



AWARE

Aprile 2022

I cavi sottomarini come infrastruttura critica

Rischi, trend e opportunità per l'Italia

AUTORI

Luigi Lo Porto
Marco Baticci

CURATORI

Edoardo Crivellaro
Alice Grieco
Alessia Baccani

SI RINGRAZIA

Alessandro Passamonti
Mariagabriella Cantone
Svetlana Falconi

INDICE

Introduzione	p.1
1. Cavi sottomarini: storia e regolazione	p.2
1.1 La storia	p.2
1.2 La regolazione del settore	p.5
1.3 Cosa ci insegna la storia?	p.8
2. I rischi	p.10
2.1 Una infrastruttura critica	p.10
2.2 Hybrid warfare	p.15
2.3 Cybersecurity	p.17
2.4 Terrorismo	p.18
2.5 Danno accidentale	p.19
2.6 Spionaggio	p.21
3. Cavi sottomarini tra economia e geopolitica	p.22
3.1 L'economia dei cavi	p.24
3.2 Geopolitica dei cavi sottomarini	p.28
4. Il caso italiano	p.31
4.1 Mitigazione dei rischi	p.31
4.2 Valorizzazione delle opportunità	p.34
Bibliografia	p.36
Contatti	

ABSTRACT

Oltre il 95% del traffico dati e voce avviene tramite cavi sottomarini, infrastrutture della larghezza di un tubo da giardino posate sui fondali marini. Ciò li rende innegabilmente un'infrastruttura strategica oltre che un trampolino di lancio per la *gigabit society*.

La storia dei cavi sottomarini è indissolubilmente legata alle contestuali evoluzioni geopolitiche. La nascita di questa infrastruttura, infatti, è legata alla politica dell'Impero britannico di metà XIX secolo, mentre il suo sviluppo si è concretizzato sotto la globalizzazione di stampo statunitense nel secondo dopoguerra. Nel passato più recente, i cavi sono stati oggetto della regolamentazione internazionale, nonostante questa presenti ancora molte lacune in tema (derivanti sia dalla natura del diritto internazionale stesso, sia dalle norme in esso contenuto).

Dal lato economico, un profondo cambiamento nel modello di business è in atto. Infatti, se prima questo si basava su consorzi di imprese di telecomunicazione interessate alla spartizione sia degli elevati costi sia della *capacity* del cavo, **il settore si muove oggi verso una concentrazione caratterizzata dalla preminenza delle compagnie Big-Tech e della loro necessità di un'ingente mole di dati.**

Il rapporto fra tecnologie e politica ha fatto poi in modo che questa infrastruttura non si sia potuta sottrarre alle dinamiche geopolitiche recenti (tra tutte, quella Cina - Stati Uniti). Se è vero che i cavi oggi vengono posati per puro interesse economico, è egualmente importante notare come le minacce ai cavi, l'importanza dei dati ivi transitanti e la rilevanza di queste infrastrutture per le ambizioni politico-economiche, rendano la politica e gli Stati attori cruciali nei processi di manifattura, posa e operatività dell'infrastruttura.

Per comprendere tali dinamiche, è quindi di primaria importanza stimare la rilevanza di questa infrastruttura per la nostra economia e la nostra società. In secondo luogo, è fondamentale delineare alcune delle principali minacce che incombono su tale infrastruttura, quali *l'hybrid warfare*, i cyber-attacchi, il terrorismo, il danno accidentale e lo spionaggio.

Questo paper si occuperà di analizzare i suddetti elementi per poi approdare alla ricerca di un approccio che massimizzi le opportunità e mitighi le vulnerabilità per il sistema-paese Italia all'interno del quadro europeo e mediterraneo.

