



I cavi sottomarini  
e la rilevanza  
strategica delle  
infrastrutture  
critiche di  
connettività



# INDICE

---

**1**

Progetti Italiani

**2**

Cavi e sicurezza fisica

**3**

Cavi e sicurezza cyber

**4**

Tecnologie di punta per la sicurezza

**5**

Piano d'Azione UE per la Sicurezza dei Cavi

# PROGETTI ITALIANI - UNITIRRENO

L'obiettivo di Unitirreno è offrire una nuova **alternativa sicura e a bassa latenza a Marsiglia** come punto di atterraggio per i cavi sottomarini nel Mediterraneo.

L'infrastruttura, lunga circa **890 km**, sarà il primo sistema **Open Cable a 24 coppie di fibre** nel Mediterraneo.

il sistema Unitirreno permetterà:

- ▶ Lo sviluppo **dell'infrastruttura digitale di Genova**, rendendola un hub di atterraggio per **cavi intercontinentali**.
- ▶ Migliorare il **flusso del traffico dati** tra il Mediterraneo e i principali nodi digitali europei.
- ▶ Migliorare la **connettività Nord-Sud in Italia e con la Sardegna**.

 **UNITIRRENO**



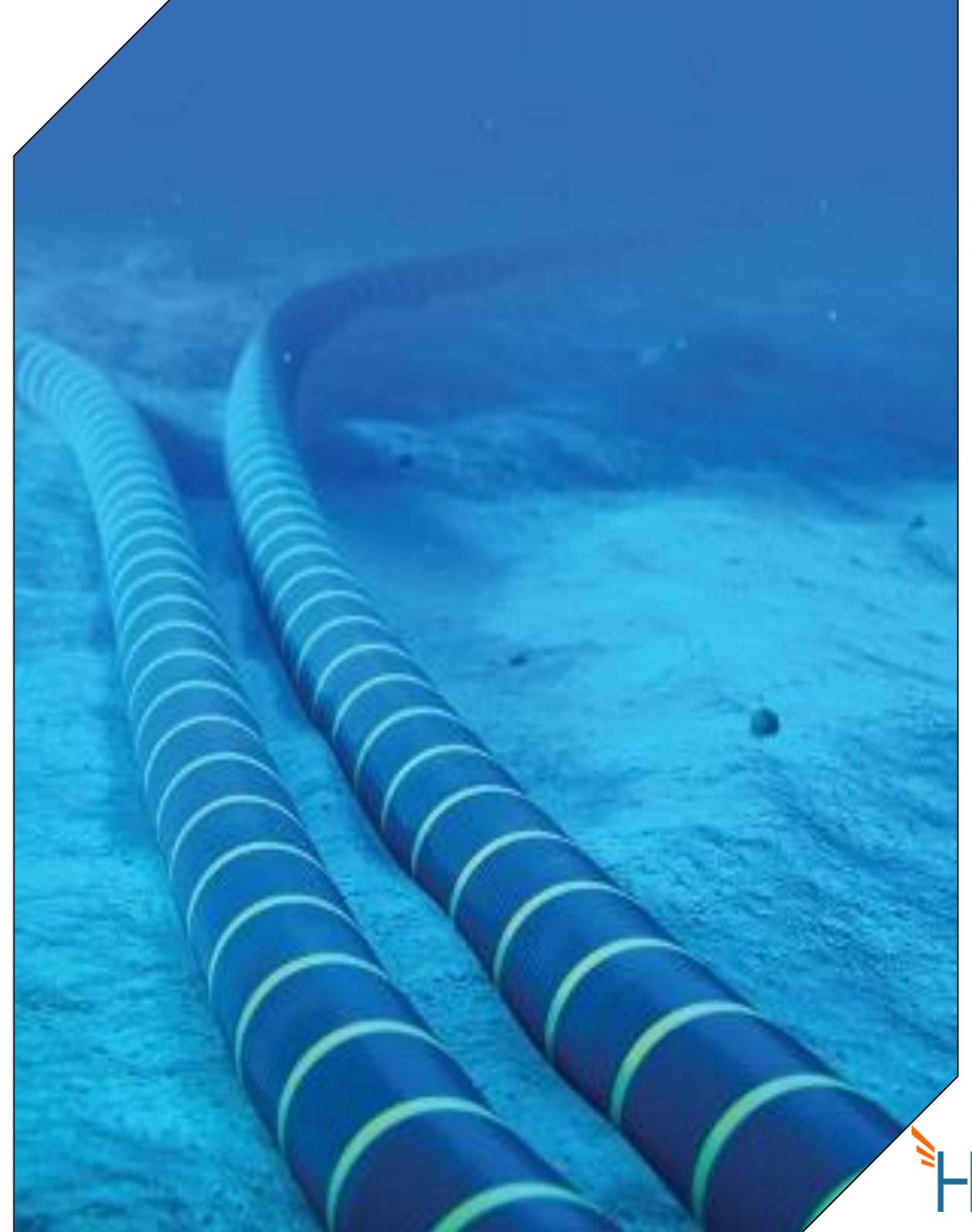
# CAVI E SICUREZZA FISICA (1/2)

