I cavi sotto il mare

L'infrastruttura fisica di internet globale: chi la possiede e chi potrebbe spegnerla o intercettarla.

CONTROPOTERE

un libro di Alessio Farinella

I cavi sotto il mare

L'infrastruttura fisica di internet globale: chi possiede i cavi sottomarini e i data center, e chi potrebbe spegnerli o intercettarli

Alessio Farinella

Indice

Prefazione

Quando mandi un messaggio dall'Italia agli Stati Uniti, quel messaggio non passa per una «nuvola» eterea sospesa da qualche parte sopra le nostre teste. Viaggia, fisicamente, dentro un cavo spesso più o meno quanto un tubo da giardino, posato sul fondo dell'oceano, a chilometri di profondità, tra squali che ogni tanto lo mordono e ancore di navi che ogni tanto lo strappano.

Il 95-99% di tutto il traffico internet che attraversa i continenti — email, videochiamate, transazioni bancarie, ordini militari — passa per circa 600 di questi cavi. Non per i satelliti, che pure esistono e servono a molto altro, ma non hanno la capacità di trasportare la quantità di dati che il mondo scambia ogni secondo. Pochissime aziende al mondo possiedono, oggi, una fetta sempre più grande di questa infrastruttura fisica: non più solo consorzi statali di telecomunicazioni, come per gran parte del Novecento, ma le stesse grandi piattaforme tecnologiche che usiamo ogni giorno per cercare, comunicare, guardare video.

Questo libro segue quel cavo, dal fondo dell'oceano fino a chi lo possiede davvero: chi lo controlla, chi può tagliarlo — per errore o non — e chi, come rivelato oltre un decennio fa da un informatico americano in fuga,

può leggere quello che ci passa dentro senza che tu lo sappia mai.

Capitolo 1 — Come funziona davvero internet: niente nuvola, solo cavi

Un'espressione comoda, ma fisicamente sbagliata

Diciamo spesso che i nostri dati sono «nella nuvola» (in inglese, «cloud»): un'immagine rassicurante, che suggerisce qualcosa di leggero, immateriale, sospeso da qualche parte sopra le nostre teste. È un'espressione comodissima per il marketing tecnologico, ma fisicamente fuorviante. Ogni email, ogni video, ogni ricerca online esiste, concretamente, come impulsi di luce che viaggiano dentro cavi fisici, di solito posati sul fondo del mare, tra un continente e l'altro.

Il numero che sorprende quasi tutti

Tra il **95% e il 99% di tutto il traffico internet intercontinentale** — non quello locale dentro un singolo paese, ma quello che collega un continente all'altro — passa attraverso circa **600 cavi in fibra ottica sottomarini**. Non attraverso i satelliti, che pure esistono, sono importanti per usi specifici (comunicazioni militari, aree remote, servizi come Starlink), ma non

hanno la capacità di trasportare l'enorme mole di dati che il mondo scambia ogni secondo attraverso questi cavi. Su questa rete transitano ogni giorno transazioni finanziarie stimate in circa **10.000 miliardi di dollari**.

Un cavo spesso quanto un tubo da giardino

Un dettaglio che sorprende chi lo scopre per la prima volta: il diametro tipico di un cavo sottomarino moderno, nella sua parte più sottile, non è molto più grande di un tubo da giardino — pochi centimetri, che racchiudono al centro le sottilissime fibre ottiche vere e proprie, protette da diversi strati di acciaio, rame e materiali isolanti per resistere alla pressione delle profondità oceaniche e ai danni accidentali.

Una storia che comincia nel 1858

Il primo tentativo di collegare due continenti con un cavo sottomarino risale al **16 agosto 1858**, quando viene inaugurato il primo cavo telegrafico transatlantico, tra Irlanda e Terranova. Il primo messaggio ufficiale trasmesso è un telegramma della Regina Vittoria d'Inghilterra al Presidente degli Stati Uniti James Buchanan, che celebra il nuovo legame tra le due sponde dell'Atlantico. Il cavo, però, smette di funzionare dopo appena tre settimane, per problemi tecnici e l'usura precoce dei materiali dell'epoca. Solo nel 1866, dopo altri tentativi falliti, viene completato un

cavo abbastanza resistente da garantire comunicazioni transatlantiche stabili — l'inizio di una tecnologia che, quasi 170 anni dopo, resta ancora oggi il modo principale in cui il mondo comunica tra un continente e l'altro.

Perché questo capitolo apre il libro

Capire che internet è, fisicamente, una rete di cavi posati sul fondo del mare — non un'astrazione senza luogo — è il punto di partenza necessario per tutto il resto di questo libro: chi possiede quei cavi (Capitolo 2), dove passano e perché alcuni punti geografici sono più vulnerabili di altri (Capitolo 3), cosa succede quando vengono danneggiati (Capitolo 4), e chi può, in teoria, ascoltare quello che ci passa dentro (Capitolo 6). Nessuno di questi temi ha senso se si continua a pensare a internet come a qualcosa che «sta nella nuvola», invece che come a un'infrastruttura fisica precisa, concentrata in mani sempre più poche.

Capitolo 2 — Chi possiede i cavi oggi

Da consorzi statali a quattro aziende private

Per gran parte del Novecento, i cavi sottomarini che collegavano i continenti erano posseduti e gestiti principalmente da consorzi di compagnie telefoniche nazionali — spesso partecipate o controllate dagli stati

stessi, che negoziavano insieme la costruzione e la gestione di ogni nuovo cavo, dividendone i costi e la capacità di trasmissione.