INTRODUZIONE

Con una larghezza massima pari a quella di un tubo da giardino e una struttura rimasta immutata per anni, i circa 436 cavi sottomarini di lunghezza complessiva pari a circa 1.3 milioni di km (1) rappresentano l'intelaiatura fondamentale del sistema di telecomunicazione e trasmissione dei dati nel mondo. **Nonostante si ritenga oggi che gran parte del traffico di dati e voce avvenga tramite satelliti, almeno il 95% (2) avviene, invece, tramite queste infrastrutture che giacciono sui fondali marini.** Inoltre, oltre 10 trilioni di transazioni finanziarie vengono effettuate giornalmente per mezzo di queste infrastrutture. Obiettivo principale di questo paper è quello di sottolineare la rilevanza del sistema-paese Italia in questo mercato e proporre a tal proposito delle politiche mirate alla valorizzazione del settore.

Per arrivare a tali proposte, il lavoro percorrerà delle tappe preliminari. La prima parte è costituita da una breve introduzione storica che consente di fornire al lettore una panoramica sull'evoluzione dell'infrastruttura dei cavi sottomarini. Quando sono stati posati e perché? Che traiettorie seguono? Sono tutte domande fondamentali a cui si cercherà di rispondere per inquadrare il dibattito e capire meglio la posizione italiana. Successivamente, ci si concentrerà sulle vulnerabilità di questa infrastruttura, l'altra faccia della medaglia delle sue opportunità. Tramite questa elencazione ci avvieremo, nell'ultima parte, a rispondere all'ultima domanda, fondamentale per decifrare le possibilità d'azione dell'Italia: quella del "chi". È importante cercare di capire chi costruisce, chi posa, chi possiede, chi mantiene e chi sorveglia i cavi sottomarini. Si scoprirà che il mercato dei cavi non è "piatto", ma è "una macchina di conflitti" (3): dietro le apparenti scelte autonome delle imprese del settore intervengono infatti le *longae manus* dei governi desiderosi di proteggere, governare e valorizzare tale infrastruttura critica. Infine, sarà analizzato il caso specifico dell'Italia, indagando il come approcciare questa infrastruttura al fine di minimizzarne le vulnerabilità e coglierne le potenzialità.

(1) Telegeography. Submarine Cable Frequently Asked Questions. <https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions>

(2) Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans – Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC.

(3) Aresu, A. (2020). Le potenze del capitalismo politico. Stati Uniti e Cina. La Nave di Teseo

1. CAVI SOTTOMARINI: STORIA E REGOLAZIONE

1.1 La storia

Un punto di partenza da tenere a mente, che sarà utile a inquadrare e comprendere meglio le dinamiche attuali descritte nelle parti finali di questo lavoro, è che **la storia dei cavi sottomarini è legata alle contestuali evoluzioni geopolitiche**. Al pari di molte altre infrastrutture, la loro principale funzione di collegamento tra vari nodi del sistema internazionale (piuttosto che tra vari punti dello stesso nodo/paese) li ha resi infatti intrinsecamente coinvolti nella natura dialogica di quest'ultimo, caratterizzata tanto da cooperazione quanto da conflitti.

La data di nascita che convenzionalmente viene attribuita ai cavi sottomarini è il **28 agosto 1850**, quando fu depositato un cavo telegrafico sul fondale del Canale della Manica, tra Dover e Calais. La data non dovrebbe sorprendere: la seconda rivoluzione industriale era in pieno decollo sulla scia delle scoperte elettriche di personalità come Morse negli Stati Uniti e Faraday, Cooke e Wheatstone nel Regno Unito (4). Ciò che egualmente non dovrebbe sorprendere è inoltre il luogo e gli attori coinvolti. Il cavo, depositato dal piroscampo a vapore *Goliath*, fu finanziato dai fratelli John e Jacob Brett, i quali costituirono per l'occasione la "English Channel Submarine Telegraph Company". La manifattura del cavo fu affidata alla "Gutta Percha Company", azienda specializzata nell'utilizzo della neoscoperta guttaperca, con ottime proprietà isolanti. Il cavo durò appena pochi giorni prima di essere danneggiato, ma diede il via a una diffusione generalizzata dell'industria.

