LA RETE GLOBALE CORRE SOTT'ACQUA

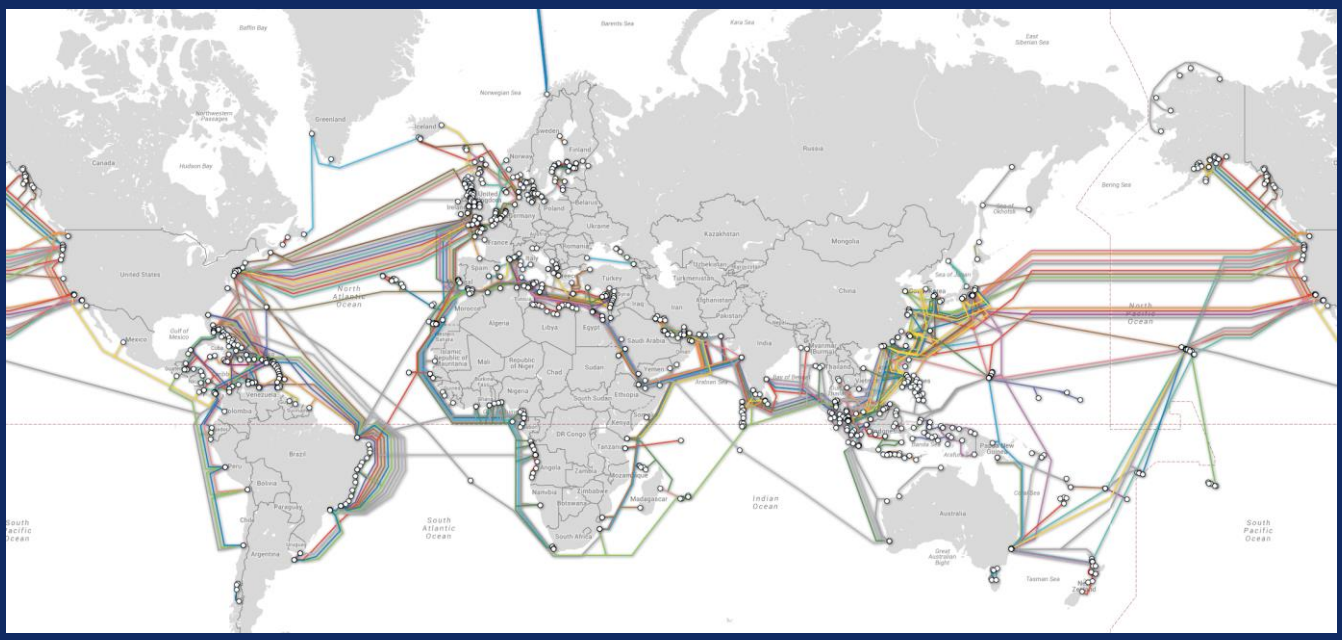
- 12 agosto 2024 -

La comunicazione globale si basa principalmente sui cavi sottomarini in fibra ottica che gestiscono la stragrande maggioranza dei flussi di dati a livello mondiale. Tuttavia, queste infrastrutture sono esposte a minacce come sabotaggi e attacchi esterni, richiedendo misure di sicurezza adeguate. L'Unione Europea ha introdotto la direttiva CER per rafforzare la resilienza delle infrastrutture critiche, ma sono necessari ulteriori sforzi per garantire la sicurezza dei cavi sottomarini e delle stazioni di atterraggio.

In riferimento a Internet, raramente si riflette sul significato intrinseco di "*rete*", ovvero un vasto complesso di linee di comunicazione che si intersecano tra loro. Tutto ciò ha luogo nelle profondità marine, dove è presente una vera e propria rete fisica globale di cavi i quali una volta erano di rame ma oggi, sempre più spesso, di fibra ottica, ovvero filamenti vetrosi e polimerici.
Gli oceani sono letteralmente attraversati da cavi che consentono di collegare i Continenti del mondo. L'umanità intera comunica perché i dati dei nostri pc, tablet

e smartphone, attraversano queste autostrade invisibili che vanno dalle dorsali montuose, al fondo degli oceani.
Quando parliamo della cablatura del mondo parliamo di un business milionario, che vede sempre più aumentare il numero dei player, da quelli tradizionali, vale a dire le ex società statali che un tempo possedevano le reti telefoniche, agli operatori di Tlc privati che dal boom della telefonia mobile degli anni '90 in poi hanno cercato di intercettare la crescente domanda di connessioni sempre più veloci, sicure e stabili.