Negli ultimi quindici anni, questo modello è cambiato radicalmente. Quattro grandi aziende tecnologiche — **Meta (proprietaria di Facebook, Instagram e WhatsApp), Amazon, Microsoft e Google** — hanno cominciato a finanziare, e in molti casi a possedere direttamente, una quota sempre più grande della rete mondiale di cavi sottomarini. Secondo i dati più recenti, disponibili al 2024, queste quattro aziende **detengono insieme oltre il 50% del mercato mondiale dei cavi sottomarini**. Meta, da sola, arriva a possedere circa il 13% del totale.

Perché le Big Tech hanno cominciato a costruire cavi propri

La ragione è semplice da capire: queste aziende gestiscono un volume di dati talmente enorme — video in streaming, servizi cloud, intelligenza artificiale — che affittare capacità sui cavi dei consorzi tradizionali era diventato, per loro, più costoso e meno affidabile che costruirsi cavi propri, dimensionati esattamente sulle proprie esigenze. Nel 2024, le reti dei grandi fornitori di contenuti e servizi cloud (Google, Meta, Microsoft, Amazon) hanno assorbito quasi **tre quarti di tutta la domanda mondiale di banda internazionale** — una quota che dà la misura di quanto il traffico globale

sia ormai dominato da un numero ristrettissimo di operatori privati.

Un mercato in forte crescita

Gli investimenti nel settore stanno accelerando rapidamente: tra il 2023 e il 2025 sono previsti oltre **10 miliardi di dollari** di nuovi investimenti, per 78 nuovi sistemi di cavi e oltre 300.000 chilometri di lunghezza complessiva — più della circonferenza terrestre otto volte. Le stime indicano che gli investimenti nei prossimi due anni raddoppieranno rispetto al biennio precedente.

Cosa significa, per chi non lavora nel settore tecnologico

Il passaggio da un modello di proprietà pubblica o consortile a un modello dominato da quattro aziende private ha una conseguenza diretta: le decisioni su dove costruire un nuovo cavo, quale rotta scegliere, quale paese collegare per primo, non rispondono più principalmente a una logica di interesse pubblico o di equilibrio geopolitico negoziato tra stati, ma a una logica commerciale privata — dove passa più traffico redditizio per quella specifica azienda, quali data center (di cui parleremo nel Capitolo 5) devono essere collegati più velocemente. Non significa che questa logica sia necessariamente contraria all'interesse pubblico — spesso coincide, ampliando comunque la connettività globale — ma significa che il controllo

di un'infrastruttura ormai critica quanto l'energia o i trasporti è concentrato in un numero di soggetti privati sorprendentemente piccolo, per un'infrastruttura da cui dipende, ormai, gran parte dell'economia mondiale.

Capitolo 3 — I punti di strozzatura geografici

Non tutto l'oceano è uguale

I cavi sottomarini non sono distribuiti in modo uniforme sui fondali di tutto il mondo. Per ragioni di geografia — la forma delle coste, la profondità dei fondali, la distanza più breve tra due continenti — decine di cavi diversi finiscono spesso per passare tutti attraverso gli stessi, pochi corridoi stretti. Gli esperti del settore li chiamano **punti di strozzatura** (in inglese, «chokepoints»): aree geografiche ristrette dove si concentra una quota sproporzionata dell'intera rete mondiale.

I tre corridoi più critici al mondo

Tre aree, in particolare, ricorrono in ogni analisi geopolitica sui cavi sottomarini: lo **stretto di Luzon**, a sud di Taiwan, lo **stretto di Malacca**, tra Malesia e Indonesia — uno dei passaggi marittimi più trafficati al mondo anche per il trasporto merci — e il **Mar Rosso**, il corridoio che collega il Mediterraneo, attraverso il Canale di Suez, all'Oceano Indiano e da lì all'Asia.

Il Mar Rosso, da solo, è attraversato da almeno **16 cavi sottomarini**, che insieme trasportano circa il **17% di tutto il traffico internet mondiale** — una concentrazione enorme in un tratto di mare relativamente stretto, per una lunghezza complessiva di circa 1.930 chilometri di cavi in quella sola area.

Perché la concentrazione geografica è un rischio

Pensa a un'autostrada a otto corsie che, per un tratto di pochi chilometri, si restringe improvvisamente a una sola corsia: un solo incidente in quel punto specifico può bloccare tutto il traffico che, per il resto del percorso, avrebbe avuto molte alternative. È esattamente la stessa logica che rende questi corridoi marittimi così delicati: un singolo evento — un'ancora trascinata sul fondale, un atto deliberato di sabotaggio, persino un terremoto sottomarino — può interrompere contemporaneamente decine di cavi diversi, con effetti su interi continenti, semplicemente perché quei cavi, per ragioni geografiche, passano tutti nello stesso stretto tratto di mare.

Un esempio concreto, prima del prossimo capitolo

Nel marzo 2024, quattro cavi sottomarini diversi — Seacom, TGN, AAE-1 ed EIG — vengono danneggiati quasi contemporaneamente nel Mar Rosso, con un impatto stimato sul 25% del traffico internet che nor-

malmente transita in quell'area. Non è stato un attacco coordinato su quattro cavi diversi in punti diversi del pianeta: è stato un singolo evento, concentrato in un tratto di mare dove — proprio per la logica dei punti di strozzatura raccontata in questo capitolo — passavano tutti insieme. Il prossimo capitolo racconta questo caso, e altri simili, nel dettaglio.

Zero alternative immediate, quando lo stretto si blocca

L'ultimo aspetto da capire è la mancanza di alternative rapide: quando un corridoio come il Mar Rosso viene interrotto, il traffico dati non può semplicemente «deviare» su un'altra rotta nello stesso modo in cui un'auto può prendere una strada diversa. I cavi alternativi, quando esistono, hanno spesso una capacità limitata, o richiedono percorsi molto più lunghi — attorno all'Africa, invece che attraverso Suez — con conseguenze dirette su velocità e affidabilità delle connessioni per milioni di utenti, ben oltre i paesi direttamente coinvolti nell'incidente.