Le imprese coinvolte si espansero vertiginosamente in stretta connessione con la politica del Regno Unito, che in quegli anni consolidava la posizione imperiale che avrebbe mantenuto fino alla fine del primo conflitto mondiale. In breve tempo, **i cavi divennero una questione quasi esclusiva del capitalismo politico britannico**: a cento anni dal cavo dei fratelli Brett, il 90% dei circa 470 mila km di cavi esistenti era stato costruito a Londra e l'82% solo da una compagnia: la Telegraph Construction & Maintenance Company (Telcon) (5), nata dalla fusione tra la "Gutta Percha Company" e la "Glass, Elliot & Company", un'altra impresa manifatturiera del settore.

(4) McGillem, C. D. (2020, March 2). telegraph. Encyclopedia Britannica.
<https://www.britannica.com/technology/telegraph>

(5) Burnett, D. R., Beckman, R., & Davenport, T. M. (Eds.). (24 Oct. 2013). Submarine Cables. Leiden, The Netherlands: Brill | Nijhoff. doi: <https://doi.org/10.1163/9789004260337>

Se si dovesse ricercare una personalità simbolo dell'espansione capillare dei cavi sottomarini, la scelta ricadrebbe proprio su **John Pender**, primo presidente della neonata compagnia. Partendo dalla posa del primo cavo transatlantico nel 1865 proprio con la Telcon, John Pender dedicò la sua carriera ad un unico obiettivo: connettere l'Impero britannico, facilitandone, così, il mantenimento e la sopravvivenza (6). Non senza l'aiuto dei suoi stretti legami con la politica britannica (siede a Westminster dagli anni Sessanta del secolo) fondò 32 compagnie ognuna incaricata della stesura di cavi nei quattro angoli del globo. All'inizio pensate come indipendenti, tali compagnie presero presto il nome di **"Eastern Telegraph Company"**, compagnia che divenne poi di fatto monopolista nella stesura di cavi.



**Rete di cavi nel 1901: da notare la centralità britannica
(A.B.C. Telegraphic Code 5th Edition)**

Attraverso la strategia *"all-red"* (dove i punti di approdo dei cavi erano tutti su territorio britannico), un controllo degli stretti (vedi l'occupazione dell'Egitto nel 1882, che garantì il controllo di Suez) e il pattugliamento della Royal Navy a garantire l'integrità dell'infrastruttura (7), il mondo divenne collegato perché **"l'Impero dove non tramonta il sole" lo era: i cavi erano lo scheletro della prima globalizzazione.**

(6) Headrick D.R (1981) *The Tools of Empire. Technology and European Imperialism in the Nineteenth Century*, New York, Oxford: Oxford University Press, p. 163.

(7) Kennedy, P. M. (1971). Imperial Cable Communications and Strategy, 1870-1914. *The English Historical Review*, 86(341), 728-752. <http://www.jstor.org/stable/563928>

In seguito all'avvento della radio, l'industria telegrafica subì notevoli perdite. Ciò costrinse, nel 1929, alla fusione della Eastern Associated Companies di Pender con la Wireless Telephone Company di Marconi, dando vita alla Cable & Wireless (sopravviverà fino al 2021). Inoltre, dal lato manifatturiero, tale evento costrinse la Telcon a fondersi con il suo principale competitor: la tedesca Siemens, la prima a tentare di scalzare il monopolio britannico.