Uno degli aspetti di maggiore rischio è l'innalzamento dei mari che, unito al riscaldamento globale, porterà, inevitabilmente, al deterioramento della cablatura sottomarina. Stando alle proiezioni sull'innalzamento degli oceani stilate dalla NOAA (National Oceanic and Atmospheric Administration) e di uno studio del 2018 dell'Università americana dell'Oregon, migliaia di chilometri di fibra ottica, posata sul fondale possano venire sommersi dal mare. La preoccupazione maggiore è proprio la tempistica di gestione del rischio: infatti nella ricerca del team del Prof Barford, si afferma che "i primi problemi alle infrastrutture possono sorgere già tra 10 o 15 anni" e, purtroppo, appunto ci siamo quasi.
Il Professore mette sotto accusa chi ha progettato tutte queste infrastrutture fino a oggi, reo di non aver minimamente tenuto in considerazione la variabile climatica come fattore incisivo.



Le comunicazioni globali avvengono principalmente attraverso reti di cavi sottomarini in fibra ottica, che gestiscono tra il 95% e il 99% dei flussi mondiali.
A differenza, i satelliti si occupano solo dall'1% al 5% delle trasmissioni globali, offrendo una qualità inferiore e costi più alti per l'installazione e la manutenzione. Attualmente, non esiste un'alternativa praticabile a queste infrastrutture, poiché la tecnologia satellitare non è in grado di soddisfare efficacemente le crescenti esigenze di comunicazione della società digitale.

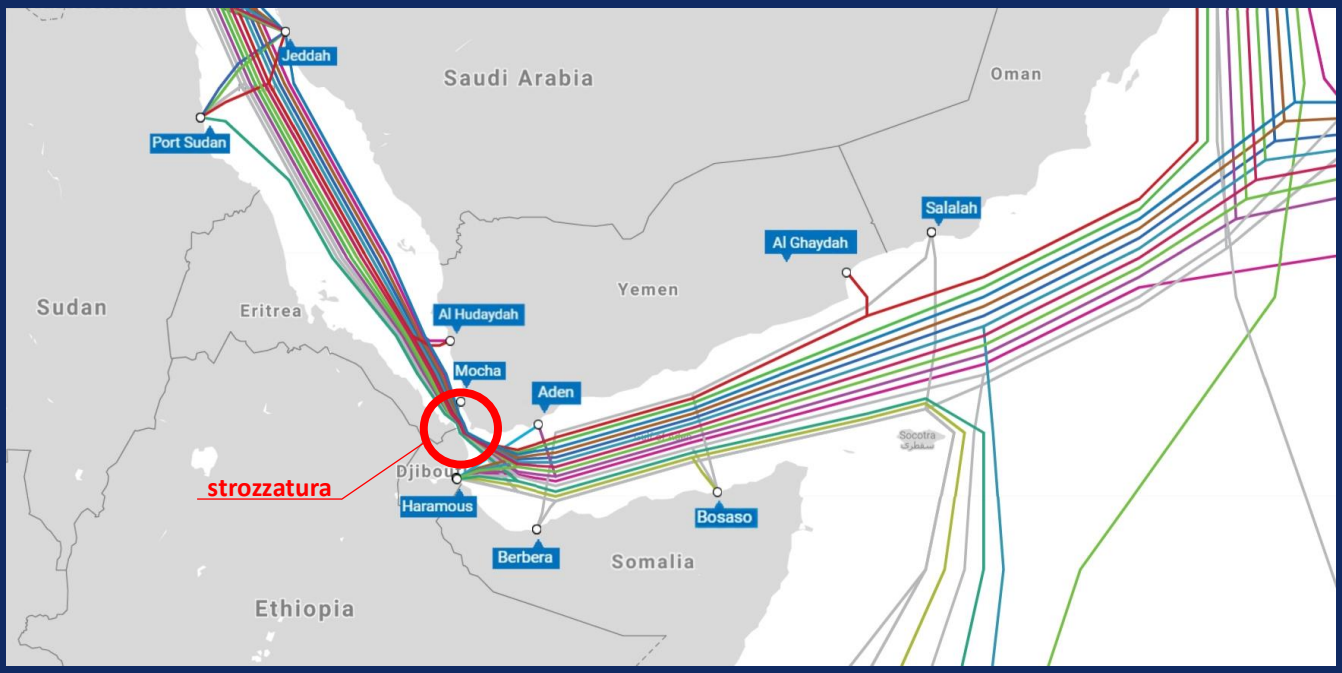
Gran parte dell'infrastruttura sottomarina per le telecomunicazioni è posizionata sui fondali oceanici. Vicino alla costa, dove i fondali sono compresi tra 1000 e 1500 metri di profondità, i cavi vengono protetti da guaine e posati sul fondo marino utilizzando imbarcazioni specializzate; nelle acque più profonde, oltre i 1500 metri, i cavi vengono posati direttamente sui fondali. Le rotte dei cavi vengono scelte mediante sondaggi marini per garantire la sicurezza morfologica e sismica, con una maggiore densità di infrastrutture nelle aree ritenute più sicure.

