Dallo Stretto di Hormuz ai fondali oceanici: quando la guerra smette di essere visibile e diventa sistemica

Pubblicato il 25/04/2026

Negli ultimi giorni, media legati all'Iran hanno pubblicato una mappa dettagliata dei cavi sottomarini che attraversano il Golfo Persico, il Mar Rosso e lo Stretto di Hormuz, portando all'attenzione uno degli elementi meno visibili ma più critici dell'infrastruttura globale, ovvero quella rete fisica che permette il funzionamento stesso di internet e che collega continenti, economie e sistemi finanziari attraverso corridoi sottomarini nei quali transitano quotidianamente enormi volumi di dati, rendendo possibile tutto ciò che oggi consideriamo normale, dalle comunicazioni alle transazioni economiche, fino ai servizi cloud su cui si regge una parte crescente della nostra società.

Un'infrastruttura fisica, localizzabile e strategica

La pubblicazione di questa mappa non introduce nulla di nuovo dal punto di vista tecnico, ma ha il merito di rendere evidente qualcosa che per anni è rimasto fuori dal dibattito pubblico, ovvero

il fatto che questa infrastruttura esiste, è fisica, è localizzabile e, soprattutto, si sviluppa in aree geografiche che non sono neutrali ma caratterizzate da tensioni, interessi strategici e capacità operative che non possono essere ignorate. Proprio per questo motivo, il valore di questa pubblicazione non è tanto informativo quanto comunicativo, perché inserita nel contesto attuale assume il significato di un messaggio indirizzato a un interlocutore ben preciso.

Da Hormuz al dominio digitale

Il contesto è quello di uno scontro sempre più evidente tra Iran e Stati Uniti, incentrato proprio sul controllo dello Stretto di Hormuz, che rappresenta da sempre uno dei principali choke point energetici globali e che negli ultimi mesi è tornato al centro di una dinamica di pressione reciproca fatta di blocchi, minacce e dimostrazioni di forza, con effetti concreti sul traffico commerciale e sugli equilibri economici globali. È proprio all'interno di questo braccio di ferro che la pubblicazione di una mappa apparentemente tecnica assume un significato diverso, perché non si limita a descrivere un'infrastruttura, ma suggerisce implicitamente un'estensione del campo di confronto, spostando l'attenzione da ciò che è sempre stato considerato il cuore del problema — il petrolio — a qualcosa di meno visibile ma potenzialmente altrettanto incisivo, ovvero la connettività digitale.

I nuovi bersagli invisibili

In tutti i conflitti siamo abituati a pensare a bersagli evidenti, conosciuti e spesso alla luce del sole, come basi militari, infrastrutture energetiche, ponti, nodi logistici e tutto ciò che rientra nella percezione classica della guerra e della difesa, ovvero ciò che è visibile, mappabile e difendibile attraverso sistemi tradizionali, uomini, mezzi e tecnologia. Tuttavia, l'evoluzione della nostra società ha progressivamente spostato il baricentro verso obiettivi completamente diversi, meno appariscenti ma non per questo meno critici, creando di fatto una nuova categoria di vulnerabilità che sfugge alla percezione comune ma che rappresenta uno dei veri punti sensibili del sistema.

Le arterie del mondo digitale

Oggi esiste infatti un'infrastruttura che non è protetta da perimetri, non è presidiata da soldati armati fino ai denti, non è coperta da radar o sistemi di difesa avanzati, e che proprio per questo tende a rimanere fuori dall'immaginario collettivo, ma che in realtà costituisce la base su cui poggia tutto il resto. È rappresentata da centinaia di cavi in fibra ottica posati sui fondali

marini, spesso non più spessi di un tubo da giardino, che attraversano gli oceani collegando tra loro i diversi continenti e trasportando la quasi totalità del traffico dati globale, diventando di fatto le vere arterie del mondo digitale.

Una vulnerabilità difficile, ma non impossibile da sfruttare

Queste infrastrutture, proprio per la loro natura, sono difficili da raggiungere per un attore improvvisato, ma non sono affatto impossibili da individuare o da colpire per chi dispone di capacità tecniche e operative adeguate, e soprattutto non sono impossibili da interrompere. Ogni anno, infatti, si registrano numerosi incidenti, spesso causati da attività apparentemente banali come la pesca o l'ancoraggio di navi, che dimostrano quanto sia sottile il margine tra il normale funzionamento del sistema e una sua interruzione.