Capitolo 4 — Sabotaggi e incidenti: i casi recenti

Il Mar Rosso, marzo 2024

Il capitolo precedente ha già anticipato il caso: nel marzo 2024, quattro cavi sottomarini — Seacom, TGN, AAE-1 ed EIG — vengono danneggiati quasi contem-

poraneamente nel Mar Rosso, con un impatto stimato sul 25% del traffico internet che normalmente passa in quell'area. Il cavo AAE-1, in particolare, collega direttamente l'Asia orientale all'Europa passando per l'Egitto — una delle arterie principali della connettività tra i due continenti.

La causa più accreditata riguarda la nave cargo **Rubymar**, colpita il 18 febbraio 2024 da un missile antinave lanciato dai ribelli Houthi dello Yemen, nel contesto degli attacchi alla navigazione internazionale nel Mar Rosso legati al conflitto in corso nella regione. Secondo la ricostruzione più diffusa, la nave colpita avrebbe trascinato l'ancora di tribordo sul fondale prima che l'equipaggio la abbandonasse, danneggiando i cavi che passavano in quel tratto di mare. Gli Houthi hanno negato pubblicamente ogni coinvolgimento diretto in un sabotaggio deliberato.

Il Mar Baltico, ottobre 2023

L'8 ottobre 2023 viene rilevata una perdita nel gasdotto Balticconnector, che collega Finlandia ed Estonia attraverso il golfo di Finlandia, insieme all'interruzione di un cavo di telecomunicazioni nella stessa area. L'ipotesi iniziale, discussa apertamente nei media, è quella di un sabotaggio russo, in un momento di forti tensioni geopolitiche nella regione baltica. Le autorità finlandesi, dopo le indagini, attribuiscono però il danno a un incidente: l'ancora di una nave portacontainer cinese, trascinata per errore lungo il fondale.

Il Mar Baltico, novembre 2024

Poco più di un anno dopo, a novembre 2024, altri due cavi di comunicazione — il BCS East-West Interlink e il C-Lion — vengono danneggiati nella stessa area del Baltico. Le autorità danesi fermano, nei giorni successivi, la nave cargo cinese **Yi Peng 3**, trovata nelle vicinanze dell'incidente. Secondo una ricostruzione dettagliata del Wall Street Journal, la nave avrebbe trascinato la propria ancora sul fondale per **oltre 170 chilometri**, un tragitto lunghissimo per essere un puro incidente casuale — un dettaglio che alimenta i sospetti, mai confermati pubblicamente, di un'azione deliberata. Tra l'equipaggio della nave figurava anche un marinaio russo. La nave viene rilasciata il 21 dicembre 2024, dopo un'ispezione internazionale i cui risultati non sono mai stati resi pubblici.

Accidentale o deliberato? Un'onestà necessaria

Per ognuno di questi casi, va detto con la massima chiarezza: **non esiste, a oggi, una prova pubblica definitiva che stabilisca con certezza l'intenzionalità** di nessuno di questi episodi. Le circostanze — il contesto geopolitico teso, la presenza di equipaggi con collegamenti a paesi in tensione con l'Occidente, la lunghezza insolita del tragitto dell'ancora nel caso della Yi Peng 3 — alimentano sospetti legittimi, ma un libro onesto deve distinguere con precisione tra un sospetto fondato e una prova ac-

certata. Nessuno dei casi raccontati in questo capitolo ha, a oggi, una conclusione giudiziaria o investigativa resa pubblica in modo definitivo.

Cosa rivelano questi casi, al di là della singola causa

Indipendentemente da chi abbia ragione sull'intenzionalità di ogni singolo episodio, questi eventi rivelano un dato di fatto incontestabile: un'infrastruttura da cui dipende una fetta enorme dell'economia e della comunicazione mondiale, come mostrato nei capitoli precedenti, è protetta, sul piano fisico e militare, in modo sorprendentemente debole. Non esistono pattugliamenti costanti e dedicati lungo la maggior parte dei tracciati dei cavi sottomarini nel mondo; il danneggiamento — accidentale o deliberato che sia — resta relativamente facile da causare, e difficile da prevenire in anticipo.

Capitolo 5 — I data center: dove vivono davvero i tuoi dati

Il punto d'arrivo dei cavi

I cavi sottomarini raccontati nei capitoli precedenti non trasportano dati senza una destinazione: li portano verso i **data center**, gli enormi edifici pieni di server dove le informazioni vengono effettivamente conservate, elaborate, restituite quando fai una ricerca online o guardi un video in streaming. Se i cavi sono le

arterie di internet, i data center sono gli organi verso cui quelle arterie convergono.

Una concentrazione geografica sorprendente

Nonostante internet sia, in teoria, una rete globale e distribuita, i data center più grandi al mondo si concentrano in pochissime aree geografiche. La **Virginia del Nord**, negli Stati Uniti, ospita la più alta concentrazione di data center al mondo: nel 2024, questi impianti assorbono da soli circa il **26% del fabbisogno elettrico** dell'intero stato. In Europa, l'**Irlanda** gioca un ruolo simile: l'incidenza dei data center sui consumi elettrici nazionali è passata dal 5% nel 2015 al **21% nel 2023** — quasi un quarto di tutta l'elettricità consumata nel paese.