Data la vastità delle reti di cavi sottomarini e il crescente rischio di minacce ibride, individuare eventuali atti di sabotaggio può risultare problematico, soprattutto nelle regioni più remote e profonde dei mari internazionali. Pertanto, è essenziale implementare sistemi di monitoraggio e reazione capaci di rilevare anticipatamente le minacce emergenti per garantire l'integrità fisica dei cavi e la sicurezza delle informazioni trasmesse.

Come già accennato, i cavi sottomarini sono infrastrutture essenziali per le comunicazioni globali, attraverso le quali passa oltre il 95 % del traffico Internet mondiale, con un flusso di dati che raddoppia ogni 24/30 mesi e con miliardi di dollari di transazioni finanziarie giornaliere, per una lunghezza totale di 1,2 milioni di chilometri (più di tre volte la distanza dal nostro pianeta alla Luna).
Il processo di transizione digitale, accelerato dalla fase pandemica, oltre all'avvento dei nuovi e più potenti standard di comunicazione, come il 5G e le tecnologie da esso abilitate, hanno posto la questione dei cavi al centro dello sviluppo economico e sociale delle società moderne, diventando oggetto della competizione geopolitica tra le grandi potenze.

Diverse, però, sono le criticità in ordine alla sicurezza, trattandosi di infrastrutture esposte a una serie di fattori che possono minacciarne l'integrità fisica e il funzionamento: atti di sabotaggio e attacchi informatici per mano di attori statali o non statali, danneggiamenti legati ad attività umane, come la pesca, oppure a eventi naturali, come terremoti e fauna sottomarina.
È proprio un evento sismico che nel mese di marzo ha messo fuori uso quattro dei più importanti cavi che servono l'Africa, lasciando quasi l'intero Continente senza accesso ad Internet e generando forti ripercussioni sul tessuto economico e sociale.
Ulteriori elementi di criticità, poi, si riscontrano nella tendenza a utilizzare rotte prestabilite nella posa dei cavi, creando punti di strozzatura che, in caso di eventi naturali o di attacchi, espongono intere reti di cavi al rischio di collasso e, quindi, al blocco delle comunicazioni tra una miriade di Paesi.

I punti di strozzatura rappresentano un rischio anche nelle aree di atterraggio sulla terraferma, si pensi, ai casi di atti terroristici o di operazioni di intelligence finalizzate a installare dispositivi per registrare o sottrarre dati (c.d. tapping).
È per queste ragioni che, in ottica di prevenzione, molti esponenti dell'industria consigliano di adottare un approccio basato sulla ridondanza e sulla diversificazione tanto delle rotte quanto delle aree di atterraggio.



