carcere ideale progettato nel 1791 dal filosofo e giurista inglese Jeremy Bentham. Il concetto chiave è la sorveglianza invisibile e totale: una struttura circolare con una torre centrale permette a un solo guardiano di osservare tutti i detenuti, senza che questi ultimi possano capire quando sono effettivamente controllati.

⁶⁵ Salgado, R. (2024), *Undersea Cables, Hyperscalers, and National Security*, Hoover Institution, Stanford University, Aegis Series Paper No. 2304

Effetto *choke-point*. Consiste nella possibilità di bloccare, limitare o manipolare i flussi di dati o energia sfruttando il controllo di punti di passaggio obbligati. Le reti infrastrutturali presentano *choke-point* geografici che conferiscono agli Stati con posizioni strategiche una leva significativa. Ad esempio, l'Egitto costituisce uno snodo cruciale per i cavi tra Asia ed Europa e più in generale il 90% del traffico Europa-Asia transita per il Mar Rosso/Bab el-Mandeb: questa concentrazione configura una dipendenza strategica in cui l'interruzione di un singolo nodo produce effetti sistemici a scala globale.

L'effetto *choke-point* può incidere sulla resilienza nelle fasi di manutenzione e riparazione. Gli Stati costieri mantengono il diritto di disciplinare l'accesso alle proprie acque territoriali per le navi specializzate nella riparazione dei cavi: possono quindi negare o ritardare il permesso di accesso a navi di riparazione, richiedere ispezioni, imporre condizioni operative che rallentano gli interventi.

Questo meccanismo, apparentemente tecnico e procedurale, può trasformarsi in uno strumento di pressione politica di notevole efficacia. Un esempio recente è quanto accaduto nello Yemen, dove la frammentazione dell'autorità politica ha rallentato le operazioni di riparazione del cavo AAE-1 nel Mar Rosso: la sovrapposizione tra le rivendicazioni degli Houthi e quelle del governo internazionalmente riconosciuto ha ostacolato per mesi il rilascio delle autorizzazioni necessarie all'ingresso delle navi di riparazione, con effetti significativi sulla connettività di una vasta area geografica.⁶⁶ La dipendenza delle infrastrutture subacquee dall'accesso fisico alle acque territoriali di Paesi terzi per le operazioni di manutenzione è una vulnerabilità strutturale che non può essere eliminata attraverso misure tecniche, ma soltanto attraverso accordi diplomatici e di cooperazione preventivi.

3.5 Mappatura dei rischi

L'analisi degli attori, dei vettori e delle fasi del ciclo di vita infrastrutturale converge nella costruzione di una matrice di rischio che consente di sistematizzare le vulnerabilità identificate e di orientare le priorità di risposta. La matrice si articola lungo due assi principali: la probabilità di occorrenza (da bassa ad alta, in funzione della frequenza storica degli eventi e della disponibilità delle capacità necessarie) e la gravità dell'impatto (da limitata a sistemica, in funzione dell'estensione degli effetti e dei tempi di ripristino).

⁶⁶ Leccese, G. (2025), "Chokepoint Above and Below the Surface: The Red Sea's Emerging Infrastructure Challenge", *Istituto Affari Internazionali (IAI)*, IAI Briefs, no. 8, <https://www.iai.it/it/pubblicazioni/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge>

Vettore	Governance & Progettazione	Costruzione	Installazione	Esercizio	Riparazione & Manutenzione
FISICO Sabotaggio · Tapping Attacchi navali	In questa fase non c'è ancora una dimensione fisica su cui eventuali attori ostili possono agire.	Possibile inserimento di backdoor e dispositivi spia (nel caso di cavi di comunicazione), ma problema maggiormente relativo a dimensione cyber e geoeconomica.	Attacchi cinetici a navi posacavi durante le operazioni di installazione o in porto. ► Statuali (marine militari) + non statuali (Houthi, pirateria ecc.)	Sabotaggio e tapping (per cavi di comunicazione) con diversi vettori in base alla profondità e alla porzione di infrastruttura (wet/dry plant). (Trascinamento ancore nel Mar Baltico 2022-2025, Operation Tempora, 2013) ► Statuali (marine militari, servizi di intelligence) + non statuali (flotte ombra, milizie e gruppi terroristici)	Attacchi cinetici a navi di riparazione durante le operazioni (Somalia 2016) o in porto ► Statuali (marine militari) + non statuali (Houthi, pirateria ecc.)
CYBER Compromissione IT/OT Supply chain digitale Pre-positioning	Supply chain HW/SW; Backdoor EMS/NMS (SMW6/PLCN) ► Statuali (PLA/MSS, HMN Tech)	Firmware compromesso; trojanized update (SolarWinds) ► Statuali + mercenari digitali (proxy)	Accesso remoto CLS; credential theft (HSI 2022) ► Statuali; IAB/ cybercrime organiz.	Management plane; pre-positioning (Volt Typhoon; Kyivstar) ► Statuali (GRU Sandworm, PLA Volt Typhoon, IRGC MuddyWater)	NOC/dispatch; recovery drag; wiper coordinamento ► Statuali (priorità); ransomware-as-a-service (non stat.)
GEO- ECON. Permessi · Choke point Weaponized interdependence Controllo supply chain	Veto su rotte; esclusioni vendor (HMN Tech/SMW6) ► Statuali (RPC/USA)	Concentrazione mercato; dipendenza vendor strategici ► Statuali (aziende nazionalizzate o sotto controllo statale indiretto) + attori economici (grandi suppliers)	Permessi posa; leve diplomatiche (choke point geografici). Possibile posizionamento di backdoor e dispositivi spia durante le operazioni. ► Statuali (stati costieri; EEZ leverage)	Nel caso dei cavi di comunicazione, dominio hyperscalers su flusso di informazioni (Google, Meta, Amazon) ► Statuali (aziende nazionalizzate o sotto controllo statale indiretto) + attori economici (hyperscalers)	Permessi per accesso ad acque territoriali. Possibile posizionamento di backdoor e dispositivi spia durante le operazioni (cavi di comunicazione). ► Statuali (controllo flotta); non statuali (logistica privata)

Tabella 1. Matrice di rischio per le infrastrutture sottomarine

Le categorie di rischio che emergono come prioritarie per il profilo strategico italiano sono:

Categoria di Rischio	Descrizione	Esempi
Rischio A — Alta probabilità / Alto impatto	Eventi con elevata possibilità di occorrenza e conseguenze gravi sulle infrastrutture critiche.	• Danni accidentali da ancore e reti da pesca nei fondali poco profondi (Canale di Sicilia, Canale di Otranto, aree adriatiche) • Attacchi cyber di pre-posizionamento contro sistemi di gestione delle landing station • Compromissione della supply chain digitale nei processi di aggiornamento software
Rischio B — Media probabilità / Alto impatto	Minacce meno probabili, ma comunque significative e potenzialmente molto dannose.	• Sabotaggio fisico di infrastrutture in acque poco profonde da parte di attori statali con capacità di negazione plausibile • Attacchi fisici o interdizione diplomatica alle navi di riparazione in crisi regionali (Mar Rosso e Stretto di Hormuz) • Danneggiamento di cavi nei choke point globali (Suez, Hormuz) per cause indirette derivanti da instabilità geopolitica
Rischio C — Bassa probabilità / Impatto sistemico	Eventi rari ma con potenziale di causare danni su vasta scala e interrompere intere reti.	• Sabotaggio coordinato di infrastrutture multiple in acque profonde (richiede capacità statale avanzata) • Attacco combinato fisico-cyber con disruption prolungata su più infrastrutture • Harvest-now-decrypt-later applicato sistematicamente al traffico governativo e militare
Rischio D — Probabilità variabile / Impatto moderato	Rischi eterogenei con impatti più contenuti ma comunque rilevanti, anche reputazionali.	• Danni da fenomeni naturali (sismicità, frane sottomarine) in aree geologicamente instabili • Operazioni hacktiviste o cybercrime con effetti limitati ma alto impatto reputazionale • Pressioni geoeconomiche tramite vendor exclusion nella supply chain

Tabella 2. Matrice Rischio - Impatto

La lettura della matrice suggerisce alcune implicazioni per le politiche di risposta. Il rischio di maggiore urgenza non è necessariamente quello di maggiore impatto potenziale (il sabotaggio coordinato multiplo in acque profonde), ma quello della categoria A: gli eventi ad alta probabilità e alto impatto che si verificano già oggi con frequenza documentata in altre zone geografiche, come il Mar Baltico. La prioritizzazione delle misure di protezione passiva (*hardening*, ridondanza), della sorveglianza nelle aree costiere e dello sviluppo di capacità di risposta rapida risponde a questo profilo di rischio prioritario. Al contempo, la gestione del rischio C, a bassa probabilità ma impatto sistemico, richiede investimenti di lungo periodo nelle capacità di deterrenza e nei meccanismi di risposta coordinata a livello NATO e UE, che non producono effetti immediati ma sono indispensabili per la resilienza strategica di lungo termine.

