Se i cavi sottomarini nel Mar Rosso venissero tagliati: quanto è fragile internet?

Maria Cattini | 18/03/2026 | Sicurezza digitale

Non è fantascienza. È già successo — e potrebbe andare molto peggio. Il 6 settembre 2025, diversi cavi in fibra ottica sul fondo del Mar Rosso vengono recisi. India, Pakistan, Arabia Saudita, Emirati Arabi Uniti, Kuwait: milioni di utenti si ritrovano con connessioni a singhiozzo, banche in difficoltà, aziende costrette a rerouting di emergenza. Microsoft segnala ufficialmente un picco di latenza su Azure per Europa e Asia. Non è un attacco nucleare. È un danno ai cavi — e basta.

Ora immagina lo scenario con lo Stretto di Hormuz chiuso e la zona militarizzata.

Il nervo digitale del pianeta passa qui

Sotto il Mar Rosso e il Golfo Persico scorrono alcuni dei cavi più critici del mondo. Secondo il Comitato Internazionale per la Protezione dei Cavi, esistono circa 1,7 milioni di chilometri di infrastrutture sottomarine globali. Di questi, i corridoi Mar Rosso–Golfo Persico trasportano **oltre il 20% del traffico internet mondiale** e fino al 95% del traffico dati tra Asia ed Europa.

Google, Meta, Amazon e Microsoft hanno investito miliardi in questi cavi — e oggi li stanno guardando con crescente preoccupazione. A novembre 2025, Meta e Google hanno rallentato i lavori sui loro mega-progetti "2Africa" e "Blue-Raman": troppi rischi per le navi da cantiere nell'area. Non è una scelta economica. È una valutazione di sicurezza.

Cosa succederebbe davvero

Nessuno ha interesse a descrivere un'apocalisse digitale: la realtà è più complessa — e per certi versi più preoccupante — di uno scenario da film.

I danni sarebbero gravi, non totali. Gli episodi del 2024 e 2025 lo confermano: il traffico si rerouta, ma a costi enormi. Le rotte alternative — via Capo di Buona Speranza o via cavi transatlantici — costano **fino a sei volte di più** e aggiungono latenza significativa. I Paesi più esposti, come India, Pakistan e Africa orientale, subirebbero i contraccolpi peggiori proprio perché dipendono da quella rotta in modo quasi esclusivo.

I tempi di riparazione sono il vero problema. Una nave specializzata per riparare un singolo cavo sottomarino impiega settimane in condizioni normali. Nella crisi del 2024, con gli Houthi che controllavano di fatto le acque, ci sono voluti quasi **sei mesi** per un singolo intervento. In un conflitto aperto come quello che si sta delineando allo Stretto di Hormuz da marzo 2026, quelle navi semplicemente non possono avvicinarsi. Si parla di 6-12 mesi di servizio degradato per ogni cavo colpito.

I mercati finanziari sentirebbero l'impatto, ma non collasserebbero. SWIFT e i sistemi di pagamento internazionale dispongono di ridondanze geografiche studiate per scenari estremi. Rallentamenti e disfunzioni ci sarebbero — lo streaming, il cloud real-time e il trading ad alta frequenza sarebbero i settori più colpiti — ma un blackout totale dei pagamenti globali resta uno scenario ipotetico.

La minaccia ibrida: Hormuz non è solo petrolio

Lo Stretto di Hormuz ha sempre evocato una sola parola: petrolio. Da qui transita il **20% del greggio mondiale e il 25% del gas liquefatto**. Ma da anni il corridoio è anche un nodo digitale critico, e Teheran lo sa.

A marzo 2026, l'Iran ha intensificato gli attacchi a navi nel Golfo Persico con piccole imbarcazioni veloci, droni e — dettaglio spesso trascurato — **GPS jamming**. Le interferenze elettroniche non colpiscono solo le rotte commerciali: disorientano le navi da riparazione, complicano le operazioni di sorveglianza sottomarina, allargano la finestra di vulnerabilità delle infrastrutture digitali.

Non serve un'operazione militare su vasta scala per danneggiare un cavo sottomarino. Come dimostra il caso della nave *Rubymar* nel 2024, un'imbarcazione alla deriva con l'ancora abbassata ha distrutto sezioni di cavo per decine di chilometri. La guerra ibrida ha trovato il suo bersaglio ideale: invisibile, difficile da difendere, lento da riparare.