Negli ultimi anni queste infrastrutture hanno subito **attacchi significativi**:

## Ottobre 2022:

- ▶ Tre cavi in fibra ottica situati al largo di **Marsiglia** sono stati **danneggiati simultaneamente**. Questi cavi collegavano Marsiglia a **Lione, Milano e Barcellona**.
- ▶ Nello stesso periodo, il cavo sottomarino Shefa-2, utilizzato per le telecomunicazioni tra **le isole Faroe, le Shetland e la Scozia**, è stato tranciato contemporaneamente in due punti distinti.
- ▶ Questo ha provocato **interruzioni significative nelle comunicazioni** e nei servizi pubblici delle aree interessate.

📌 Fonti: ENISA "Threat Landscape for Submarine Cables" (2023) e ICPC Report 2023.



# CAVI E SICUREZZA FISICA (2/2)



## Novembre 2024:

- ▶ Ha smesso di funzionare il cavo che collega l'isola svedese di **Gotland** alla **Lituania**, fondamentale per le **telecomunicazioni tra Scandinavia e Baltico**. Dalle fonti si evince che sono stati danneggiati anche cavi verso **Lettonia** ed **Estonia**.
- ▶ Il giorno successivo, il cavo sottomarino C-Lion1, che collega **Helsinki (Finlandia)** a Rostock (Germania), è stato danneggiato da un "impatto esterno".
- ▶ Grazie a **rotte alternative** non ci sono state interruzioni significative nei servizi.

Per entrambi gli incidenti si sospettano azioni deliberate di **sabotaggio** legato alla guerra ibrida.

# CAVI E SICUREZZA CYBER (1/2)

**2022 - 2024:** Spionaggio cinese sui cavi nel Mediterraneo

- ▶ Il gruppo **APT31** ha preso di mira gli operatori dei cavi **MedNautilus (Grecia-Italia)** e **2Africa (Europa-Medio Oriente)**.
- ▶ Sono state sfruttate vulnerabilità nei sistemi SCADA delle stazioni di approdo, tra cui la CVE-2022-3714.
- ▶ L'attacco ha permesso **l'intercettazione di comunicazioni diplomatiche** e il furto di dati sensibili dell'Unione Europea.
- ▶ Il monitoraggio delle trasmissioni ha esposto potenziali **falle nei protocolli di sicurezza** delle reti sottomarine.

📌 Fonti: Indagini di SentinelOne e rapporti dell'Agencia per la Cybersicurezza Nazionale (2024).



# CAVI E SICUREZZA CYBER (2/2)



**2023** - Cyber-spionaggio russo ai cavi del Baltico

- ▶ Il Gruppo **Callisto (APT29)** ha preso di mira gli operatori dei cavi **Baltic Sea Submarine Cable**, che collegano **Svezia ed Estonia**.
- ▶ Utilizzate tecniche di **spear phishing** contro ingegneri delle telecomunicazioni per ottenere accesso alle reti.
- ▶ Installato il **malware Cannonball** per monitorare i flussi di dati e **intercettare le comunicazioni** trasmesse sui cavi.
- ▶ Gli operatori dei cavi e CERT-EE hanno **identificato e rimosso il malware**, isolando le reti compromesse e bloccando l'accesso russo.
- ▶ Sono state applicate **patch di sicurezza** per prevenire nuovi attacchi.