Panorama mondiale

Quattro cavi sottomarini sono stati danneggiati nel Mar Rosso il 24 febbraio 2024. L'accaduto, secondo i dati della società di telecomunicazioni di Hong Kong HGC Global Communication, ha bloccato almeno il 25% del traffico Internet tra l'Asia e l'Europa. Due giorni dopo i media israeliani hanno diffuso la notizia secondo la quale i danneggiamenti sarebbero causa delle rappresaglie portate avanti dagli Houthi, i ribelli yemeniti filo iraniani che, per spirito di solidarietà verso il popolo palestinese, stanno compiendo nel Mar Rosso e nel Golfo di Aden attacchi missilistici e atti di sabotaggio contro navi che ritengono collegate a Israele e non solo.

Per gli statunitensi l'ipotesi più accreditata ricollega il danneggiamento accaduto nel Mar Rosso all'attacco missilistico degli Houthi, proprio i ribelli yemeniti che hanno mosso un'azione offensiva il 18 febbraio contro la nave Rubyma, la cui àncora, come precisato dal portavoce del Consiglio per la sicurezza nazionale americana, avrebbe danneggiato i cavi durante l'affondamento.

Il tutto appare ancora incerto, ma l'incidente nel Mar Rosso evidenzia nuovamente la fragilità dei cavi sottomarini e di tutte le infrastrutture strategiche subacquee, fondamentali per la connettività e per il trasporto di energia.
Il processo di transizione digitale, accelerato dalla fase pandemica, e l'avvento dei nuovi e più potenti standard di comunicazione, come il 5G e le tecnologie da esso abilitate, hanno posto i cavi al centro dello sviluppo economico e sociale delle società moderne, diventando oggetto della competizione geopolitica tra le grandi potenze.

La strategia NATO

Il sabotaggio dei gasdotti Nord Stream 1 e 2 ha catalizzato l'attenzione della politica e dell'opinione pubblica europea sull'ambiente *underwater*. Già durante il vertice NATO di Vilnius dell'11 e 12 luglio 2023, è stato affrontato il tema per il quale l'Alleanza ha ufficialmente riconosciuto la centralità delle infrastrutture strategiche sottomarine, impegnandosi altresì a lavorare per la loro protezione. Infatti nel comunicato finale, al punto 65 è possibile leggere: "*La minaccia contro le*

infrastrutture sottomarine critiche è reale e sta aumentando" e si precisa che "*Qualsiasi attacco deliberato contro le infrastrutture critiche degli Alleati sarà affrontato con una risposta unita e determinata; questo vale anche per le infrastrutture sottomarine*", aggiungendo che "*Siamo impegnati a identificare e mitigare le vulnerabilità e le dipendenze strategiche rispetto alle nostre infrastrutture critiche e a prepararci, dissuadere e difendere dall'uso coercitivo dell'energia e da altre tattiche ibride da parte di attori statali e non statali*".

Il vertice ha prodotto anche la decisione di istituire il *Centro marittimo per la sicurezza delle infrastrutture critiche sottomarine* all'interno del *Comando Navale dell'Alleanza Atlantica* (MARCOM) e di creare una rete che riunisca la NATO, gli alleati, il settore privato e altri attori rilevanti per migliorare la condivisione delle informazioni e lo scambio delle migliori pratiche. Ed è appunto in quest'ottica che la NATO ha stretto la cooperazione con l'Unione Europea, lanciando nel gennaio 2023 la task force per la protezione e la resilienza delle infrastrutture critiche.

Nelle conclusioni, il documento individua alcuni punti sui quali fondare la cooperazione NATO-EU.