L'Europa si sveglia (in ritardo)

A febbraio 2026, la Commissione Europea ha pubblicato la Submarine Cable Security Toolbox e stanziato **347 milioni di euro** per rafforzare la protezione delle infrastrutture. Il piano prevede quattro assi: prevenzione, rilevamento, risposta rapida e deterrenza diplomatica. Tra le misure concrete: una flotta europea di navi da riparazione di riserva — la cosiddetta *EU Cable Vessels Reserve Fleet* — per abbattere i tempi di intervento.

È un segnale positivo. Ma arriva dopo che gli episodi del 2024 e 2025 hanno già dimostrato quanto ci si fosse mossi tardi. Gli Stati del Baltico, a gennaio 2026, sono entrati in stato di allerta elevata dopo una serie di danni sospetti ai cavi del Mar Baltico. Il pattern si ripete: prima il danno, poi la risposta.

Il rischio che nessuno vuole calcolare

La vera domanda non è "se" un attacco ai cavi avverrà, ma **quanto costerebbe non avere un piano B**. Con 150-200 incidenti ai cavi sottomarini ogni anno nel mondo — la maggior parte accidentali, ma una quota crescente sospetta — e con la geopolitica di Hormuz che nel marzo 2026 ha raggiunto livelli di tensione inediti, il corridoio digitale del Mar Rosso è diventato uno dei punti più

vulnerabili dell'infrastruttura globale.

I cavi sottomarini trasportano il 97% del traffico internet del pianeta. Sono protetti da normative internazionali risalenti al 1884. Sono sorvegliati — dove va bene — da qualche pattuglia navale. E riposano sul fondo del mare, invisibili, a portata di ancora.

Vuoi testare la resilienza della tua infrastruttura digitale in uno scenario di crisi? La *Submarine Cable Security Toolbox* dell'UE è pubblica e scaricabile: è un buon punto di partenza per capire quanto siamo davvero preparati.

Se ti interessano strumenti di **AI, OSINT e ricerca digitale**, entra nella community:

Newsletter
https://coondivido.substack.com/

Telegram
https://t.me/osintaipertutti
https://t.me/osintprojectgroup

https://coondivido.it/monitorare-stretto-hormuz-osint/
Non è fantascienza. È già successo — e potrebbe andare molto peggio. Il 6 settembre 2025, diversi cavi in fibra ottica sul fondo del Mar Rosso vengono recisi. India, Pakistan, Arabia Saudita, Emirati Arabi Uniti, Kuwait: milioni di utenti si ritrovano con connessioni a singhiozzo, banche in difficoltà, aziende costrette a rerouting di emergenza. Microsoft segnala ufficialmente un picco di latenza su Azure per Europa e Asia. Non è un attacco nucleare. È un danno ai cavi — e basta.

Ora immagina lo scenario con lo Stretto di Hormuz chiuso e la zona militarizzata.

Il nervo digitale del pianeta passa qui

Sotto il Mar Rosso e il Golfo Persico scorrono alcuni dei cavi più critici del mondo. Secondo il Comitato Internazionale per la Protezione dei Cavi, esistono circa 1,7 milioni di chilometri di infrastrutture sottomarine globali. Di questi, i corridoi Mar Rosso–Golfo Persico trasportano **oltre il 20% del traffico internet mondiale** e fino al 95% del traffico dati tra Asia ed Europa.

Google, Meta, Amazon e Microsoft hanno investito miliardi in questi cavi — e oggi li stanno guardando con crescente preoccupazione. A novembre 2025, Meta e Google hanno rallentato i lavori sui loro mega-progetti "2Africa" e "Blue-Raman": troppi rischi per le navi da cantiere nell'area. Non è una scelta economica. È una valutazione di sicurezza.

Cosa succederebbe davvero

Nessuno ha interesse a descrivere un'apocalisse digitale: la realtà è più complessa — e per certi versi più preoccupante — di uno scenario da film.

I danni sarebbero gravi, non totali. Gli episodi del 2024 e 2025 lo confermano: il traffico si rerouta, ma a costi enormi. Le rotte alternative — via Capo di Buona Speranza o via cavi transatlantici — costano **fino a sei volte di più** e aggiungono latenza significativa. I Paesi più esposti, come India, Pakistan e Africa orientale, subirebbero i contraccolpi peggiori proprio perché dipendono da quella rotta in modo quasi esclusivo.