📌 Fonti: Rapporto congiunto di CERT-EE (Estonia) e VigiCypher (Francia).

# DRONI AUV

Gli AUV (**Autonomous Underwater Vehicles**) sono veicoli sottomarini autonomi utilizzati per l'ispezione, la sorveglianza e la manutenzione di infrastrutture subacquee.

- ▶ Sono dotati di **sonar, telecamere HD e sensori avanzati**.
- ▶ Possono operare a **grandi profondità senza equipaggio**.

Terna, nel progetto **Odisseo**, utilizza il drone GAVIA (in basso) per **l'ispezione degli elettrodotti sottomarini**, raccogliendo dati dettagliati sul fondale e permettendo di valutare l'integrità delle infrastrutture e prevenire guasti.

Le stesse tecnologie possono essere impiegate per proteggere i cavi sottomarini delle telecomunicazioni. Gli AUV potrebbero **rilevare tentativi di sabotaggio**, spostamenti del fondale o deterioramenti del cavo, garantendo una **sorveglianza continua** e una **risposta rapida** a eventuali minacce.

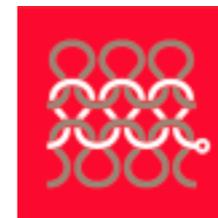
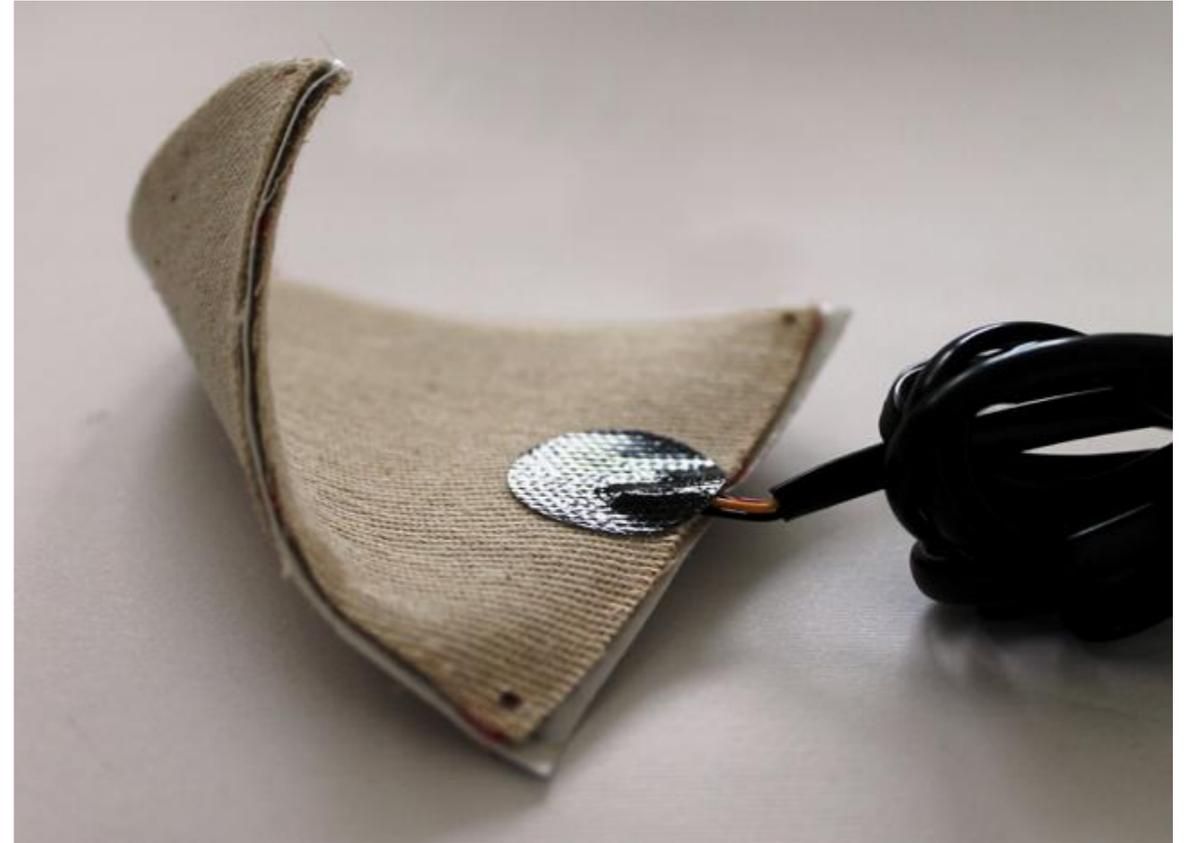