10. Soluzioni di difesa e modelli di protezione

4.1 Misure di prevenzione, sorveglianza e deterrenza nel contesto subacqueo

La protezione delle infrastrutture critiche sottomarine va inquadrata in un'ottica integrata. Troppo spesso ci si focalizza sulla fase di riparazione e ripristino. Va invece considerato tutto il ciclo di vita dell'infrastruttura per rendere veramente operativo il sistema di sicurezza. In questo modo i primi accorgimenti di sicurezza vanno implementati già nella fase di programmazione e di decisione di costruzione dell'opera. Ulteriori considerazioni vanno fatte a riguardo della catena di approvvigionamento che porta alla costruzione del cavo. A ciò, seguono le valutazioni sulla posa in mare, sul monitoraggio, sulla deterrenza e prevenzione. Soltanto dopo queste fasi è opportuno focalizzarsi sulla fase di riparazione e ripristino.

La *Maritime Domain Awareness* (MDA) è riconosciuta come la dottrina più funzionale nel garantire la sicurezza dello spazio marittimo⁶⁷.

Muovendo da questa premessa, la conoscenza dell'ambiente marittimo non può esaurirsi in un'operazione di semplice raccolta di dati, ma deve estendersi ad un processo di "comprensione" che trasforma le informazioni provenienti da sensori e fonti umane in conoscenza utile per definire misure adeguate di protezione e risposta. Ciò, dal punto di vista dottrinale, è presentato come fondamentale per la cosiddetta *deterrence by detection*, ovvero la capacità di rilevare e attribuire con maggiore probabilità attività anomale, scoraggiando così uno o più attori ostili dal ricorso a tattiche ibride.

In riferimento all'ambiente subacqueo questo pensiero si è evoluto nel concetto di *Underwater Domain Awareness* (UDA). Le implicazioni pratiche di questa evoluzione sono diverse. Negli abissi, infatti, la barriera non è più esclusivamente di accesso ai dati, ma è anzitutto fisica: l'acqua è infatti un elemento eccellente nello schermare le onde radio e quelle elettromagnetiche.

Se nel quadro dell'MDA la consapevolezza del dominio marittimo si fonda in larga parte su attività di pattugliamento e monitoraggio (basate sulle tecnologie che operano nello spazio aereo-marittimo), nel contesto subacqueo questo primo livello di sorveglianza si confronta con una realtà diversa, dove tali strumenti incontrano i limiti fisici dell'ambiente acquatico.

Pertanto, la complessità della dimensione subacquea impone un passaggio dall'utilizzo di dati isolati alla creazione di reti integrate che aggregino diverse tecnologie, con l'obiettivo di rendere più trasparente la colonna d'acqua e proteggere al meglio le infrastrutture critiche che vi si trovano immerse.

A livello tecnico, le tecnologie più efficaci per la dottrina UDA sono i *sonar*, distinti in attivi e passivi, che sono alla base del ciclo operativo SDCL-A (*Search, Detect, Classify, Localize to Attack*). I primi offrono certamente una localizzazione più accurata tramite l'emissione di impulsi, risultando più efficaci per la fase *Search-Detect-Localize* del ciclo SDCL-A lungo i tracciati di cavi e condotte, grazie alla capacità di generare profili

⁶⁷ Bueger & Edmunds (2024), "Understanding Maritime Security": Pag. 173

dettagliati del fondale; di contro, espongono però la piattaforma che li impiega, rivelandone la posizione⁶⁸.

I *sonar* passivi si limitano invece a raccogliere segnali acustici e sono perciò privilegiati per la fase *Classify–Localize* del ciclo, in quanto consentono di monitorare in modo più prolungato e “silenzioso” le aree intorno a gasdotti e cavi; il loro principale limite è però rappresentato dai possibili falsi allarmi causati dal rumore di fondo oceanico e dalla minore precisione nella stima di distanza e profondità. Accanto ai sensori acustici, vi sono anche i sistemi basati sulla *Magnetic Anomaly Detection* (MAD), che lavorano tramite la misurazione di piccole variazioni nel campo magnetico terrestre dovute alla presenza di masse metalliche, come gli scafi dei sottomarini. Parallelamente, negli ultimi anni si stanno diffondendo sempre più tecnologie che utilizzano sensori ottici e strumenti di *Light Detection and Ranging* (LiDAR) batimetrici, che consentono, attraverso la tecnologia laser, di acquisire modelli tridimensionali ad alta risoluzione di condotte e cavi sulla superficie del fondale. Essi permettono di identificare deformazioni strutturali, erosioni locali e, rispetto agli aspetti più strettamente di difesa, segni di manipolazione fisica⁶⁹.

L'efficacia delle tecnologie di rilevamento dipende tuttavia dalle piattaforme attraverso cui essi vengono dispiegate e utilizzate operativamente. In passato lo strumento per eccellenza dell'ambiente subacqueo erano i sottomarini, il cui impiego negli ultimi decenni ha però conosciuto un forte cambio di paradigma nelle strategie di sicurezza marittima degli Stati: da deterrenti strategici per le loro capacità di lancio dei missili balistici intercontinentali, nonché per essere gli assetti principali per la lotta antisommergibile o antinave, si sono progressivamente evoluti in chiave multi-dominio⁷⁰. Come visibile anche dallo sviluppo del prossimo U212 NFS italiano o dello svedese A26, i sottomarini sono ormai progettati per proiettare potenza di combattimento, raccogliere informazioni e dirigere azioni in aria, in superficie, nello spazio, nel cyberspazio e nello spettro elettromagnetico.⁷¹ In questo senso, oltre a fungere da nodi di una rete di sensori subacquei e non, questi dovranno essere in grado di funzionare come “navi madre” per sistemi unmanned quali ROV e AUV. Tali sistemi senza pilota forniscono infatti diversi vantaggi e opportunità per la protezione delle infrastrutture subacquee: nel caso degli AUV, questi possono eseguire percorsi pianificati su vaste aree, raccogliendo informazioni sullo stato delle infrastrutture lungo rotte prestabilite; mentre i ROV sono utili per un impiego finalizzato ad ispezioni ravvicinate ed interventi diretti su cavi e condotte, grazie ad un equipaggiamento composto da videocamere ad alta definizione e bracci operativi⁷².

Nel lungo periodo, infine, un cambiamento rilevante rispetto a questi mezzi riguarderà l'evoluzione delle capacità operative tramite modelli di Intelligenza Artificiale. Gli studi più recenti sui contesti applicativi dell'IA nell'ambiente subacqueo evidenziano alcune linee di sviluppo prioritarie, tra cui un miglioramento dell'autonomia decisionale, tanto con riferimento ai percorsi da attraversare quanto nelle capacità di scelta degli obiettivi della missione, se non addirittura di individuazione del *target*⁷³. Ciò risponde alla

⁶⁸ Sensors (2025), *Route Optimization for Active Sonar in Underwater Surveillance*, p. 2

⁶⁹ Milan Vego (2019), *Maritime Strategy and Sea Denial*, p. 112

⁷⁰ CeSI (2024), *Il (quasi) dominio sottomarino*, p. 45

⁷¹ Fincantieri, “U212 NFS”, <https://www.fincantieri.com/it/business/prodotti/navi-per-la-difesa/sommergibili/u212nfs>; Saab, “The world’s first 5th-generation submarine”, <https://www.saab.com/products/5th-generation-submarine>

⁷² European Commission Expert Group (2026), *Security and Resilience of EU Submarine Cable Infrastructures*, p. 9

⁷³ Fondazione Leonardo (2023), *Rapporto Civiltà del Mare*, pp. 34-36

necessità di aggirare i problemi di comunicazione con chi si trova in superficie, che spesso risulta limitata o addirittura assente.