Perché proprio questi luoghi

La scelta di dove costruire un data center non è casuale: dipende da un mix di fattori — clima fresco (che riduce i costi di raffreddamento dei server, che generano calore enorme), disponibilità di energia elettrica a basso costo, stabilità politica e normativa, e — spesso l'elemento decisivo — agevolazioni fiscali offerte dai governi locali per attirare questi investimenti, che portano occupazione e indotto economico, anche se in misura relativamente modesta rispetto alla scala degli investimenti stessi.

La fame di energia e acqua dell'intelligenza artificiale

Negli ultimi anni, la crescita esplosiva dei servizi di intelligenza artificiale ha reso questo tema ancora più urgente. Addestrare e far funzionare i grandi modelli di intelligenza artificiale richiede una potenza di calcolo enorme, con un consumo energetico proporzionalmente enorme: le stime indicano che la domanda energetica dei carichi di lavoro legati all'IA dovrebbe più che raddoppiare tra il 2023 e il 2028, crescendo a un ritmo del **44,7% l'anno** fino al 2027.

Meno noto, ma altrettanto significativo, è il consumo d'acqua: i data center usano grandi quantità d'acqua per i sistemi di raffreddamento, soprattutto durante le fasi più intensive di addestramento dei modelli di intelligenza artificiale. In Virginia, il consumo d'acqua dei data center è cresciuto di **due terzi tra il 2019 e il 2023** — un aumento che comincia a entrare in competizione diretta con altri usi civili e agricoli dell'acqua nelle stesse aree.

Chi decide, e chi ne subisce le conseguenze

Le decisioni su dove costruire un nuovo data center — con quale impatto su rete elettrica locale, prezzo dell'energia per i residenti, disponibilità di acqua — vengono prese quasi sempre dalle stesse grandi aziende tecnologiche che, come visto nel Capitolo 2,

possiedono ormai una quota crescente anche dei cavi sottomarini che alimentano questi impianti di dati. Le comunità locali che vivono vicino a un grande data center si trovano spesso a sperimentare direttamente gli effetti collaterali — bollette più alte, minore disponibilità d'acqua — di una decisione presa altrove, in base a criteri che raramente includono, come priorità principale, l'interesse della comunità che ospita fisicamente l'infrastruttura.

Capitolo 6 — La sorveglianza sui cavi: cosa hanno rivelato i casi Snowden

Un ex tecnico dei servizi segreti, migliaia di documenti

Nel 2013, Edward Snowden, ex collaboratore tecnico della National Security Agency (NSA) statunitense, rende pubblici migliaia di documenti riservati che rivelano l'esistenza di programmi di sorveglianza di massa condotti dalle agenzie di intelligence di Stati Uniti e Regno Unito — programmi che, per la prima volta, mostrano con dettagli tecnici precisi come i cavi sottomarini raccontati in questo libro non siano solo infrastrutture di comunicazione, ma anche punti privilegiati di intercettazione.

Il programma Tempora

Tra i documenti più rilevanti per il tema di questo libro c'è la rivelazione del programma **Tempora**, gestito dal GCHQ, l'agenzia di intelligence britannica — l'equivalente della NSA americana per il Regno Unito. Testato dal 2008 e diventato pienamente operativo alla fine del 2011, Tempora permetteva di intercettare direttamente i dati che transitano attraverso i cavi in fibra ottica che approdano sul territorio britannico — una posizione geografica privilegiata, dato che il Regno Unito è un punto di passaggio obbligato per gran parte del traffico dati tra Europa e Nord America.

Cosa veniva raccolto, davvero

I documenti Snowden mostrano che Tempora non si limitava a intercettare comunicazioni di specifici sospetti individuati in anticipo: raccoglieva, analizzava e archiviava enormi quantità di dati relativi alle comunicazioni di **milioni di persone**, incluse moltissime prive di qualunque interesse concreto per le attività di intelligence — semplici cittadini che facevano telefonate, mandavano email, navigavano su internet, senza alcun sospetto specifico a loro carico. I dati raccolti attraverso questo programma venivano inoltre condivisi direttamente con la NSA statunitense, in base ad accordi di cooperazione tra le due agenzie che risalgono alla Guerra Fredda.

Altri programmi collegati

Le slide interne rese pubbliche da Snowden fanno riferimento anche ad altri programmi con nomi altrettanto espliciti: «Mastering the Internet» e «Global Telecoms Exploitation» — entrambi dedicati, come suggeriscono gli stessi nomi, al monitoraggio sistematico delle infrastrutture globali di telecomunicazione, cavi sottomarini inclusi.

Perché i cavi sono un punto debole strutturale

Il motivo tecnico per cui i cavi sottomarini si prestano particolarmente bene a questo tipo di intercettazione è semplice: a differenza di una comunicazione via etere, che si diffonde in tutte le direzioni ed è difficile da isolare senza un'antenna dedicata, un cavo sottomarino concentra un'enorme quantità di traffico dati in un unico punto fisico. Chi ha accesso legale o tecnico a quel punto — per esempio, dove il cavo approda fisicamente sulla terraferma, in una stazione di atterraggio (in inglese, «landing station») — può, in teoria, copiare e analizzare una quota enorme del traffico mondiale, senza dover intercettare milioni di singole comunicazioni separate.

Cosa è cambiato, e cosa no, dopo il 2013

Le rivelazioni Snowden hanno scatenato un dibattito pubblico e giudiziario che dura ancora oggi: nel settembre 2018 la Corte Europea dei Diritti dell'Uomo ha

condannato il Regno Unito proprio per il regime di intercettazione di massa rivelato da Tempora, giudicandolo incompatibile con il diritto alla privacy garantito dalla Convenzione Europea dei Diritti dell'Uomo — una condanna confermata e rafforzata nel maggio 2021 dalla Grande Camera della stessa Corte, il grado di giudizio più alto disponibile, che ha stabilito come il GCHQ avesse intercettato illegalmente le comunicazioni pubbliche per decenni. Ma una sentenza di condanna non equivale, automaticamente, allo smantellamento del programma: le capacità tecniche di intercettazione sui cavi sottomarini restano, secondo gli esperti del settore, sostanzialmente intatte più di un decennio dopo le rivelazioni originarie — cambiano le cornici legali che ne regolano, sulla carta, l'uso, non necessariamente le capacità tecniche reali delle agenzie coinvolte.