I tempi di riparazione sono il vero problema. Una nave specializzata per riparare un singolo cavo sottomarino impiega settimane in condizioni normali. Nella crisi del 2024, con gli Houthi che controllavano di fatto le acque, ci sono voluti quasi **sei mesi** per un singolo intervento. In un conflitto aperto come quello che si sta delineando allo Stretto di Hormuz da marzo 2026, quelle navi semplicemente non possono avvicinarsi. Si parla di 6-12 mesi di servizio degradato per ogni cavo colpito.

I mercati finanziari sentirebbero l'impatto, ma non collasserebbero. SWIFT e i sistemi di pagamento internazionale dispongono di ridondanze geografiche studiate per scenari estremi. Rallentamenti e disfunzioni ci sarebbero — lo streaming, il cloud real-time e il trading ad alta frequenza sarebbero i settori più colpiti — ma un blackout totale dei pagamenti globali resta uno scenario ipotetico.

La minaccia ibrida: Hormuz non è solo petrolio

Lo Stretto di Hormuz ha sempre evocato una sola parola: petrolio. Da qui transita il **20% del greggio mondiale e il 25% del gas liquefatto**. Ma da anni il corridoio è anche un nodo digitale critico, e Teheran lo sa.

A marzo 2026, l'Iran ha intensificato gli attacchi a navi nel Golfo Persico con piccole imbarcazioni veloci, droni e — dettaglio spesso trascurato — **GPS jamming**. Le interferenze elettroniche non colpiscono solo le rotte commerciali: disorientano le navi da riparazione, complicano le operazioni di sorveglianza sottomarina, allargano la finestra di vulnerabilità delle infrastrutture digitali.

Non serve un'operazione militare su vasta scala per danneggiare un cavo sottomarino. Come dimostra il caso della nave *Rubymar* nel 2024, un'imbarcazione alla deriva con l'ancora abbassata ha distrutto sezioni di cavo per decine di chilometri. La guerra ibrida ha trovato il suo bersaglio ideale: invisibile, difficile da difendere, lento da riparare.

L'Europa si sveglia (in ritardo)

A febbraio 2026, la Commissione Europea ha pubblicato la Submarine Cable Security Toolbox e stanziato **347 milioni di euro** per rafforzare la protezione delle infrastrutture. Il piano prevede quattro assi: prevenzione, rilevamento, risposta rapida e deterrenza diplomatica. Tra le misure concrete: una flotta europea di navi da riparazione di riserva — la cosiddetta *EU Cable Vessels Reserve Fleet* — per abbattere i tempi di intervento.

È un segnale positivo. Ma arriva dopo che gli episodi del 2024 e 2025 hanno già dimostrato quanto ci si fosse mossi tardi. Gli Stati del Baltico, a gennaio 2026, sono entrati in stato di allerta elevata dopo una serie di danni sospetti ai cavi del Mar Baltico. Il pattern si ripete: prima il danno, poi la risposta.

Il rischio che nessuno vuole calcolare

La vera domanda non è "se" un attacco ai cavi avverrà, ma **quanto costerebbe non avere un piano B**. Con 150-200 incidenti ai cavi sottomarini ogni anno nel mondo — la maggior parte accidentali, ma una quota crescente sospetta — e con la geopolitica di Hormuz che nel marzo 2026 ha raggiunto livelli di tensione inediti, il corridoio digitale del Mar Rosso è diventato uno dei punti più vulnerabili dell'infrastruttura globale.

I cavi sottomarini trasportano il 97% del traffico internet del pianeta. Sono protetti da normative internazionali risalenti al 1884. Sono sorvegliati — dove va bene — da qualche pattuglia navale. E riposano sul fondo del mare, invisibili, a portata di ancora.

Vuoi testare la resilienza della tua infrastruttura digitale in uno scenario di crisi? La *Submarine Cable Security Toolbox* dell'UE è pubblica e scaricabile: è un buon punto di partenza per capire quanto siamo davvero preparati.

Se ti interessano strumenti di **AI, OSINT e ricerca digitale**, entra nella community:

Newsletter
https://coondivido.substack.com/

Telegram
https://t.me/osintaipertutti
https://t.me/osintprojectgroup

https://coondivido.it/monitorare-stretto-hormuz-osint/