# SMART TEXTILE

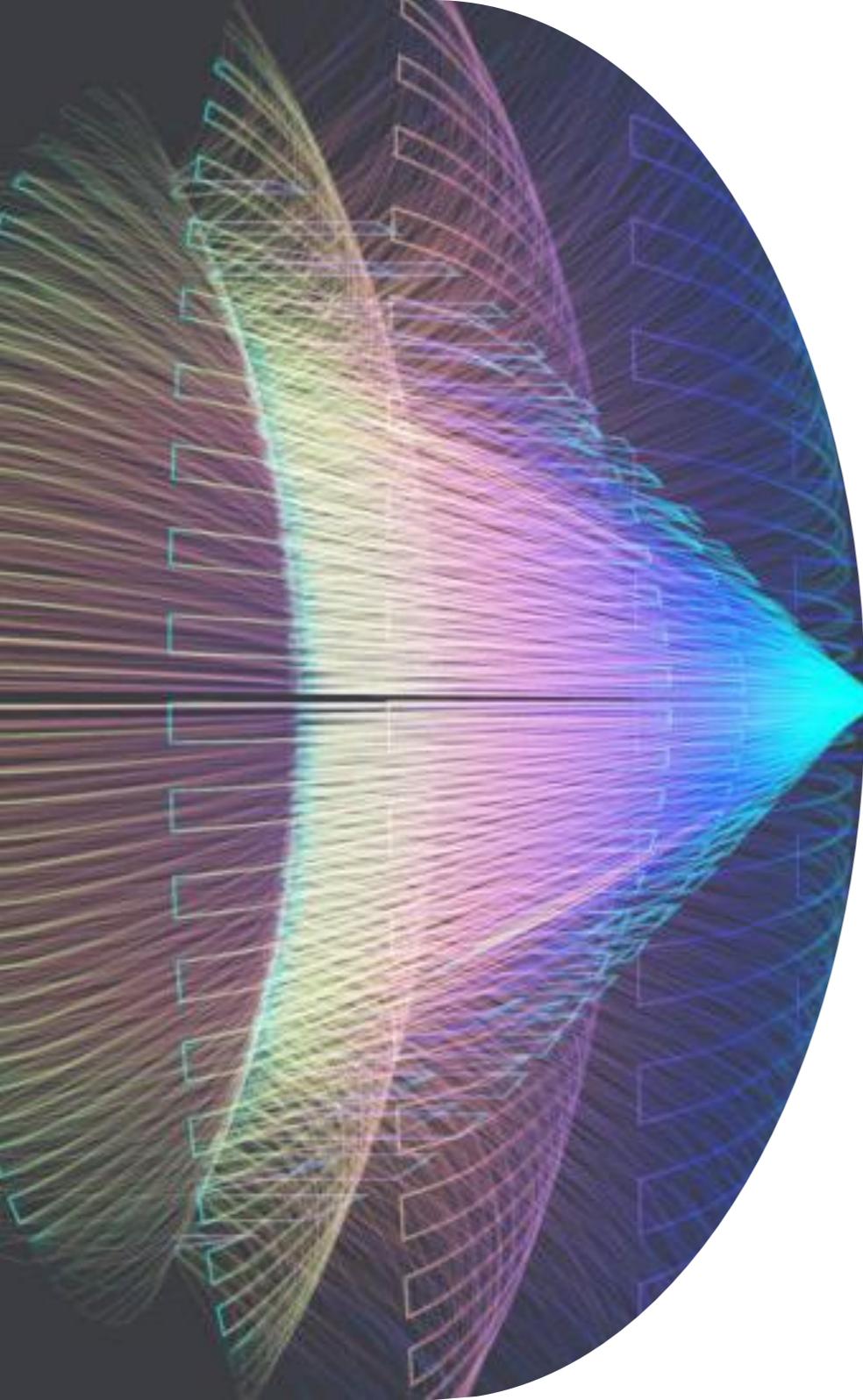
Knitronix ha sviluppato un **tessuto intelligente** in grado di comportarsi come un “**sensore continuo**”.