Mentre il mondo delle telecomunicazioni entrava nell'era del telefono, un altro attore si affacciava sulla scena: gli Stati Uniti. Mentre oltreoceano, già da tempo, si paventava l'idea di rendersi indipendenti dalla **"cavocrazia"** di Londra (8), questa esigenza si fece più urgente con l'avvento della Seconda Guerra Mondiale che segnerà, di fatto, la definitiva uscita degli USA dal suo secolare isolazionismo. Infatti, il **26 dicembre 1941**, appena tre settimane dopo Pearl Harbor, il governo australiano acconsentì a un ponte radio diretto tra Sidney e San Francisco (9). In due anni gli Stati Uniti erano connessi direttamente in quasi tutto il mondo, da lì in poi tale posizione dominante si concretizzerà anche tramite l'infrastruttura di cavi. Il rapido sviluppo dei satelliti fece perdere importanza ai cavi telefonici/coassiali degli anni '70, ancora a banda non abbastanza larga e troppo costosi per percorrere lunghe distanze, per cui dovevano essere installati numerosi ripetitori. Con l'arrivo della **fibra ottica**, tuttavia, la situazione si volse di nuovo in favore dei cavi. Tale tecnologia, implementata per la prima volta nel 1979, dimostrò di essere resistente agli stress e di garantire stabilità e velocità. **I cavi consolidarono il primato di infrastruttura fondamentale per le telecomunicazioni moderne via Internet e tuttora lo mantengono.**

La manifattura dei cavi si è nel tempo diversificata lungo la sua catena del valore, ora ai vertici delle classifiche ci sono ora aziende francesi, svizzere, giapponesi e cinesi. Tuttavia, dalla metà degli anni '80 in poi, ciò che è rimasto simile alla situazione nell'era telegrafica è la sostanziale egemonia americana nei tre già menzionati ruoli che esercitava il Regno Unito: controllo e messa in sicurezza degli stretti in cui passano molti cavi, pattugliamento delle rotte e punti di approdo. Le opportune mutazioni di contesto sono necessarie: questi ultimi non si trovano più in colonie, ma, per la maggior parte, in Paesi alleati la cui politica estera è comunque subordinata (laddove non completamente delegata) a quella di Washington.

(8) Aresu, A (2019). Gli Imperi dei Cavi Sottomarini. Limes, rivista italiana di geopolitica, 9/2019.

(9) Headrick D.R (1991) The Invisible Weapon: Telecommunications and International Politics, 1851-1945, New York, Oxford: Oxford University Press, p. 262

1.2 La regolazione del settore

L'industria dei cavi sottomarini ha dato poi vita all'International Cable Protection Committee (ICPC), organizzazione che raggruppa oltre 180 entità (statali e non) in tutto il mondo e lungo l'intera catena del valore del settore. **Circa il 98% dell'infrastruttura è operata o posseduta da membri dell'ICPC.** L'organizzazione agisce come un vero e proprio gruppo di interesse, curandosi di affari istituzionali e contribuendo inoltre a formare degli standard di operazione nel settore.

Dalla fine '800 alla fine '900 la comunità internazionale ha adottato quattro diverse convenzioni che concernono i cavi sottomarini:

1. **La Convenzione per la Protezione dei Cavi Sottomarini Telegrafici del 1885.**
2. **La Convenzione di Ginevra sull'Alto Mare del 1958.**
3. **La Convenzione di Ginevra sulla Piattaforma Continentale del 1958.**
4. **La Convenzione delle Nazioni Unite sul Diritto del Mare di Montego Bay (UNCLOS), 1982.**

Naturalmente, come spesso capita per tali legislazioni, la normativa internazionale concernente i cavi sottomarini può, al giorno d'oggi, quasi completamente riferirsi alla più recente Convenzione di Montego Bay e sarà ciò su cui ci si soffermerà. Le norme della Convenzione riguardo i cavi possono essere raggruppate in tre aree: quelle riguardanti le operazioni di **messa in posa e riparazione** di cavi, quelle riguardanti la loro **protezione** e quelle riguardanti la **risoluzione di controversie**. È bene ricordare che, sebbene il diritto internazionale si rivolga agli Stati, le norme che si rivolgono ai cavi sottomarini si riferiscono nella prassi anche alle persone (fisiche o giuridiche) della nazionalità dello Stato a cui è imposto l'obbligo o il diritto (10).