Al di là dei progressi tecnologici, l'efficacia di questi sistemi continua a dipendere dalle capacità umane: il processo di raccolta e analisi dei dati perde la sua importanza se non è integrato in sistemi efficienti di comando e controllo capaci di aggregare le informazioni ricevute da agenzie e istituzioni diverse, attraverso un processo definito "interagenzia".⁷⁴

Di conseguenza, un limite forse ancora più significativo di quelli tecnologici è di natura sociale: ci si riferisce alla scarsa disponibilità delle organizzazioni coinvolte nella sicurezza marittima a condividere informazioni tra loro, che si riscontra perfino tra agenzie e istituzioni pubbliche appartenenti al medesimo quadro istituzionale di sicurezza.

Inoltre, una dinamica simile emerge anche in relazione al rapporto tra pubblico e privato, anch'esso essenziale per realizzare un'efficace protezione delle infrastrutture subacquee⁷⁵.

Gli elevati costi di progettazione, sviluppo e integrazione hanno, almeno finora, limitato l'accesso alla dimensione subacquea a poche potenze tecnologicamente avanzate, rendendo inoltre estremamente rara la presenza di attori non statali organizzati in questa dimensione operativa⁷⁶. In previsione è tuttavia probabile che nel medio-lungo periodo questi sistemi comincino a diffondersi in modo analogo a quanto avvenuto per i droni aerospaziali: la miniaturizzazione, l'abbattimento dei costi e il passaggio di *know-how* ad un numero più ampio di attori renderanno dunque accessibili le capacità di osservazione, intrusione o manipolazione di infrastrutture subacquee ad un numero crescente di Stati, *proxy actors* ed entità non statali. Da ciò consegue che questo processo di proliferazione incrementerà la complessità delle minacce ibride e renderà ancora più impegnativa la sfida della *deterrence by detection*, conferendo un'importanza ancora più cruciale ai sistemi di UDA.

4.2 Protezione passiva e resilienza delle infrastrutture

La protezione delle infrastrutture critiche sottomarine non può esclusivamente basarsi sulla capacità di individuare attività ostili, poiché è difficile immaginare che nel breve periodo si possa ottenere una protezione totale dalle possibili minacce in un ambiente tanto vasto come quello subacqueo. È questa la ragione per cui, accanto alle misure di deterrenza e sorveglianza, lo sviluppo di strategie di protezione passiva e resilienza delle infrastrutture assume un ruolo di primaria importanza quando si discute di protezione dei fondali marini⁷⁷.

In questo contesto, la prima regola di un processo che non permetta che la continuità del servizio venga interrotta in modo significativo da un danneggiamento riguarda la capacità di una rete di ridistribuire i flussi, cioè deviarli su percorsi alternativi

⁷⁴ Critical Maritime Infrastructure Protection: What's the Trouble? (Bueger & Liebetrau, Marine Policy 155), p. 6

⁷⁵ Why Adversaries Target CUI and Challenges in Protection (in WHY-CUI-IS-THE-TARGET.pdf), p. 3.

⁷⁶ La minaccia alle infrastrutture sottomarine del "Mediterraneo Allargato". I mezzi e le possibili tecniche, pp. 2, 4. (Art-R.M.-su-Minaccia-CUI.pdf)

⁷⁷ Critical maritime infrastructure protection: What's the trouble?, 2023, p. 6

assorbendo così l'interruzione di uno o più segmenti senza collassare⁷⁸. Difatti, il concetto di diversificazione delle rotte si riferisce tanto all'aumentare il numero dei cavi quanto ad evitare una concentrazione eccessiva lungo le stesse traiettorie, in particolare se sono ad alto rischio di danni accidentali ovvero di natura geopolitica. La diversificazione geografica, oltre a rispondere a criteri quantitativi, utilizza quindi anche criteri qualitativi che fanno riferimento alla distribuzione del rischio percepito.

Dal punto di vista economico, tuttavia, è chiaro che sia la ridondanza dei cavi che la diversificazione dei punti di approdo e delle interconnessioni possono risultare economicamente non convenienti per gli operatori privati⁷⁹. Questo si deve tenere in conto perché le esigenze economiche possono creare contrasti tra il settore privato e quello pubblico: quest'ultimo, infatti, non può che valorizzare primariamente la continuità del servizio, al di là dei costi, poiché da esso dipendono gran parte dei servizi essenziali di uno Stato, tra cui le stesse componenti della sicurezza nazionale.

Un ulteriore livello di protezione si realizza quando si rende materialmente più difficile (e quindi meno probabile) un'interruzione del servizio; questo può avvenire attraverso interventi di protezione fisica delle infrastrutture collocate sui fondali. L'esempio più immediato è l'interramento dei cavi nei fondali. È però utile precisare che non esiste una soluzione standard di *hardening* applicabile indistintamente a tutti i contesti, perché l'efficacia dipende dalle caratteristiche geologiche dei diversi fondali, nonché dalla natura della minaccia che si intende prevenire. Inoltre, non sempre una maggiore profondità di interrimento equivale ad un aumento proporzionale della sicurezza dell'infrastruttura. Va infatti considerata la possibilità di guasti imprevisti e le conseguenti operazioni di riparazione o sostituzione. A livello tecnico va quindi trovato un compromesso, cioè un equilibrio tra protezione e necessità di manutenzione. Accanto all'interrimento, un'ulteriore misura di protezione passiva è invece rappresentata dall'*armouring*, ossia dal rafforzamento fisico del cavo nei tratti maggiormente esposti a urti, abrasioni o altri traumi cinetici non prevedibili⁸⁰.

Le operazioni di *hardening* racchiudono, infine, alcune misure apparentemente meno "materiali" ma altrettanto importanti nel contesto della protezione passiva, come ad esempio l'istituzione delle cosiddette "*cable protection zones*"⁸¹. Una misura come quest'ultima permette di evitare molti dei possibili danni accidentali e allo stesso tempo si inserisce tra le strategie più propriamente difensive nei confronti di possibili attori ostili, a cui viene negato l'accesso all'area di interesse.⁸² Tuttavia, il contraltare di questo tipo di misure è il rischio di limitare eccessivamente alcune attività economiche essenziali (ad esempio la pesca). Quindi anche misure come queste devono seguire una logica di equilibrio tra la difesa e il rischio effettivo.

Il concetto di resilienza può configurarsi infine come l'insieme delle azioni atte a mantenere le funzioni essenziali, pur in forma degradata, a seguito di un evento (sia

⁷⁸ Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure (UNIDIR), p. 10

⁷⁹ The diversity, frequency and severity of natural hazard impacts on subsea telecommunications networks, p. 14

⁸⁰⁸⁰ The diversity, frequency and severity of natural hazard impacts on subsea telecommunications networks, 2024, p. 14

⁸¹ Enhancing the Resilience of the Global Submarine Cable Ecosystem (CCPL, 2025), p. 21

⁸² Le cable protection zones sono "sono aree geografiche, individuate e proclamate dagli Stati costieri, al cui interno vengono ridotte o proibite alcune attività, in grado di danneggiare i cavi sottomarini [...]". Nigro, E. (2024), "I Cavi Sottomarini tra Problemi Giuridici e Problemi Spaziali", Rivista Diritto dei Trasporti, Anno XXXVII n. 1, <https://www.dirittodeitrasporti.it/app/uploads/2024/06/IV.-Nigro.pdf>

che esso sia deliberato o di natura accidentale) che mette in crisi il sistema. In questo contesto, la continuità operativa costituisce dunque un punto di raccordo tra i concetti di protezione passiva, gestione dell'emergenza e ripristino della funzionalità, consentendo di trasformare una vulnerabilità in un danno gestibile, anziché in una paralisi sistemica⁸³. Ciò implica la presenza di protocolli capaci di assicurare una segnalazione tempestiva dell'avvenimento e l'attivazione di un coordinamento tra il livello operativo e il livello politico-amministrativo⁸⁴.