Capitolo 7 — Chi controlla i «punti di scambio» (Internet Exchange Point)

Dove le reti si incontrano

Oltre ai cavi che attraversano gli oceani e ai data center dove i dati vengono conservati, esiste un terzo tipo di infrastruttura fisica cruciale, meno conosciuta dal grande pubblico: gli **Internet Exchange Point** (IXP, punti di scambio internet). Sono luoghi fisici — spesso

edifici enormi, apparentemente anonimi dall'esterno — dove le reti di operatori diversi (compagnie telefoniche, provider internet, grandi aziende tecnologiche) si collegano direttamente tra loro, scambiandosi traffico dati senza dover passare attraverso intermediari esterni.

Perché servono

Immagina decine di compagnie di autobus diverse che devono farsi scambio di passeggeri tra loro in una grande città. Invece di costruire un percorso diretto tra ogni singola coppia di compagnie — un lavoro enorme e inefficiente — è molto più semplice costruire un unico grande terminal centrale, dove tutte le compagnie si fermano e i passeggeri possono cambiare autobus. Un Internet Exchange Point funziona secondo la stessa logica: invece che ogni rete debba negoziare una connessione diretta separata con ogni altra rete nel mondo, si collega a un hub centrale dove avviene lo scambio.

Pochi hub, per un traffico enormemente concentrato

Nonostante ne esistano centinaia in tutto il mondo, una quota sproporzionata del traffico dati globale passa attraverso un numero molto ristretto di hub particolarmente grandi: **Francoforte** (sede del più grande IXP al mondo per volume di traffico), **Londra**, **Amsterdam** e **Singapore** sono, da soli, responsabili

di una fetta enorme dello scambio dati mondiale, in particolare per il traffico che collega Europa e Asia.

Lo stesso problema dei cavi, in un altro punto della rete

Questa concentrazione replica, in un punto diverso della rete, lo stesso rischio strutturale raccontato nei capitoli precedenti a proposito dei cavi sottomarini e dei loro punti di strozzatura geografici: se uno di questi grandi hub subisce un guasto tecnico grave, un attacco informatico su larga scala, o un evento fisico imprevisto, l'effetto si propaga su una porzione enorme del traffico dati mondiale, ben oltre il singolo paese che ospita fisicamente l'infrastruttura.

Chi possiede, davvero, questi hub

A differenza dei cavi sottomarini, dove abbiamo visto nel Capitolo 2 una crescente concentrazione nelle mani di poche grandi aziende tecnologiche, molti dei principali Internet Exchange Point restano gestiti da consorzi non-profit o da operatori misti pubblico-privati, radicati storicamente nel paese che li ospita. È una differenza importante rispetto al resto di questo libro: non tutta l'infrastruttura critica di internet segue la stessa traiettoria di concentrazione privata. Ma anche in questo caso, la domanda di fondo resta la stessa che attraversa tutto il libro: cosa succede alla connettività di un intero continente se uno di questi

pochissimi punti nevralgici smette di funzionare, per qualsiasi motivo?

Capitolo 8 — La corsa ai cavi come strumento geopolitico

Un cavo non è mai solo un cavo

Costruire un nuovo cavo sottomarino non è più, oggi, solo una decisione commerciale su dove serve più capacità di trasmissione. È diventata, sempre più spesso, una decisione con implicazioni geopolitiche esplicite: quale paese collegare, quale evitare, quale rotta scegliere per non passare vicino a un rivale strategico.

Il caso del cavo bloccato: PLCN

L'esempio più diretto e documentato di questa dinamica riguarda il **Pacific Light Cable Network** (PLCN), un cavo sottomarino progettato per collegare Stati Uniti, Hong Kong, Taiwan e Filippine, costruito e posseduto congiuntamente da Google, Meta e da un'azienda con base a Hong Kong, la Pacific Light Data Communication.

Nel giugno 2020, il comitato interagenzie del governo statunitense noto come «Team Telecom» raccomanda formalmente alla Federal Communications Commission (FCC), l'autorità che regola le telecomunicazioni negli Stati Uniti, di negare la parte della licenza relativa al collegamento diretto tra Stati Uniti e Hong Kong,

citando esplicitamente rischi per la sicurezza nazionale legati a possibili legami tra l'azienda coinvolta ed entità statali cinesi. Google e Meta, di fronte a questa raccomandazione, ritirano la domanda originale e la ripresentano senza il tratto verso Hong Kong: il cavo, riconfigurato, ottiene finalmente la licenza dalla FCC nel gennaio 2022 — ma senza il collegamento diretto che era stato uno degli obiettivi originari del progetto.

Perché un cavo di dati diventa una questione di sicurezza nazionale

La logica dietro casi come questo è la stessa che attraversa tutto questo libro: chi possiede fisicamente un cavo — o l'azienda che lo gestisce — ha, in teoria, una capacità tecnica di accesso ai dati che vi transitano, come mostrato nel Capitolo 6 a proposito della sorveglianza rivelata da Snowden. Un governo che sospetta legami tra l'azienda proprietaria di un cavo e un servizio di intelligence straniero considera quel cavo non solo un'infrastruttura di comunicazione, ma un potenziale canale di accesso privilegiato ai propri dati, o un possibile punto di sabotaggio in caso di crisi geopolitica.