Per quanto riguarda le operazioni di rilevamento topografico delle potenziali rotte, la posa dei cavi e la loro riparazione, gli Stati costieri sono soggetti a obblighi e diritti diversi a seconda di dove, tra i tre principali "livelli" marini individuati dalla Convenzione (*acque territoriali/interne, zone economiche esclusive/piattaforme continentali, acque internazionali*), si svolgono tali operazioni.

(10) Nordquist et al. (eds.), United Nation on the Law of the Sea 1982: Commentary, volume III (martinus nijhoff publishers, 1995), (nordquist et al., vol III, 1995), p. 264.

Per quanto riguarda le prime zone di **sovranità nazionale esclusiva**, la norma più specifica in materia si riferisce all'inserimento delle attività di rilevamento del fondale tra quelle che possono pregiudicare la definizione di "passaggio inoffensivo" in acque territoriali (*art. 19.2.j*) e che quindi garantiscono l'autorità dello Stato costiero di regolare tali operazioni, autorità che si estende poi nell'*art. 21* all'intera categoria di "protezione di cavi e tubi".

La questione si complica quando si passa alla regolazione nelle **Zone Economiche Esclusive** (ZEE) e nelle Piattaforme Continentali. Nelle ZEE, secondo gli *articoli 58 e 87*, vige la libertà per *tutti* gli Stati, costieri o meno, di posa dei cavi sottomarini e di tutte le operazioni associate. L'*articolo 79* prevede più o meno gli stessi diritti per le piattaforme continentali. Tuttavia, nell'esercizio di queste operazioni, secondo l'*articolo 79*, gli Stati devono prestare attenzione ai cavi già esistenti e non pregiudicare le possibilità di riparazione. Inoltre, devono prestare attenzione ai diritti e i doveri dello Stato costiero a cui la ZEE/piattaforma afferisce (in breve, si tratta di esplorazione e sfruttamento di risorse in tali aree). Se gli *articoli 58 e 79* lasciano un margine di spazio alla sovranità nazionale su tali aree nell'affermare che gli Stati operanti in tali zone, pur nella loro garantita libertà, devono rispettare le leggi degli Stati costieri, tali leggi si riducono sostanzialmente alle "misure ragionevoli per l'esplorazione della piattaforma continentale e lo sfruttamento delle sue risorse naturali" indicate nell'*articolo 79.2*, ma la cui definizione resta molto vaga, soprattutto nel concetto di "ragionevolezza" e il cui spazio di manovra viene comunque attenuato dal divieto (*must not*) di interferenza nelle libertà degli altri Stati (*art.78.2*). A nostro avviso, ciò che emerge da questo intricato groviglio di norme in materia, è la possibile equivalenza tra la regolazione dei cavi sottomarini per le telecomunicazioni in queste zone e il mare aperto, considerando la difficoltà di trovare un qualsiasi tipo di collegamento tra le funzioni che questi svolgono e i diritti degli stati costieri di sfruttamento delle risorse nelle Zone Economiche Esclusive e nella piattaforma continentale.

L'*articolo 87* sancisce la libertà del mare aperto, specificando al *comma 1, lettera c*, proprio la libertà di posa di cavi sottomarini; è affiancato dall'*articolo 112*, dove tale libertà è vincolata soltanto dal non pregiudizio dei cavi già esistenti e le operazioni a essi riferite.

La Convenzione garantisce agli Stati il diritto di attuare norme a protezione dei cavi dai possibili danni. Oltre al già citato diritto per gli Stati costieri di adottare leggi e regolamenti riguardo ai cavi nelle loro acque territoriali, gli *articoli dal 113 al 115* trattano della protezione dei cavi sottomarini nelle restanti zone marittime.