Tuttavia, il mantenimento delle funzioni essenziali è tanto una questione di tecnologia quanto di *governance*⁸⁵. Ciò vale tanto in tempo di pace, con interruzioni derivanti da eventi di natura incidentale, che in scenari ambigui o apertamente conflittuali. Di fatto la continuità operativa deve essere pensata come la capacità di attraversare tutto l'intervallo temporale che separa il momento del danno dal ripristino del sistema e non ai soli momenti immediatamente successivi all'interruzione.

4.3 Risposta e ripristino a seguito dell'interruzione

Al verificarsi di un evento che interrompe i flussi di energia o di dati che scorrono attraverso i fondali è essenziale che si avvii un processo di risposta rapida ben definito. A seguito della segnalazione del guasto, è dunque fondamentale un accertamento preliminare, che consenta di raccogliere fin dal primo momento le informazioni sul tipo di interruzione, se può considerarsi di natura dolosa, nonché sul suo eventuale impatto transfrontaliero, così da poter allertare i paesi vicini e alleati. In questa fase, l'accertamento preliminare può essere orientato anche da alcuni indicatori operativi, come la presenza di navi battenti bandiera potenzialmente ostile in sosta anomala in prossimità delle tratte sensibili, o ancora la disattivazione dei sistemi AIS nonché altri comportamenti di navigazione irregolari. Se è vero che tali elementi non possono ritenersi sufficienti di per sé a dimostrare una condotta ostile, danno però un'idea più precisa delle probabilità che l'evento sia plausibilmente accidentale ovvero un episodio compatibile con un sabotaggio sottosoglia.

Il processo di risposta iniziale, parallelamente all'operazione di ricostruzione informativa, richiede anche una messa in sicurezza rapida dei segmenti più accessibili e/o vulnerabili dell'infrastruttura. Ne consegue che, soprattutto in contesti in cui si ipotizza un danneggiamento deliberato già nelle prime ore successive all'avvenimento, la risposta deve includere misure di controllo degli accessi e protezione dei siti costieri, così da impedire che all'interruzione iniziale si sommino ulteriori vulnerabilità.

I primi problemi di attribuzione acquistano una rilevanza politico-strategica non trascurabile. Ne consegue che l'evento ha un vero e proprio significato politico, che influenza il tipo e il grado di risposta mobilitata da parte delle autorità nazionali, o se necessario, prendendo ad esempio il contesto euro-atlantico, dei quadri di cooperazione multilaterali. Nell'odierno contesto di rinnovata competizione internazionale, la protezione delle infrastrutture sottomarine viene infatti sempre più considerata una questione di coordinamento tra autorità nazionali, Unione europea e

⁸³ Critical Infrastructure Protection, Risk Management, and Resilience (Pesch-Cronin & Marion, 2024), pp. 11, 14

⁸⁴ Maritime Critical Infrastructure Protection (MCIP), MARSEC COE, 2023, pp. 14-15

⁸⁵ Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure, UNIDIR, 2025, pp. 41-42

NATO, soprattutto nei casi in cui è difficile distinguere tra un'interruzione accidentale e minaccia deliberata da parte di un attore ostile.

In merito all'Alleanza Atlantica, si tende spesso a collocarla in un quadro strategico di deterrenza e di risposta militare. Diversamente, l'UE si muove più su un terreno di *governance* delle dipendenze critiche, quindi più vicino alla regolazione e al concetto di resilienza.

La differenza tra le due entità emerge anche dalle formule strategiche richiamate nei documenti ufficiali: mentre la NATO è spesso ricondotta alla logica “*prepare, deter, defend*”, l'approccio dell'Unione europea viene più facilmente sintetizzato nei termini di “*awareness, resilience, response*”⁸⁶.

Questo dualismo nel Continente Europeo non è però privo di attriti, che infatti emergono in quella che rischia di sfociare in una sovrapposizione funzionale più che in una complementarità necessaria, anche a causa della diversa natura istituzionale delle due organizzazioni.

La gestione di una crisi riguardante una o più infrastrutture sottomarine si presenta quindi come un banco di prova per la capacità Euro-Atlantica di creare un'unica architettura di sicurezza.

In un contesto ambiguo non vi è semplicemente un problema rispetto “chi comanda”: la pressione fatta nella società assume infatti più valenze, dal punto di vista operativo ma anche politico e simbolico. Di conseguenza, la comunicazione istituzionale riveste uno strumento fondamentale, la cui sottovalutazione o mancanza rischia di aggravare il quadro della situazione. Comunicare rapidamente che le procedure di risposta sono state attivate e che il ripristino è in corso può contribuire tanto a rassicurare gli utenti quanto a contenere il rischio di *escalation* e di perdita di credibilità istituzionale.

Una comunicazione può dunque definirsi davvero efficace se diventa un elemento di tenuta dell'assetto istituzionale, allontanando il rischio che si diffonda una percezione di perdita di controllo politico. Si può dunque sostenere che la gestione di una crisi, nella dimensione subacquea, richieda una doppia credibilità: operativa, legata alla rapidità e alla coerenza del coordinamento tra gli attori coinvolti, e narrativa, cioè la capacità delle istituzioni di presentare il fatto come oggetto di una risposta ordinata e non di una reazione improvvisata.

4.4 Il processo di riparazione

Le tecniche di riparazione costituiscono il segmento conclusivo, ma anche più concretamente verificabile, dell'intera catena di risposta all'incidente.

Difatti, dopo che il tratto da riparare è stato individuato, si avvia una riflessione riguardante qual è la migliore tecnica per intervenire. Questo tipo di attività richiedono l'utilizzo di piattaforme senza equipaggio di tipologia ROV o, nei tratti meno profondi, la possibilità di far intervenire subacquei specializzati. Un elemento che assume una

⁸⁶ NATO, *Baseline Requirements for the Protection of Critical Undersea Infrastructure* (Brussels: NATO, 2023), pp. 12–17. Cfr. anche EU Expert Group, *Cable Security Toolbox*, misura TM03, pp. 21–24

particolare importanza è quindi l'effettiva disponibilità di queste capacità. Alcuni rapporti sottolineano che fino al 2025 esistevano circa un'ottantina di navi adatte a livello globale, spesso però costantemente impegnate per la posa di nuove tratte, con evidenti ripercussioni sulla possibilità di intervenire in modo rapido in caso di guasti⁸⁷. Di fatto si confida che i guasti restino sempre gestibili entro una soglia ordinaria: se in un contesto di conflitto aperto queste infrastrutture venissero prese di mira in modo più massiccio, emergerebbero tutti i limiti di un sistema non in grado di reggere un'eventualità simile. In questo scenario, infatti, le criticità provocate da più guasti concorrenti saturerebbero rapidamente le capacità di risposta già limitate.

Oltre che dal punto di vista delle capacità, i processi di riparazione hanno delle ripercussioni che toccano il piano del diritto e della diplomazia. Come anticipato nel capitolo precedente, i fattori geopolitici hanno infatti una loro influenza, ad esempio in merito all'accesso delle navi riparatrici in acque territoriali di Stati diversi. Un altro elemento riguarda invece la possibilità, per le istituzioni pubbliche, di disporre delle competenze e dei mezzi necessari all'intervento, il che favorisce un processo più rapido slegato dalle dinamiche aziendali e di politica internazionale.

Ancora una volta queste tematiche, pur altamente tecniche, tendono a sfociare in modo naturale nel contesto del coordinamento politico-istituzionale.