Rotte alternative, promosse da entrambe le parti

Sia gli Stati Uniti sia la Cina promuovono oggi, separatamente, progetti di cavi pensati esplicitamente per evitare di dipendere da infrastrutture controllate,

anche solo in parte, dall'altra potenza. Progetti di cavi sponsorizzati da consorzi vicini agli interessi americani evitano deliberatamente rotte che passerebbero per infrastrutture di atterraggio in territorio cinese o vicino ad esso; allo stesso modo, la Cina ha promosso propri progetti di cavi alternativi, per garantirsi collegamenti internazionali che non dipendano da infrastrutture controllate da paesi occidentali.

Una frammentazione silenziosa

Il risultato di questa dinamica, capitolo dopo capitolo di questo libro, è una progressiva frammentazione geopolitica di un'infrastruttura che, per sua natura tecnica, dovrebbe essere la più globale e interconnessa possibile. Non si tratta ancora di una separazione netta in due internet paralleli — un'ipotesi discussa da alcuni analisti come scenario futuro possibile, ma non ancora realtà compiuta — ma di una tendenza chiara: sempre più spesso, la domanda su dove costruire un nuovo cavo, e quale rotta fargli seguire, non è più solo «dove serve più capacità», ma anche «quale rotta evita di dipendere dall'infrastruttura del rivale geopolitico del momento».

Capitolo 9 — Cosa succede se un paese viene «scollegato»

Un interruttore che esiste davvero

I capitoli precedenti hanno raccontato come internet possa essere interrotto dall'esterno — un cavo tagliato, un sabotaggio, un incidente. Questo capitolo racconta l'altra faccia della stessa medaglia: cosa succede quando è un governo stesso a decidere di staccare la spina, deliberatamente, all'accesso internet della propria popolazione.

Il caso Egitto, 2011

Il caso più noto e meglio documentato risale alla notte tra il 27 e il 28 gennaio 2011, nel pieno delle proteste della Primavera araba contro il governo egiziano. Il presidente Hosni Mubarak ordina il blackout totale dell'accesso a internet in tutto il paese. Poco dopo mezzanotte, le società internazionali che monitorano il traffico globale osservano l'Egitto scomparire quasi completamente dalla rete mondiale — un intero paese di oltre 80 milioni di persone, isolato digitalmente con una decisione politica dall'oggi al domani.

Il blackout dura cinque giorni. Ma l'effetto politico è opposto a quello sperato dal governo: privati della possibilità di comunicare online, i manifestanti si organizzano comunque, e l'affluenza alle piazze cresce ulteriormente nei giorni successivi, fino a raggiunge-

re, secondo alcune stime, i due milioni di persone. Il caso egiziano diventa, da allora, il modello di riferimento — in negativo — studiato da ricercatori e organizzazioni per i diritti digitali, e purtroppo anche, in alcuni casi, da altri governi che hanno successivamente adottato blackout simili in momenti di tensione politica interna, dall'Iran al Myanmar.

Come è tecnicamente possibile

Un blackout nazionale di questo tipo è possibile perché, in molti paesi, l'accesso internet passa attraverso un numero relativamente ristretto di punti di controllo centralizzati — spesso gli stessi cavi sottomarini e le stazioni di atterraggio raccontate nei capitoli precedenti, o un numero limitato di fornitori di connettività nazionale sui quali il governo ha, per legge o per pressione diretta, un potere di intervento immediato. Più un paese dipende da pochi punti di accesso centralizzati, più diventa tecnicamente semplice per chi controlla quei punti — un governo, ma in teoria anche un attore esterno capace di comprometterli — interrompere l'accesso per l'intera popolazione con una singola decisione.

Un rischio diverso, ma collegato al resto del libro

Un blackout nazionale imposto da un governo è, in un certo senso, l'opposto di un sabotaggio esterno di un cavo sottomarino raccontato nel Capitolo 4: nel

primo caso, chi controlla l'infrastruttura sceglie di interromperla; nel secondo, qualcun altro la danneggia dall'esterno. Ma entrambi gli scenari condividono la stessa lezione di fondo: la connettività di un intero paese può dipendere, in ultima istanza, da un numero sorprendentemente piccolo di punti fisici o decisionali — che si tratti di un cavo sul fondo del mare o di un interruttore nelle mani di un singolo governo.

Capitolo 10 — Le obiezioni, trattate con onestà

«È sempre stato così, e il sistema ha sempre retto»

È vero: la rete di cavi sottomarini funziona, nel complesso, da oltre un secolo, e i pochi incidenti gravi raccontati in questo libro non hanno mai causato un collasso permanente delle comunicazioni globali. La ridondanza tecnica esiste — quando un cavo si rompe, il traffico viene in gran parte reindirizzato su altre rotte, spesso in modo automatico e quasi impercettibile per l'utente finale. Questo è un argomento solido, e va riconosciuto senza sconti: il sistema, finora, ha dimostrato una capacità di assorbire i singoli incidenti superiore a quanto un osservatore esterno potrebbe immaginare guardando solo i titoli dei giornali dopo un sabotaggio.

Ma «ha sempre retto» non è la stessa cosa di «reggerà sempre». La concentrazione della proprietà nelle mani di poche aziende (Capitolo 2), la densità di cavi in pochissimi punti di strozzatura geografici (Capitolo 3), gli incidenti che si sono moltiplicati proprio negli ultimi anni nel Mar Baltico e nel Mar Rosso (Capitolo 4) sono tendenze recenti, non costanti storiche. Il fatto che il sistema abbia retto finora dice poco su quanto reggerà di fronte a scenari che, fino a pochi anni fa, erano considerati remoti — un conflitto aperto in una delle aree di massima concentrazione di cavi, per esempio.