Questo smart textile, già sperimentato in altri tipi di tubazioni e condotte, può avvolgere l'infrastruttura sottomarina consentendo di **rilevare alterazioni o manomissioni** su tutta la sua lunghezza in tempo reale.

Il tessuto intelligente rileva **cambiamenti di pressione, vibrazioni e variazioni termiche**, segnalando immediatamente anomalie.



**Knitronix**  
industrial flexible sensors



# COMUNICAZIONI QUANTISTICHE

Le comunicazioni quantistiche sfruttano le leggi della meccanica quantistica per trasmettere informazioni in modo impossibile da intercettare.

Il metodo più avanzato è la **Distribuzione a Chiave Quantistica (QKD)**, che utilizza fotoni per generare chiavi crittografiche uniche.

Se un hacker tenta di intercettare la chiave, il sistema lo rileva immediatamente perché la misura altera lo stato dei fotoni.

- ▶ Progetti come **EuroQCI** e sperimentazioni in Italia (es. Porto di Trieste) stanno **integrando QKD nei cavi in fibra ottica** per proteggere trasmissioni sensibili.
- ▶ **Telsy** ha testato la QKD su reti di fibra ottica terrestre e sottomarina, dimostrando la possibilità di applicarla su grandi distanze.

# AI MONITORING

Le reti di cavi sottomarini più avanzate stanno integrando **sistemi di monitoraggio basati su AI**, che permettono la rilevazione immediata di anomalie nel traffico dati e nelle condizioni fisiche dei cavi sottomarini.

Questi sistemi analizzano continuamente i dati in arrivo dai **sensori ottici, vibrazionali e termici**, rilevando attività sospette e **attivando protocolli di risposta automatizzata**.

Le stesse tecnologie possono essere impiegate per **identificare intrusioni informatiche** e bloccare tentativi di accesso non autorizzati.

- ▶ Progetti come **SMART Cable** nel Mar Ionio stanno sviluppando prototipi di cavi sottomarini multifunzionali che prevedono l'utilizzo di questa tecnologia.





# AZIONI CHIAVE: PREVENZIONE

## Commissione Europea:

- ▶ **Mappatura** delle infrastrutture di cavi sottomarini esistenti e pianificate.
- ▶ **Valutazione coordinata dei rischi**, delle vulnerabilità e delle dipendenze.
- ▶ "**Cable Security Toolbox**", un insieme di misure di mitigazione per la sicurezza dei cavi.
- ▶ Lista prioritaria dei Progetti di Interesse Europeo (**CPEIs**) nel settore dei cavi sottomarini.
- ▶ Revisione del quadro normativo sulla **sicurezza dell'approvvigionamento energetico**.
- ▶ Facilitare investimenti e migliorare la sicurezza dei cavi elettrici attraverso **l'European Grids Package**.

## Stati Membri:

- ▶ Devono recepire e attuare urgentemente le direttive **CER** e **NIS2**.
- ▶ Sono incoraggiati a **garantire che tutti gli operatori** di infrastrutture di comunicazione sottomarine **rientrano nella legislazione nazionale che recepisce la direttiva NIS2**.
- ▶ Dovrebbero considerare attentamente le **entità che forniscono servizi essenziali** per le comunicazioni elettroniche sottomarine e la trasmissione di energia elettrica nell'attuazione della direttiva CER, in particolare per **la strategia, la valutazione dei rischi e l'identificazione delle entità critiche**.
- ▶ Devono garantire che i cavi elettrici siano progettati e installati in modo da **massimizzare la sicurezza**.