⁸⁷ Runde, D. F., Murphy, E. L., & Bryja, T. (2024). Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition. Center for Strategic and International Studies

11. Esperienze estere

5.1 Stati Uniti

Gli Stati Uniti esercitano la leadership globale nella dimensione subacquea grazie alle capacità offensive del Cyber Command, che opera secondo la dottrina Defend Forward, e ai sistemi di sorveglianza navale avanzata, tra cui il sistema Mainsail per il tracking della flotta ombra russa. La governance è tuttavia frammentata tra DHS (Department of Homeland Security) - CISA (Cybersecurity and Infrastructure Security Agency), DoD (Department of Defense), DoS (Department of State) e FCC (Federal Communications Commission), in assenza di un'agenzia dedicata centralizzata. Il principale paradosso strutturale è che il 69% della capacità globale dei cavi è controllata da hyperscaler privati americani, rendendo la protezione delle infrastrutture critiche intrinsecamente dipendente dalla cooperazione pubblico-privata⁸⁸. Il collo di bottiglia più critico è la capacità di riparazione: solo due navi specializzate operano sotto bandiera americana su una flotta globale di 65-80 unità, una vulnerabilità esplicitamente riconosciuta dal DHS e non ancora risolta⁸⁹.

5.2 Francia

La Francia è l'unico Paese europeo che combina sovranità normativa, industriale e militare nella dimensione subacquea, rappresentando il benchmark di riferimento per l'Italia. Orange Marine gestisce il 15% della flotta mondiale di navi posacavi (6 unità, operative entro 24 ore) e Alcatel Submarine Networks (ASN), nazionalizzata all'80%, aggiunge ulteriori 6 navi con 650.000 km di cavi posati nel mondo: una Base Industrielle et Technologique de Défense senza equivalenti nel continente. La dottrina militare "conoscere, sorvegliare, agire" è operazionalizzata dalla cellula CEPHISMER della Marina, con AUV e ROV operativi fino a 6.000 metri⁹⁰. Il quadro normativo è stato spostato da civile a securitario, con pene severe per il danneggiamento delle infrastrutture e controllo rafforzato sui droni sottomarini. Il principale punto di attenzione è la concentrazione di 8-13 cavi intercontinentali sull'hub di Marsiglia, che configura un single point of failure potenziale per la connettività europea⁹¹.

5.3 Giappone

Il Giappone ha sviluppato l'approccio più sistematico e integrato in Asia, combinando governance centralizzata (Cabinet Secretariat, National Security Secretariat), capacità industriale sovrana e proiezione multilaterale. Con una quota stimata intorno al 30% del mercato globale delle navi di posa e riparazione cavi e sussidi statali fino al 50% per l'acquisizione di nuove unità⁹²; Tokyo è l'unico competitor credibile alla predominanza francese in questo settore. Sul piano multilaterale, guida la Quad Partnership for Cable Connectivity and Resilience e il programma di capacity building

⁸⁸ Abels, J., & Babić, M. (2026). Cable wars? Mapping the political economy of submarine cables in an era of geoeconomic competition. Globalizations

⁸⁹ Mahle, M. B. (2025). Subsea cables and US national security. Steptoe LLP

⁹⁰ Secrétariat général de la mer. (2022). L'économie bleue en France - Édition 2022

⁹¹ Ianc, F. (2018, Giugno). Géopolitique des câbles : une vision sous-marine de l'Internet. Centre pour la Technologie et la Société, Département de droit, Fundação Getulio Vargas.

⁹² Cybersecurity Strategic Headquarters, Government of Japan. (2024). The cybersecurity policy for critical infrastructure protection.

verso gli Stati insulari del Pacifico nell'ambito della visione Free and Open Indo-Pacific⁹³. L'accordo Yokohama Zone garantisce coordinamento regionale per gli interventi di emergenza. La minaccia di riferimento, esplicitamente identificata, è la combinazione di capacità russe e cinesi nella dimensione subacquea dell'Indo-Pacifico.

5.4 Australia

L'Australia ha costruito il quadro normativo più maturo tra i Paesi anglofoni: le Cable Protection Zones istituite dal Telecommunications Act 1997 limitano navigazione, pesca e ancoraggio nei corridoi adiacenti ai punti di approdo, e il Critical Infrastructure Risk Management Program impone obblighi vincolanti agli operatori privati. La governance è coordinata dal Department of Home Affairs con l'Australian Signals Directorate per la dimensione cyber. Il principale gap strutturale è la mancanza di una nave nazionale di riparazione cavi: in caso di incidente, Canberra dipende interamente da operatori internazionali, con tempi di intervento non controllabili, una vulnerabilità esplicitamente riconosciuta ma non ancora risolta nei documenti di strategic assessment⁹⁴.

5.5 Svezia

La Svezia ha trasformato radicalmente la propria postura dopo il 2022, elevando la protezione delle infrastrutture marittime critiche (CMI) a priorità di sicurezza nazionale nell'ambito del modello di Difesa Totale (Totalförsvär), che integra dimensione civile e militare. L'adesione alla NATO ha trasformato il Baltico in un "lago alleato" e ha abilitato la partecipazione alla missione Baltic Sentry e all'operazione Nordic Warden (JEF), che utilizza sistemi AI per il monitoraggio in tempo reale della flotta ombra russa. La governance è centralizzata presso la Swedish Civil Contingencies Agency (MSB). Anche Stoccolma, come Australia e Irlanda, non dispone di una flotta statale di navi posacavi, dipendendo da operatori privati per la riparazione, con ulteriori complicazioni operative legate alle condizioni invernali del Baltico settentrionale.

5.6 Regno Unito

Il Regno Unito dispone di una delle infrastrutture di cavi sottomarini più estese al mondo nell'Atlantico nord-orientale e di una base industriale navale di difesa significativa. Il Joint Maritime Security Centre (JMSC) garantisce il coordinamento interagenzia tra Marina Reale, Guardia Costiera e operatori civili, con l'NCSC responsabile della dimensione cyber. I sommergibili della classe Astute svolgono funzioni di sorveglianza e intelligence nelle aree strategiche. La partecipazione ad AUKUS proietta la cooperazione su tecnologie sottomarine avanzate, inclusi AUV di nuova generazione, con USA e Australia. Il principale punto di attenzione è la dipendenza da operatori privati internazionali per le operazioni di riparazione ad alta profondità.

⁹³ Cannon, B. J. (2025). Undersea cable security in the Indo-Pacific: Enhancing the Quad's collaborative approach. *Marine Policy*, 171, 106415.

⁹⁴ Bashfield, S. (2025). Defending seabed lines of communication. *Australian Journal of Maritime & Ocean Affairs*, 17(4), 557-569

5.7 Irlanda

L'Irlanda incarna il paradosso più marcato del panorama europeo: circa i tre quarti dei cavi sottomarini dell'emisfero settentrionale transitano attraverso o vicino alle sue acque, con transazioni finanziarie giornaliere stimate in 10 trilioni di dollari, ma la sicurezza marittima è rimasta a lungo sottodimensionata. Il Nord Stream (2022) ha agito da catalizzatore: il Paese sta centralizzando le competenze sotto il Department of Defence, con una nuova Maritime Security Unit e l'Autorità di Regolamentazione dell'Area Marittima. La dipendenza totale da consorzi privati per la riparazione e l'assenza di capacità autonome di sorveglianza della ZEE, dieci volte più estesa della massa terrestre nazionale, rimangono le vulnerabilità strutturali più urgenti.

5.8 Israele

Israele presenta un profilo di dipendenza marittima estrema: il 99% del commercio estero transita via mare, il mix energetico è composto per il 44% da gas naturale offshore e al 39% da petrolio, e i cavi sottomarini, tra cui il cavo JONAH (2.300 km, Tel Aviv-Bari), costituiscono l'unica connessione digitale praticabile con il resto del mondo, data l'impossibilità di sviluppare rotte terrestri per ragioni geografiche e geopolitiche. Il Paese viene per questo spesso descritto come "un'isola strategica", con tre direttrici di rischio marittimo primarie: il Canale di Suez, lo Stretto di Tiran e le rotte mediterranee adiacenti ad aree ostili (Libia, Siria, Maghreb). La tutela dei giacimenti di gas offshore rappresenta la priorità assoluta dell'agenda di sicurezza marittima israeliana, in un quadro di minaccia dominato dall'Iran e dai suoi proxy regionali (Houthi, Hezbollah). La governance delle infrastrutture critiche subacquee è distribuita e priva di un'autorità centralizzata: il *National Security Council* coordina la pianificazione strategica, la *Israel Security Agency* e la *National Cyber Directorate* gestiscono il monitoraggio delle minacce, mentre il settore privato, guidato da Bezeq ed Exelera, opera in larga autonomia rispetto agli organi governativi. Sul piano operativo, Israele non dispone di capacità nazionali di riparazione dei cavi (la riparazione post-attacco del 2024 fu delegata all'italiana E-marine) e punta sulla cooperazione multilaterale per colmare il gap: emblematico è l'accordo trilaterale con Cipro e Grecia per la costituzione del *Joint Maritime Cybersecurity Centre of Excellence* (MarCCE), dedicato al monitoraggio delle cyber-minacce e allo sviluppo coordinato di capacità operative.