«Le grandi aziende tecnologiche investono i loro soldi, hanno tutto l'interesse a proteggere l'infrastruttura»

Anche questo è vero, ed è un argomento che merita rispetto: nessuna azienda che investe miliardi in un cavo sottomarino ha interesse a vederlo danneggiato, e la proprietà privata di un'infrastruttura non implica automaticamente negligenza nella sua manutenzione. Le grandi aziende tecnologiche che possiedono quote crescenti della rete di cavi (Capitolo 2) hanno, sul piano puramente tecnico, ogni incentivo a mantenerla efficiente.

Il punto sollevato in questo libro, però, non riguarda la manutenzione tecnica, ma il controllo. Un'azienda privata che possiede un cavo decide, secondo la

propria logica commerciale, dove instradare il traffico, quali paesi collegare in via prioritaria, a quali condizioni concedere l'accesso — decisioni che, come mostrato nel Capitolo 8, hanno sempre più spesso ricadute geopolitiche che vanno ben oltre l'interesse della singola azienda. Un'infrastruttura essenziale al pari dell'energia elettrica o dell'acqua, ma governata prevalentemente secondo logiche di mercato private, pone una domanda legittima sul chi decide, indipendentemente da quanto bene quell'infrastruttura venga materialmente mantenuta.

«Parlare di sorveglianza sui cavi è dietrologia, i governi devono pur difendersi da minacce reali»

Le due cose non si escludono a vicenda. Che i governi abbiano legittime esigenze di sicurezza e intelligence è un fatto che nessuno, in questo libro, ha messo in discussione. Il caso Tempora raccontato nel Capitolo 6, però, non riguarda un'intercettazione mirata su sospetti specifici legata a una minaccia concreta: riguarda, per stessa ammissione dei documenti resi pubblici, la raccolta indiscriminata di comunicazioni di milioni di persone senza alcun sospetto a loro carico — un fatto giudicato illegale due volte dalla Corte Europea dei Diritti dell'Uomo, l'ultima delle quali dalla sua Grande Camera, il grado di giudizio più alto disponibile. Non è dietrologia riportare una sentenza

definitiva di un tribunale internazionale; è cronaca giudiziaria.

«Un trattato del 1884 non può essere davvero il quadro legale di riferimento oggi»

Su questo punto non c'è obiezione da controbattere: è semplicemente vero, ed è uno dei problemi più concreti descritti in questo libro. Il capitolo successivo affronta proprio la domanda su cosa si potrebbe fare per aggiornare un quadro normativo che, per sua stessa ammissione degli esperti del settore, non è mai stato pensato per un mondo in cui il 99% delle comunicazioni globali dipende da quei cavi.

Capitolo 11 — Cosa si potrebbe cambiare

Aggiornare un trattato vecchio 140 anni

Il punto di partenza più concreto è anche il più semplice da enunciare: la Convenzione di Parigi del 1884, che ancora oggi resta il principale riferimento internazionale per la protezione dei cavi sottomarini (Capitolo 11 della ricerca, richiamato più volte in questo libro), è stata scritta per un mondo di cavi telegrafici, non per un'infrastruttura da cui dipende il 99% delle comunicazioni digitali del pianeta. Diversi esperti internazionali di diritto marittimo e diversi governi — tra cui,

negli ultimi anni, gli stessi paesi nordici colpiti dai sabotaggi nel Mar Baltico raccontati nel Capitolo 4 — hanno chiesto l'apertura di negoziati per un trattato aggiornato, con regole più chiare su cosa costituisce sabotaggio, su come attribuire la responsabilità di un danno, e su quali strumenti di deterrenza e sorveglianza congiunta gli stati possano legittimamente adottare per proteggere questa infrastruttura condivisa.

Più trasparenza sulla proprietà

Una parte consistente dei problemi descritti in questo libro — dalla concentrazione nelle mani di poche aziende tecnologiche (Capitolo 2) ai casi di cavi bloccati per motivi di sicurezza nazionale (Capitolo 8) — sarebbe più facile da valutare pubblicamente se esistessero registri obbligatori e realmente accessibili su chi possiede ogni singolo cavo, chi ne gestisce il traffico, e con quali accordi contrattuali. Oggi gran parte di queste informazioni è dispersa tra documenti societari, autorizzazioni nazionali frammentate e comunicati stampa aziendali, ricostruibile solo con un lavoro di ricerca lungo come quello alla base di questo libro. Una trasparenza sistematica, imposta per legge, non cambierebbe la proprietà dei cavi, ma renderebbe visibile — a giornalisti, ricercatori, parlamenti nazionali — ciò che oggi resta in gran parte invisibile.

Investimento pubblico europeo in infrastrutture proprie

L'Unione Europea, che ospita alcuni dei punti di atterraggio più densi al mondo (Marsiglia, Londra fino alla Brexit, i grandi hub di scambio di Francoforte e Amsterdam raccontati nel Capitolo 7), dipende ancora in larga parte da cavi posseduti o co-posseduti da aziende extraeuropee. Diversi analisti e alcune istituzioni europee hanno cominciato a discutere, negli ultimi anni, la possibilità di sostenere con investimento pubblico congiunto la costruzione di cavi strategici a proprietà europea o a partecipazione pubblica, sul modello di quanto già avviene per altre infrastrutture critiche come le reti elettriche transfrontaliere. Non si tratta di un'ipotesi già realizzata su larga scala, ma di una direzione di policy discussa apertamente in sede europea negli anni recenti, proprio a partire dai casi di sabotaggio nel Baltico.