L'*articolo 113* richiede che gli Stati adottino norme che si assicurino che il danneggiamento di un cavo da parte di una nave battente la loro bandiera nazionale sia un'offesa punibile. L'*articolo 114* richiede che gli Stati adottino normative che riguardino la responsabilità dei connazionali proprietari dei cavi per i costi di riparazione di cavi danneggiati nel corso di operazioni di posa o riparazione. L'*articolo 115* sostiene che ogni Stato *dovrebbe* adottare leggi o regolamenti per lo stabilimento di un'indennità che i proprietari dei cavi dovrebbero pagare agli armatori per eventuali danni o perdite risultanti in una nave che tentava di evitare il danno di un cavo.

Per quanto riguarda la risoluzione di controversie, Burnett, Beckman e Davenport (11) sottolineano, giustamente, come la posa e il mantenimento dei cavi sottomarini godano del più alto livello di protezione all'interno del sistema di risoluzione di controversie previsto dalla Convenzione nella *parte XV*, facendovi rientrare le dispute concernenti: sia l'interpretazione delle norme della Convenzione riguardanti l'esercizio di uno Stato costiero dei suoi diritti sovrani, sia la possibilità che uno Stato costiero abbia agito in contravvenzione alle norme sulle operazioni dei cavi. Per esempio, uno Stato potrebbe presentare istanza contro un altro Stato qualora quest'ultimo abbia imposto eccessive regolamentazioni sulla posa dei cavi nella sua ZEE. Naturalmente, tale sistema soffre di tutti i *vulnus* di cui soffre il diritto internazionale ovvero: l'impossibilità dei privati di appellarsi direttamente a tale sistema e discussa efficacia dell'enforcement di tali norme. Nella pratica, infatti, **la politica regna sovrana sul tema e il settore manca di una vera e propria cristallizzazione normativa**, soprattutto se a mancare è il riconoscimento politico della Convenzione di Montego Bay da parte degli Stati Uniti.

In ogni caso, aldilà della dibattuta efficacia del diritto internazionale in sé, la normativa in materia è criticata proprio dal punto di vista contenutistico. L'attuale Cancelliere dello Scacchiere Rishi Sunak, in un paper (12) del 2017, evidenzia come le norme dell'UNCLOS siano deficitarie. La Convenzione, infatti, non impedisce agli Stati di trattare i cavi sottomarini come bersagli legittimi in guerra, il già menzionato articolo 113 (oltre a mancare di un'estensiva applicazione tra gli Stati firmatari) non conferisce alle navi militari un diritto "preventivo" di investigazione su imbarcazioni sospettate di danneggiamento, *"rendendo difficili le operazioni di deterrenza per le potenze navali"* (13). In sostanza, conclude Sunak, la protezione internazionale dell'infrastruttura sembra ancora confinata al ruolo prettamente periferico che i cavi svolgevano negli anni dell'adozione della Convenzione.

(11) Burnett, D. R., Beckman, R., & Davenport, T. M. (Eds.). (24 Oct. 2013). *Submarine Cables*. Leiden, The Netherlands: Brill | Nijhoff. doi: <https://doi.org/10.1163/978900426033>

(12) Sunak, Rishi. «Undersea Cables, Indispensable, insecure». Policy Exchange, 2017, p.16

(13) Ibid., pg.17

1.3 Cosa ci insegna la storia?

Per un'appendice storica più dettagliata, si rimanda ai testi citati come fonte. In questa sede, l'obiettivo è di fornire al lettore una panoramica di come tale infrastruttura, tanto cruciale anche ai giorni nostri, sia nata da un rapporto dialettico tra imprese e governi. Non è un segreto che gran parte delle innovazioni tecnologiche sia nato da fini politici (14) (anzi, più spesso imperiali) e, come è noto, l'intelaiatura globale di cavi era fondamentale per la tenuta dell'impero britannico. Alla dissoluzione di quest'ultimo, tuttavia, le infrastrutture sono rimaste e, mentre continuavano a svolgere la funzione di connessione dei centri nevralgici del sistema internazionale in evoluzione, non si sono potute sottrarre alle nuove dinamiche geopolitiche.