5.9 Cina

La Cina opera contemporaneamente su tre livelli: militare (Marina dell'APL con crescente proiezione atlantica), commerciale-industriale (HMN Technologies/ex Huawei Marine Networks nelle gare per nuovi cavi) e normativo (quadro della Digital Silk Road per la creazione di interdipendenze infrastrutturali favorevoli). La combinazione tra accesso fisico ai sistemi nelle fasi di costruzione e riparazione e la capacità di compromissione dei sistemi di gestione è il profilo di minaccia più preoccupante per l'Europa e per l'Italia. Le esclusioni di HMN da progetti in rotte atlantiche e indo-pacifiche hanno ridotto ma non eliminato la penetrazione cinese nel settore; la difficoltà di esclusione totale è strutturale, data la competitività di prezzo degli operatori cinesi rispetto agli alternativi occidentali.

5.10 Egitto

L'Egitto controlla geograficamente il Canale di Suez, choke point obbligato per oltre il 90% del traffico dati tra Europa e Asia, e ospita alcune delle stazioni di atterraggio più strategiche del Mediterraneo nella zona di Alessandria. La governance è caratterizzata da elevata centralizzazione statale e regime di sicurezza fisica robusto, ma con limitata trasparenza verso i partner internazionali. Gli attacchi Houthi alle infrastrutture subacquee nel corridoio del Mar Rosso (2024) hanno aumentato la pressione sul Cairo per un maggiore coordinamento regionale nella protezione delle dorsali di transito.

5.11 Turchia

La Turchia controlla lo Stretto del Bosforo e i Dardanelli, choke point fondamentali per il traffico tra Mar Nero e Mediterraneo, e ha centralizzato la governance della sicurezza delle infrastrutture critiche sotto la Presidenza della Repubblica, con la Presidenza della Sicurezza Cyber come autorità di coordinamento digitale e il Ministero della Difesa per gli asset marittimi. L'industria della difesa turca in rapido sviluppo include programmi di AUV e sorveglianza subacquea che riducono la dipendenza da fornitori esteri. La postura di autonomia strategica, che mantiene relazioni con tutti gli attori regionali, incluse Russia e Iran, complica la condivisione di intelligence sulle infrastrutture con gli alleati NATO, pur mantenendo piena interoperabilità formale nell'Alleanza.

6. La dimensione subacquea al 2050: quattro futuri per l'Italia

6.1 Perché guardare al 2050, e come.

Le sezioni precedenti hanno restituito la fotografia di una dimensione in rapida trasformazione: un'infrastruttura fisica in espansione, una minaccia in via di strutturazione, un quadro normativo e capacitivo in costruzione. Una fotografia, tuttavia, invecchia in fretta, e le decisioni che il Paese è chiamato ad assumere sul perimetro normativo, sugli investimenti capacitivi della Marina, sulla postura da tenere nei formati NATO e UE, dispiegheranno i loro effetti su un orizzonte misurabile in decenni, non in cicli di bilancio. Per questa ragione la sezione presente integra l'analisi con un esercizio di scenario a orizzonte 2050.

L'esercizio adotta una prospettiva dichiaratamente esplorativa: non intende prevedere quale futuro si realizzerà, né disegnare il futuro desiderabile, ma delimitare lo spazio dei futuri plausibili entro cui l'Italia dovrà comunque muoversi, così da distinguere le scelte robuste, valide in tutti i futuri, da quelle contingenti, valide soltanto in alcuni⁹⁵. Sul piano metodologico si è seguita la tecnica degli scenari a futuri alternativi (*Alternative Futures Scenarios*), che struttura il lavoro in fasi successive: censimento dei fattori di cambiamento, separazione tra tendenze pesanti e incertezze critiche, selezione (verificata attraverso una matrice a impatti incrociati) delle due incertezze dominanti, costruzione dei quattro futuri risultanti dalla loro combinazione e definizione di indicatori di allerta precoce che consentano, negli anni, di riconoscere verso quale scenario il sistema stia scivolando⁹⁶. L'orizzonte a venticinque anni non è casuale: è il tempo minimo perché si compiano le trasformazioni strutturali già in Corso (p.e. la transizione energetica, il rinnovo generazionale delle dorsali in fibra, la maturazione dei sistemi autonomi) e insieme il tempo massimo entro cui le scelte capacitive avviate oggi produrranno flotte, sensori e competenze effettivamente operativi.

6.2 Ciò che accadrà comunque: gli elementi predeterminati.

Prima di divergere, i quattro futuri condividono un terreno comune. Alcune dinamiche presentano infatti un grado di incertezza sufficientemente basso da poter essere considerate elementi predeterminati di qualunque scenario, e conviene dichiararle in apertura perché costituiscono il carico di fondo su cui le incertezze critiche si innestano.

La prima è la crescita strutturale della domanda: il traffico dati, trainato dai servizi cloud e dall'intelligenza artificiale e la domanda elettrica continueranno ad aumentare, e con essi il numero di cavi, di interconnessioni e di nodi che poggiano sul fondale. La

⁹⁵ Sulla distinzione tra scenari predittivi, esplorativi e normativi: Börjeson, L., Höjer, M., Dreborg, K.-H., Ekvall, T., Finnveden, G., "Scenario types and techniques: Towards a user's guide", *Futures*, 38(7), 2006, pp. 723-739;

⁹⁶ Per la tecnica degli *Alternative Futures Scenarios* e il relativo processo (definizione di scopo e orizzonte, identificazione e selezione dei fattori, sviluppo e comparazione degli scenari, definizione degli indicatori, monitoraggio e aggiornamento), nonché per l'impiego della matrice a impatti incrociati a supporto della selezione dei fattori: Valeriani, M., *Intelligence Analysis for Global Politics: Concepts and Techniques to Analyze an Uncertain World*, Routledge, 2025, cap. 6

seconda è l'espansione fisica della superficie di esposizione nazionale: l'eolico offshore previsto nei mari meridionali, le nuove interconnessioni elettriche e l'eventuale nuova capacità di importazione gas aggiungeranno chilometri di infrastruttura e nuovi punti di approdo a un perimetro già oggi esteso. La terza è la persistenza del rischio accidentale (ancoraggi, pesca a strascico, eventi naturali) che la matrice del capitolo 3 colloca nella categoria ad alta probabilità e alto impatto e che crescerà in valore assoluto proprio perché crescerà la superficie esposta, indipendentemente da qualunque evoluzione geopolitica. La quarta, infine, è la maturazione tecnologica della sensoristica subacquea: la capacità tecnica di osservare il fondale migliorerà comunque; ciò che resta aperto è chi la possiederà e con quale copertura, ed è precisamente qui che l'incertezza comincia.

6.3 Le due incertezze critiche.

Dal censimento dei fattori condotto sulla base dei capitoli precedenti emergono due incertezze che dominano tutte le altre per impatto, apertura della traiettoria e reciproca indipendenza.