# AZIONI CHIAVE: RILEVAZIONE

## Commissione Europea e Stati Membri:

- ▶ Sosterranno lo sviluppo e l'implementazione, su base volontaria, di un **Meccanismo Integrato di Sorveglianza** per i cavi sottomarini per ciascun bacino marittimo. Questo sistema collegherà e integrerà dati provenienti da diverse fonti per creare un quadro situazionale marittimo preciso e in tempo reale.
- ▶ Lanceranno un **hub regionale dedicato nel Mar Baltico**, che fungerà da piattaforma di test per l'approccio di sorveglianza integrata.
- ▶ Esploreranno la possibilità di creare una **rete di sensori subacquei** dedicati alla protezione dei cavi sottomarini.
- ▶ Avvieranno un programma specifico per **droni di sorveglianza** (aerei, di superficie e subacquei) per potenziare la capacità di monitoraggio e sicurezza delle infrastrutture sottomarine.
- ▶ Prepareranno un rapporto tecnico per promuovere l'**adozione di nuove tecnologie** per la rilevazione e la prevenzione di incidenti sui cavi.
- ▶ Favoriranno la **collaborazione pubblico-privato** con gli operatori di cavi, incentivando un **sistema volontario di segnalazione tempestiva** degli incidenti che coinvolgono le infrastrutture sottomarine.

# AZIONI CHIAVE: RISPOSTA E RECOVERY

## Commissione Europea e Stati Membri:

- ▶ **Miglioreranno l'efficacia della risposta alle crisi** rafforzando le sinergie tra i quadri normativi esistenti e valutando, insieme agli Stati membri, la necessità di un approccio più specifico per la protezione dei cavi sottomarini.
- ▶ **Ottimizzeranno l'uso dei fondi dell'UE**, consentendo trasferimenti volontari dagli **Fondi di Coesione** al **Connecting Europe Facility (CEF)** per finanziare l'aumento della capacità delle **navi per la riparazione dei cavi** e l'acquisto di attrezzature modulari di riparazione.
- ▶ **Proporranno la creazione di una flotta di riserva UE per la riparazione dei cavi**, operativa su richiesta, attraverso un **Atto di Esecuzione** nell'ambito del **Meccanismo di Protezione Civile dell'UE (rescEU)**. Questa iniziativa potrebbe essere integrata da accordi regionali per garantire la disponibilità immediata di navi specializzate con equipaggi esperti.
- ▶ **Svilupperanno un piano congiunto per garantire la sicurezza dell'approvvigionamento dei componenti di ricambio**, creando scorte strategiche mirate.

## Commissione Europea e Alto Rappresentante:

- ▶ **Rafforzeranno la cooperazione operativa con la NATO** per migliorare la resilienza e la protezione delle infrastrutture critiche sottomarine, inclusi i cavi di comunicazione e di energia.

# AZIONI CHIAVE: DETERRENZA

## Commissione Europea, Alto Rappresentate e Stati Membri:

- ▶ **Avvieranno una diplomazia proattiva sui cavi**, coinvolgendo partner strategici e organismi multilaterali per rafforzare la cooperazione sulla sicurezza delle infrastrutture sottomarine.
- ▶ **Potenzieranno le capacità dell'UE per contrastare e ridurre l'impatto della "flotta ombra"**, spesso utilizzata per operazioni clandestine contro le infrastrutture critiche.
- ▶ **Rafforzeranno i meccanismi di attribuzione e sanzione**, sfruttando al massimo i regimi sanzionatori esistenti per individuare e perseguire gli attori responsabili di attacchi ai cavi sottomarini.
- ▶ **Miglioreranno la comunicazione strategica** per contrastare le campagne ibride che sfruttano la plausibile negabilità (plausible deniability) come strumento di disinformazione.
- ▶ **Promuoveranno una discussione internazionale** su come utilizzare appieno il **Diritto del Mare** per migliorare la protezione dei cavi sottomarini.
- ▶ **Intensificheranno il dialogo e la cooperazione con la NATO** per integrare la sicurezza dei cavi nelle strategie di difesa collettiva.

Dott. Ing. Luisa Franchina, PhD  
l.franchina@hermesbay.com

# Contatti

## Hermes Bay S.r.l.

 Via Nazionale 214, 00184 Roma

 Tel. 06 98795241

 [www.hermesbay.com](http://www.hermesbay.com)

 [l.franchina@hermesbay.com](mailto:l.franchina@hermesbay.com)