In particolare, nei punti 7 e 8, si raccomanda di:

- migliorare la consapevolezza delle implicazioni sulla sicurezza derivanti dalla partecipazione o dal controllo delle infrastrutture critiche da parte di entità o fornitori di paesi considerati come concorrenti strategici, anche nelle reti 5G;

- esplorare le possibilità di scambio su come migliorare sia il monitoraggio che la protezione delle infrastrutture critiche nel dominio marittimo da parte delle autorità competenti e discutere le modalità per migliorare la *situational awareness* in ambito marittimo.

In Europa, l'Unione ha lavorato in più direzioni, dapprima aggiornando la strategia di sicurezza marittima, poi trattando la tematica della sicurezza dei cavi sottomarini in una recente raccomandazione della Commissione che ha l'obiettivo di promuovere sinergie a livello UE per aumentare la sicurezza e la resilienza dell'infrastruttura.

La Commissione raccomanda agli Stati membri azioni specifiche per valutare e migliorare il coordinamento sia per quanto riguarda la sicurezza e la resilienza delle infrastrutture di cavi sottomarini nuove ed esistenti sia per quanto riguarda il sostegno alla realizzazione congiunta o al potenziamento significativo di tali infrastrutture attraverso progetti di interesse europeo sui cavi. Inoltre, la Commissione ha annunciato la creazione di un gruppo informale di esperti il cui scopo è fornire alla Commissione consulenza e competenze in relazione alle azioni future da intraprendere in base alla raccomandazione. Si chiede inoltre agli Stati di assistere la Commissione nella presentazione di un *toolbox* per la sicurezza dei cavi, che stabilisca misure per mitigare rischi, vulnerabilità e dipendenze, in particolare in relazione ai fornitori ad alto rischio, oltre a cooperare per sviluppare capacità di manutenzione e riparazione delle infrastrutture di cavi sottomarini.

Esiste la direttiva UE 2022/2557, nota come "*Critical Entities Resilience*" (CER), la quale mira a rafforzare la resilienza fisica delle entità che forniscono servizi essenziali nel mercato europeo, con particolare attenzione ai settori delle infrastrutture digitali, dei trasporti e dello spazio. Sebbene la direttiva CER non sia specifica per i cavi sottomarini, la Commissione è impegnata a promuovere un approccio coordinato per rafforzare la resilienza delle infrastrutture critiche,

compresi i cavi sottomarini, attraverso prove di *stress test* e altre misure preventive. Tuttavia, il monitoraggio delle infrastrutture sottomarine rimane complesso e costoso, soprattutto nei tratti che attraversano acque internazionali.

Le minacce alle stazioni di atterraggio dei cavi sottomarini possono essere molteplici, dalle azioni di sabotaggio agli attacchi esterni. I danni ai cavi in fibra ottica possono essere riparati facilmente, ma quelli alle stazioni di atterraggio possono causare a loro volta danni economici significativi e tempi di ripristino più lunghi. Sebbene siano documentati vari episodi di danneggiamenti, la maggior parte è attribuita a eventi naturali o accidentali.
Per monitorare le rotte e le condizioni dei cavi sottomarini, esistono diversi siti web, come Submarine Cable Map e TeleGeography, che forniscono informazioni dettagliate sulla loro posizione e proprietà. I cavi sottomarini sono indicati sulle carte nautiche con linee di colore magenta, ma in alcune circostanze l'accesso a queste aree può essere limitato per evitare danni accidentali.

Il dominio subacqueo e il ruolo dell'Italia

Vista la sua posizione strategica nel Mediterraneo e non solo, il nostro Paese si candida a svolgere un ruolo cruciale e strategico. Nel mar Mediterraneo viene ospitato circa il 16% del traffico Internet mondiale, a questo si aggiunge, nell'ambito della politica estera italiana del Piano Mattei, il Polo nazionale della dimensione subacquea (PNS), nato il 12 dicembre 2023 a La Spezia è che punta a diventare un hub strategico. Esso ha origine sotto l'egida della Marina militare con l'obiettivo di diventare un incubatore delle conoscenze e delle tecnologie necessarie per esplorare la dimensione sottomarina e difendere le sue infrastrutture critiche. La governance del Polo sarà interministeriale e si fonderà sulla cooperazione tra strutture pubbliche e private, secondo una logica di sistema che riunirà la marina Militare, il mondo accademico, scientifico e l'industria, come ha spiegato Nello Musumeci, Ministro per la Protezione civile e le Politiche del mare, in sede di inaugurazione del Polo. Si tratta dunque di una nuova realtà che mira ad aggregare e valorizzare le eccellenze italiane e contribuirà, sul piano esterno, a consolidare la leadership dell'Italia nel

settore, proponendosi come un punto di riferimento per NATO e UE nella protezione delle infrastrutture critiche sottomarine.