La prima, di natura tecnologico-strategica, riguarda la proliferazione delle capacità operative subacquee. Oggi la possibilità di agire con efficacia sul fondale sia per mappare, manipolare, riparare o sabotare a profondità significative, resta un oligopolio di poche marine militari e di un ristretto segmento industriale. La traiettoria dei sistemi autonomi e remotizzati, la discesa dei costi, la natura intrinsecamente duale delle tecnologie e la porosità dei regimi di controllo delle esportazioni rendono però plausibile, su un orizzonte venticinquennale, una vera e propria democratizzazione della minaccia: droni subacquei a lungo raggio accessibili a marine minori, ad attori per procura e potenzialmente a soggetti non statuali, con effetti sull'attribuzione che abbiamo già visto è oggi il tallone d'Achille della risposta, sono tutti aspetti destinati ad aggravarsi. All'estremo opposto, regimi di controllo efficaci, colli di bottiglia industriali persistenti e la complessità operativa dell'ambiente profondo potrebbero mantenere la capacità concentrata. L'esito non è scritto: è la prima dimensione di variazione.

La seconda, di natura politico-capacitiva, riguarda la coesione e la capacità collettiva euro-atlantica nella protezione delle infrastrutture subacquee, inclusa la sua base industriale. Il rapporto ha documentato l'avvio di una costruzione istituzionale, dal il coordinamento NATO, alla Raccomandazione (UE) 2024/779 e all'Action Plan europeo sulla sicurezza dei cavi che al 2050 potrà essersi consolidata in un sistema integrato di sorveglianza, deterrenza e risposta, dotato di ciò che oggi manca in modo più vistoso: una capacità industriale presidiata di posa e riparazione, oggi affidata a una flotta mondiale di poche decine di unità specializzate, in larga parte non europee e contese da una domanda crescente. Oppure potrà essersi arenata nella frammentazione: iniziative nazionali scoordinate, dipendenza strutturale dagli operatori privati extraeuropei, a partire dagli hyperscaler, che già oggi controllano una quota dominante della nuova capacità in fibra e a cui si aggiunge una base industriale atrofizzata proprio mentre la superficie da proteggere si espande. Anche qui, l'esito dipenderà da scelte politiche, industriali e di bilancio ancora tutte davanti a noi. Si noti che questa seconda dimensione non è interamente esogena: l'Italia contribuisce a determinarla. Lungi dall'essere un difetto metodologico è la ragione stessa dell'esercizio: nella tradizione

della *prospective*, il futuro non è soltanto qualcosa che accade, ma qualcosa che le istituzioni concorrono a costruire⁹⁷.

L'incrocio delle due dimensioni genera quattro futuri. A ciascuno è associata una denominazione sintetica, una logica interna, la posizione che l'Italia vi occuperebbe e gli indicatori che ne segnalerebbero l'avvicinamento.

I quattro scenari sono riassunti nell'immagine sottostante.

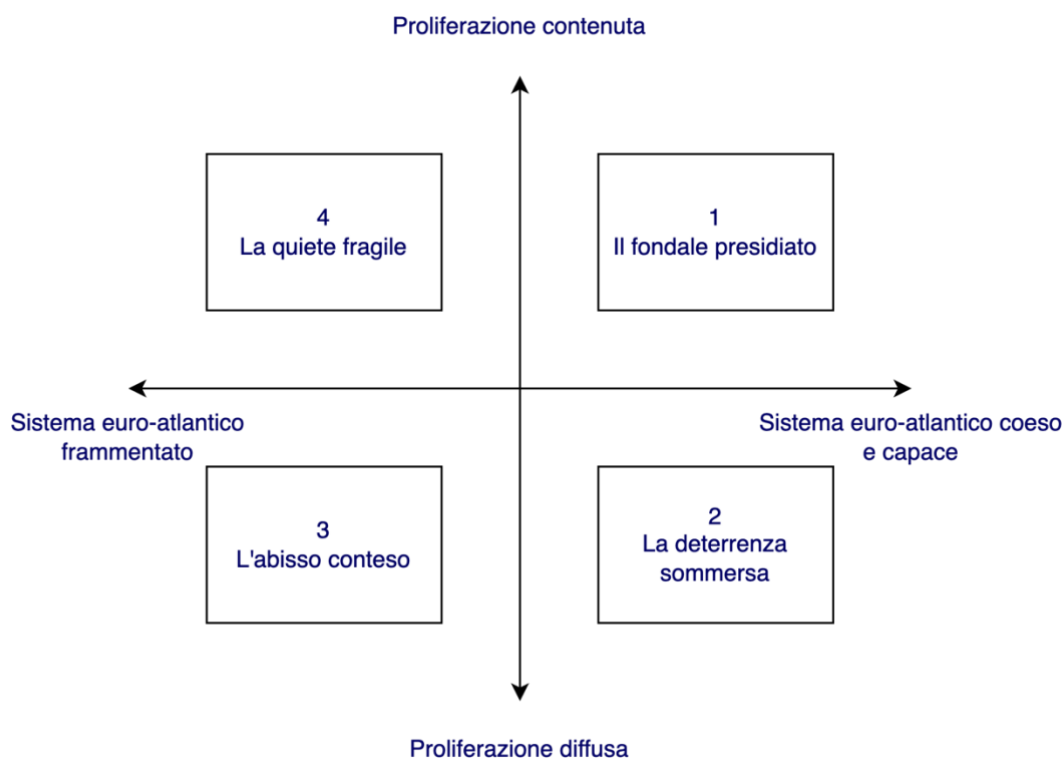


Figura 6: Scenari futuri per l'Italia

6.3.1 Primo scenario - Il fondale presidiato

Proliferazione contenuta, sistema euro-atlantico coeso e capace.

È il futuro della costruzione riuscita. Al 2050 la capacità di operare in profondità è rimasta appannaggio di poche marine, mentre il sistema euro-atlantico ha completato la propria architettura: sorveglianza integrata dei fondali critici con sensoristica distribuita e fusione dei dati alleati, un meccanismo permanente di risposta agli incidenti, e, snodo decisivo, una flotta europea di navi posacavi e riparacavi costruita nell'arco degli anni Trenta attraverso programmi industriali congiunti, che ha ridotto i tempi di ripristino da settimane a giorni e sottratto la funzione al mercato spot. La deterrenza opera principalmente per rilevamento: la probabilità di attribuzione è divenuta abbastanza alta da rendere il sabotaggio un'opzione costosa, e la minaccia

⁹⁷ Sulla tradizione della *prospective* e sull'orientamento anticipazione-azione dello strategic foresight: Coates, J., Durance, P., Godet, M., "Strategic Foresight Issue: Introduction", *Technological Forecasting and Social Change*, 77(9), 2010

deliberata si è spostata verso il dominio cibernetico, dove l'attribuzione resta più sfumata.

In questo futuro l'Italia ha capitalizzato la propria geografia: i porti e i cantieri nazionali ospitano una quota della flotta europea, la Marina esercita il ruolo di presidio del quadrante mediterraneo che la legge 9/2026 aveva prefigurato, e l'hub dei cavi si è consolidato perché la sicurezza percepita del corridoio italiano è divenuta un vantaggio competitivo rispetto alle rotte alternative. Il rischio dominante, paradossalmente, torna a essere quello accidentale della categoria A (ancore e reti), insieme a un rischio più sottile: l'assuefazione. Un sistema che funziona genera la tentazione di definanziarlo. Un ulteriore consolidamento della tenuta di questo sistema potrebbe arrivare anche da investimenti in ambito infrastrutturale che vadano ad aumentare la ridondanza dell'infrastruttura complessiva.

Indicatori di avvicinamento: varo dei programmi europei congiunti per unità posacavi/riparacavi e partecipazione italiana; crescita del tasso di attribuzione pubblica degli incidenti; riduzione tendenziale dei tempi medi di riparazione nel Mediterraneo; regimi di controllo delle esportazioni estesi ai sistemi autonomi subacquei ed effettivamente applicati.

6.3.2 Secondo scenario - La deterrenza sommersa

Proliferazione diffusa, sistema euro-atlantico coeso e capace.

È il futuro della vigilanza armata. La democratizzazione tecnologica si è compiuta: sistemi autonomi a lungo raggio sono nella disponibilità di numerose marine, di attori per procura e di organizzazioni non statuali, e gli incidenti in zona grigia sono divenuti una costante a bassa intensità. Ma il sistema alleato ha retto e si è irrobustito proprio sotto pressione, come già accadde nel Baltico a metà degli anni Venti: la sorveglianza è capillare, la risposta rapida, la ridondanza pianificata. Ne risulta un equilibrio dinamico e costoso delineato da una competizione permanente tra misure e contromisure sul fondale, analoga per logica alla corsa cyber. Un futuro quindi in cui gli attacchi riusciti non scompaiono, ma restano sotto la soglia sistemica perché il ripristino è veloce e la ridondanza assorbe.