Il problema dei choke point digitali

Il punto però non è la vulnerabilità in senso assoluto, perché qualsiasi infrastruttura lo è, ma il fatto che questa vulnerabilità sia concentrata e sistemica. La rete globale non è distribuita in modo uniforme, ma tende a convergere in alcuni corridoi geografici obbligati, veri e propri choke point, nei quali più linee si sovrappongono creando una dipendenza strutturale che, in condizioni normali, rappresenta un vantaggio in termini di efficienza, ma che in condizioni di crisi può trasformarsi rapidamente in un fattore di rischio.

La ridondanza non è infinita

Esistono naturalmente meccanismi di ridondanza, e il traffico dati può essere deviato su percorsi alternativi in caso di interruzione di una singola linea, ma questa capacità non è infinita. Soprattutto, funziona realmente solo quando le alternative sono indipendenti tra loro, mentre perde efficacia quando più cavi condividono gli stessi corridoi geografici, perché in quel caso il problema non viene eliminato ma semplicemente distribuito, con effetti che si traducono in rallentamenti, congestioni e, nei casi più gravi, vere e proprie interruzioni regionali dei servizi.

Perché i satelliti non bastano

A questo punto è fondamentale chiarire un aspetto spesso frainteso, ovvero l'idea che esistano sistemi alternativi in grado di sostituire realmente i cavi sottomarini in caso di interruzione. Se è vero che nel dibattito pubblico si tende a pensare ai satelliti come a una possibile rete parallela, la realtà tecnica è molto più netta: questi sistemi rappresentano solo una componente

marginale della connettività globale e non una vera alternativa al backbone fisico, essendo limitati in termini di capacità, latenza e sostenibilità operativa, mentre la quasi totalità del traffico intercontinentale continua a viaggiare attraverso i cavi sottomarini.

Una rete che si appoggia su se stessa

Questo significa che non esiste una vera ridondanza su sistemi completamente differenti, ma piuttosto una rete che si appoggia su se stessa, moltiplicando i percorsi ma mantenendo invariato il principio di base: il traffico passa attraverso cavi fisici, e quando questi vengono meno, ciò che resta non è un sistema alternativo pienamente funzionante, ma una capacità residuale del tutto insufficiente per sostenere il funzionamento normale di economie, mercati finanziari e servizi digitali su larga scala.

La differenza con l’energia

A differenza di quanto avviene nel settore energetico, dove esistono modalità alternative di trasporto — come nel caso del gas che può essere spostato via nave compensando almeno in parte l’interruzione di una pipeline — nel caso della connettività globale questa flessibilità semplicemente non esiste. Internet, nella sua dimensione intercontinentale, non può essere trasferito su un’infrastruttura diversa senza subire un degrado significativo, ed è proprio questa assenza di alternativa reale che trasforma una vulnerabilità tecnica in una dipendenza strategica.

La leva strategica della connettività

Ed è proprio qui che il messaggio iraniano assume il suo significato più profondo. Così come lo Stretto di Hormuz è stato storicamente utilizzato come leva di pressione sul piano energetico, la pubblicazione di questa mappa suggerisce che anche la dimensione digitale può essere trasformata in una leva strategica, non necessariamente attraverso un attacco diretto, ma semplicemente rendendo evidente dove si trovano i punti di pressione, come in una partita di poker in cui mostrare le carte non serve a giocarle immediatamente, ma a cambiare il comportamento dell’avversario.

Il precedente Nord Stream

In questo contesto, il parallelo con il Nord Stream diventa immediato non tanto per una somiglianza diretta tra le due infrastrutture, quanto per il principio che rappresenta: colpire

un’infrastruttura fisica critica, spesso invisibile al grande pubblico, significa intervenire direttamente sul funzionamento della società, creando effetti che vanno ben oltre il danno immediato e che si propagano lungo l’intero sistema.

La zona grigia del degrado

Il vero punto quindi non è immaginare scenari estremi in cui “internet si spegne”, ma comprendere che esiste una zona grigia molto più realistica e, per certi versi, più pericolosa, nella quale l’infrastruttura continua a funzionare ma in modo degradato, creando effetti sistemici difficili da attribuire, da gestire e da contrastare.

La vulnerabilità come vantaggio operativo

La vera domanda, a questo punto, non è se queste infrastrutture siano vulnerabili, perché lo sono per definizione, ma quanto siamo disposti ad accettare questa vulnerabilità come parte del sistema, finché qualcuno non decide di trasformarla in un vantaggio operativo.