Tutto ciò, in particolare quando si affronta il problema delle varie "sicurezze nazionali", rappresenta l'immenso sistema nervoso centrale delle telecomunicazioni globali: il 99% di tutto il traffico internazionale voce e dati di 7,8 miliardi di persone passa per cavi lunghi migliaia di chilometri stesi sui fondali degli oceani.

È opportuno ricordare che proprietario di queste autostrade sottomarine è chi le posa, mentre la gestione è nelle mani di chi le attiva fornendo i flussi di informazioni, cioè in primis le compagnie telefoniche ed elettriche.
La loro rilevanza deriva dal fatto che esse memorizzano e conservano tutto ciò che transita lungo i cavi, ed è dunque possibile mandare in tilt il sistema informatico di interi Paesi, bloccando così la fornitura di energia, compromettere la distribuzione idrica, il sistema dei trasporti pubblici, interrompere le trasmissioni di un satellite, le transazioni elettroniche, le comunicazioni via Internet, i sistemi di trasmissione delle informazioni sensibili di ministeri e istituzioni.

Oramai solo "*i nostalgici*" posso credere che le prossime guerre saranno come quelle che purtroppo l'umanità ha dovuto soffrire e soffrono e in vaste zone del pianeta. Ma in futuro il tutto ruoterà intorno alla tecnologia, e non quindi più lieve ma anzi la devastazione potrebbe assumere dimensioni ancor più smisurate e globali.

Gli esperti di tutte le intelligence mondiali sono al corrente di questo rischio elevato e nella catastrofica ipotesi di una guerra mondiale questa sarebbe avviata da un innesco che porterebbe al controllo dei cavi sottomarini a fibra ottica, bersaglio perfetto nel contempo per il moderno terrorismo internazionale.

La protezione delle infrastrutture sottomarine, quindi, è cruciale per garantire la continuità delle comunicazioni globali. È fondamentale implementare sistemi di monitoraggio avanzati e promuovere la cooperazione internazionale per contrastare le minacce emergenti. Inoltre, non è piu procrastinabile sviluppare strategie nazionali e comunitarie specifiche per garantire la resilienza e la sicurezza delle reti di cavi sottomarini in quest'era digitale in così rapida evoluzione.

Biagino Costanzo
- CISINT Research Analyst
- Presidente di KNOSSO (Knowledge for a Safe and Secure Organization)
- Professore a contratto in Scienze Forensi e Criminologiche per la difesa e la sicurezza

INFOGRAFICA:

Pag 1 - https://zmscable.es/wp-content/uploads/2024/03/cable-submarino-roto-1024x597.jpg
Pag 2 - https://www.primapaginamazara.it/i-9-cavi-sconosciuti-che-collegano-mazara-al-mondo-intero-spionaggio-o-business-seconda-parte
Pag 4 - https://www.corriere.it/tecnologia/24_marzo_06/perche-il-mar-rosso-e-il-punto-piu-vulnerabile-di-internet-gli-attacchi-houti-e-i-4-cavi-sottomarini-danneggiati-6cb62233-a3d3-4ca9-b3d6-0d4451653xlk.shtml
Pag 6 - https://defence-industry.eu/eu-and-nato-are-stepping-up-protection-of-critical-infrastructure/
Pag 8 - https://ricerca2.unibs.it/?page_id=25742
https://www.news9live.com/technology/tech-news/red-sea-internet-cable-cuts-impact-connectivity-2457079