Protocolli di riparazione più rapidi e condivisi

Uno degli elementi meno raccontati dai titoli dei giornali, ma centrale per la resilienza reale del sistema, riguarda la capacità pratica di riparazione: nel mondo esiste un numero limitato di navi specializzate in grado di riparare un cavo danneggiato sul fondale oceanico, e la loro disponibilità è già oggi un collo di bottiglia nei momenti di maggiore domanda. Rafforzare — con finanziamenti pubblici o accordi multilaterali

tra stati e aziende — la flotta di navi posacavi e riparazione disponibile in ogni area geografica critica, in particolare nel Mar Baltico e nel Mar Rosso, è una misura concreta già proposta da diversi governi europei dopo gli incidenti raccontati nel Capitolo 4, e non richiede di risolvere prima le questioni più complesse di proprietà o governance internazionale.

Nessuna di queste soluzioni, da sola, elimina il rischio

Vale la pena dirlo con chiarezza, per onestà verso chi legge: nessuna delle misure descritte in questo capitolo elimina del tutto la vulnerabilità strutturale raccontata in questo libro. Un'infrastruttura fisica concentrata in poche centinaia di cavi e in un numero ancora più ristretto di punti di strozzatura geografici resterà, per la sua stessa natura tecnica, un bersaglio possibile. L'obiettivo realistico di queste proposte non è l'invulnerabilità, ma la riduzione del rischio e — soprattutto — una maggiore trasparenza su un sistema da cui dipende, ogni giorno, la vita digitale di miliardi di persone che, nella grande maggioranza dei casi, ne ignorano completamente l'esistenza.

Capitolo 12 — Cosa puoi fare tu, adesso

Informarti su dove passano davvero i tuoi dati

Esistono mappe pubbliche, aggiornate e liberamente consultabili online, che mostrano il tracciato dei principali cavi sottomarini del mondo e chi li possiede — gli stessi strumenti usati per la ricerca alla base di questo libro. Dedicare anche solo qualche minuto a guardare quella mappa, e a capire da quali cavi e da quali paesi passano le comunicazioni che usi ogni giorno, è il primo passo per smettere di considerare internet come una «nuvola» astratta, come raccontato nel Capitolo 1, e cominciare a vederla per quello che è davvero: un'infrastruttura fisica, concentrata, con proprietari precisi.

Sostenere il giornalismo che segue questi temi

Le vicende raccontate in questo libro — dai sabotaggi nel Mar Baltico ai cavi tagliati nel Mar Rosso, dal caso PLCN alle rivelazioni Snowden — sono diventate pubblicamente note grazie al lavoro di giornalisti investigativi, ricercatori indipendenti e organizzazioni per i diritti digitali che seguono con continuità un tema tecnico, poco spettacolare e spesso trascurato dai grandi media generalisti. Sostenere — con un abbonamento,

con la semplice lettura e condivisione dei loro articoli — le testate e i ricercatori che continuano a monitorare questo settore è un modo concreto per mantenere alta l'attenzione pubblica su un'infrastruttura che, per sua natura, tende a restare invisibile finché non si rompe.

Chiedere trasparenza alle istituzioni, non solo alle aziende

Molte delle decisioni raccontate in questo libro — dal blocco del segmento Hong Kong del cavo PLCN alle discussioni europee su un nuovo trattato per la protezione dei cavi — vengono prese da autorità pubbliche, nazionali o europee, spesso con scarsissima copertura mediatica e nessun dibattito pubblico preventivo. Seguire il lavoro delle commissioni parlamentari nazionali ed europee competenti in materia di telecomunicazioni e sicurezza digitale, e segnalare ai propri rappresentanti eletti l'interesse per una maggiore trasparenza su questi temi, è un'azione concreta alla portata di qualunque cittadino, anche senza competenze tecniche specifiche.

Non credere alla prima spiegazione, e nemmeno all'ultima

Come mostrato più volte in questo libro — nel caso del Balticconnector nel 2023, in quello dei cavi Yi Peng 3 nel 2024, in quello dei cavi tagliati nel Mar Rosso nel 2024 — la causa reale di un incidente su un cavo sottomarino è quasi sempre più incerta e più lenta da

accertare di quanto suggeriscano i titoli dei giornali nelle prime 24 ore. La lezione pratica per chi legge notizie su questi temi è la stessa applicata nella ricerca di questo libro: distinguere sempre, con attenzione, i fatti accertati dalle ipotesi, per quanto plausibili, ancora non confermate — un esercizio di prudenza che vale per i cavi sottomarini come per qualunque altra notizia complessa.

Nota sulla trasparenza nell'uso dell'intelligenza artificiale

Questo libro è stato scritto con il supporto di strumenti di intelligenza artificiale, usati per la ricerca preliminare delle fonti, la prima stesura dei testi a partire da una scaletta e da indicazioni editoriali definite dall'autore, e la revisione linguistica e strutturale.

Restano interamente umane: la scelta del tema e la tesi del libro, la verifica di ogni fatto, cifra e citazione contro una fonte primaria o istituzionale prima della pubblicazione, la decisione editoriale finale su cosa viene pubblicato o corretto, e la responsabilità editoriale dei contenuti — che resta in capo all'autore, mai allo strumento di intelligenza artificiale utilizzato.

Questa nota risponde agli obblighi di trasparenza previsti dall'art. 50 del Regolamento (UE) 2024/1689 (AI Act), applicabile dal 2 agosto 2026.

Se trovi un errore, una fonte imprecisa o un'affermazione che ritieni non verificata correttamente, scrivi a redazione@contropotere.com — ogni segnalazione fondata porta a una correzione pubblica del testo. Questo libro fa parte della collana **Contropotere**: gli altri titoli sono disponibili gratuitamente su **contropotere.com**.