Per l'Italia è il futuro della prima linea: la centralità mediterranea, altrove vantaggio, qui significa esposizione massima al traffico di sistemi ostili diretti verso le strozzature di Sicilia e Otranto, dove il nuovo carico infrastrutturale della transizione energetica concentra bersagli e attenzione avversaria. La Marina opera a ritmi operativi elevati e permanenti; la spesa per la protezione subacquea diventa una voce strutturale e crescente del bilancio della difesa; la selezione delle infrastrutture realmente prioritarie evidenziata dalla gerarchizzazione proposta nel capitolo 1, smette di essere un esercizio analitico e diventa una necessità operativa quotidiana, perché non tutto è difendibile contemporaneamente. Al tempo stesso, in questo futuro, la centralità italiana per gli alleati aumenta e il Paese potrebbe andare a ricoprire un ruolo di leadership nella gestione della dimensione subacquea.

Indicatori di avvicinamento: comparsa di sistemi autonomi subacquei a lungo raggio nei cataloghi di esportazione di produttori di seconda fascia; primi incidenti attribuiti ad attori non statuali o per procura; incremento della frequenza di incidenti "sotto

soglia" a fronte di tempi di riparazione stabili; istituzionalizzazione di operazioni alleate permanenti di pattugliamento dei fondali nel Mediterraneo.

6.3.3 Terzo scenario - La quiete fragile

Proliferazione diffusa, sistema euro-atlantico frammentato.

È il futuro peggiore, e va descritto senza indulgere alla distopia proprio perché la sua funzione è disciplinante. La minaccia si è democratizzata e la risposta si è frammentata: sul fondale del Mediterraneo operano sistemi autonomi di provenienza plurima e attribuzione pressoché impossibile, il sabotaggio a basso costo è divenuto strumento ordinario di pressione, sia essa statuale, per procura o criminale, e ciascun Paese protegge ciò che può con ciò che ha. Il danno si trasferisce all'economia per via assicurativa e logistica: premi crescenti sugli asset sottomarini, ritardi di ripristino misurabili in mesi per chi non dispone di flotte proprie, ridondanza come privilegio di chi se la può permettere. Le zone d'ombra giuridiche dell'alto mare, che il capitolo 2 ha descritto come vulnerabilità normativa, sono divenute lo spazio operativo standard degli attori ostili.

Per l'Italia è lo scenario della rinazionalizzazione forzata e tardiva. Ci si troverebbe costretti a ricostruire in emergenza, e quindi al costo massimo, capacità di sorveglianza, riparazione e deterrenza che una pianificazione ventinquennale avrebbe potuto sviluppare in modo incrementale. La geografia, che negli scenari cooperativi è una rendita, qui è una condanna: le strozzature di Sicilia e Otranto e la densità infrastrutturale dei mari italiani offrono agli attori ostili il massimo rendimento per unità di sforzo. La gerarchizzazione delle infrastrutture diventa triage.

Indicatori di avvicinamento: combinazione degli indicatori negativi dei due scenari precedenti; comparsa di sabotaggi seriali non attribuiti in bacini diversi dal Baltico; ritiro o ridimensionamento di operatori privati da tratte mediterranee giudicate non assicurabili; primi casi di negazione di servizio infrastrutturale usati esplicitamente come leva negoziale.

6.3.4 Quarto scenario - L'abisso conteso

Proliferazione contenuta, sistema euro-atlantico frammentato.

È il futuro ingannevole, e per questo forse il più insidioso. La minaccia non si è democratizzata: la capacità di agire in profondità resta concentrata in poche mani statuali. Ma la costruzione euro-atlantica si è arenata e la protezione delle infrastrutture è regredita a mosaico di iniziative nazionali, mentre la funzione industriale di posa e riparazione si è concentrata quasi interamente in operatori privati extraeuropei e negli hyperscaler, che garantiscono ai propri sistemi livelli di ridondanza e capacità di ripristino precluse alle infrastrutture pubbliche o minori. La sicurezza apparente è alta perché gli incidenti deliberati sono rari; la sicurezza reale è bassa, perché i pochi attori capaci conservano un potere di ricatto intatto e selettivo, esercitabile nel momento di massima leva e il pre-posizionamento documentato nel capitolo 3 suggerisce che la preparazione di quel momento avverrebbe in silenzio, anni prima.

L'Italia, in questo futuro, ha esternalizzato senza averlo mai deciso: la connettività nazionale dipende dalla pianificazione commerciale di soggetti privati che negoziano da pari a pari con gli Stati; la capacità di riparazione si compra sul mercato, con tempi e priorità dettati da altri; la Marina mantiene competenze di eccellenza ma su scala insufficiente, e la legge 9/2026 resta un'architettura giuridica cui non corrispondono mezzi. È lo scenario della vulnerabilità dormiente: nulla accade, finché tutto accade insieme.

Indicatori di avvicinamento: mancato rinnovo o svuotamento progressivo dei formati NATO/UE dedicati; quota crescente di nuovi sistemi di cavi mediterranei interamente privati e privi di partecipazione europea; allungamento dei tempi medi di riparazione per le infrastrutture non-hyperscaler; declino degli investimenti nazionali in capacità subacquee a valle di anni senza incidenti maggiori.

6.4 Ciò che gli scenari insegnano: misure robuste e misure contingenti

Il valore dell'esercizio non sta nelle narrative, ma in ciò che permette di distinguere. Sottoponendo le linee di risposta emerse nei capitoli precedenti alla prova dei quattro futuri, alcune misure risultano robuste e necessarie in tutti gli scenari, mentre altre rimangono contingenti, il cui rendimento dipende dal futuro che si materializzerà.

Sono robuste, in primo luogo, quattro linee d'azione. La capacità nazionale di sorveglianza e conoscenza situazionale dei fondali: serve nello scenario cooperativo come contributo al sistema alleato, in quello competitivo come strumento di prima linea, in quelli frammentati come presidio minimo di sovranità e alimenta in ogni caso l'attribuzione, preconditione di qualunque risposta. In secondo luogo, la piena attuazione dell'architettura della legge 9/2026, che in tre scenari su quattro fa la differenza tra una postura e un organigramma. In terzo luogo, il presidio del collo di bottiglia industriale posa e riparazione: è la variabile che più nettamente separa i futuri sostenibili da quelli subiti, e ogni sua declinazione (partecipazione a programmi europei, incentivo alla capacità nazionale, accordi di priorità con gli operatori) produce valore in tutti i quadranti. In quarto luogo, la gerarchizzazione delle infrastrutture avviata nel capitolo 1: negli scenari benigni orienta gli investimenti, in quelli maligni è lo strumento del triage.

Sono invece contingenti, e vanno quindi accompagnate da indicatori più che da impegni irreversibili: il dimensionamento della componente di risposta rapida (cruciale nella *Deterrenza sommersa*, sovradimensionato nel *Fondale presidiato*); il grado di affidamento sui meccanismi collettivi (razionale nei quadranti coesi, rischioso in quelli frammentati, dove va bilanciato da capacità minime autonome); la scommessa sull'hub dei cavi come vettore di crescita, che rende molto nei futuri ordinati e aumenta l'esposizione in quelli contesi.

Ne discende l'ultima indicazione, di metodo più che di merito: questo capitolo non è un punto d'arrivo ma un dispositivo di monitoraggio. Gli indicatori associati a ciascuno scenario andrebbero riletti con cadenza periodica con la revisione biennale che appare proporzionata alla velocità della dimensione, aggiornando le narrative quando i segnali si accumulano, secondo la logica di monitoraggio e aggiornamento continuo che la letteratura metodologica considera parte integrante, e non accessoria, dell'analisi di scenario. Al 2050 non arriverà lo scenario che oggi giudichiamo più probabile: arriverà quello che avremo saputo, o non saputo, riconoscere mentre prendeva forma.