Queste, già nella prima metà del Novecento, erano chiaramente mutate dall'epoca che lo storico Eric Hobsbawm chiama l'età degli Imperi: il post Seconda guerra mondiale, l'ascesa statunitense e, in seguito, la contrapposizione con l'URSS contribuirono a creare una scacchiere internazionale all'apparenza formato da pari ma in realtà fortemente gerarchico, sebbene in forme diverse dal passato. La rete chiamata "*globalizzazione*", che si dispiegherà in maggior misura con impeto dopo il crollo del rivale sovietico, non può essere considerata come indipendente dalla vittoria di Washington, che oggi consolida la sua egemonia anche tramite la forza del *World Wide Web* che su quei cavi sottomarini viaggia.

A tal proposito, è opportuna una precisazione: i cavi di oggi vengono posati per puro interesse economico dai giganti delle telecomunicazioni e del tech di tutto il mondo. Non c'è una riunione in una stanza del Pentagono ogni volta che Google decide di costruire un cavo. Tuttavia, l'attenzione della politica si desta quando tale cavo viene minacciato, quando le risorse (i dati) che lo attraversano possono essere utili o sensibili o quando una potenza che cerca di aumentare la sua influenza regionale (o, perché no, globale) utilizza i cavi come trampolini di lancio infrastrutturali per le proprie ambizioni politico economiche (si veda la Cina con il progetto **PEACE**, un network di cavi che ambisce a collegare il Pakistan con l'Est Africa e l'Europa all'interno delle Nuove vie della Seta).

(14) A tal riguardo si rimanda alla lettura del best-seller mondiale di Yuval Noah Harari: *Sapiens*, che dedica un intero capitolo 15 (appunto chiamato il matrimonio tra scienza e imperi) alla questione

Acquisire consapevolezza delle relazioni tra politica e imprese in questo settore chiave è, quindi, fondamentale per immaginare una soluzione utile per il contesto italiano: quello dei cavi sottomarini, infatti, è terreno di **politica industriale**. Tale soluzione non può, infatti, ridursi a richiedere più investimenti per un settore senza che venga definito cosa e come il sistema Italia può trarre vantaggio dal settore dei cavi sottomarini, definizione che non può prescindere da un'analisi di contesto sull'infrastruttura: **cos'è e a cosa serve? Quali rischi e quali opportunità comporta? Quali sono i margini di manovra su tali rischi e opportunità?**

Questa e le seguenti parti del paper tentano di rispondere a queste domande.

2. I RISCHI

2.1 Una infrastruttura critica

I cavi sottomarini rappresentano l'infrastruttura abilitante delle nostre economie, delle nostre società e della nostra sicurezza, infatti, **all'interno di questi cavi transita circa il 95-99% del traffico Internet mondiale** (15).

Tali infrastrutture permettono di rispondere alla domanda, sempre più crescente, di trasmissione dati necessaria a gestire *manufacturing and supply chains* più complesse ed interconnesse. Difatti le aziende, soprattutto quelle internazionali, si affidano al *World Wide Web* per la propria connessione sia interna che esterna (16). Di conseguenza, la specializzazione delle economie globali e la loro crescita economica dipendono in gran parte dalla disponibilità di infrastrutture capaci di integrare la produzione nazionale in catene di creazione di valore globali (17).

I cavi sottomarini sono anche fondamentali nel settore della finanza; **è stimato che queste infrastrutture veicolino transazioni finanziarie giornaliere per un valore complessivo di oltre 10 trilioni di dollari** (18). Anche il network SWIFT si affida ai cavi in fibra ottica sottomarini per le proprie comunicazioni (19). Per il settore finanziario la *velocità delle trasmissioni* è di fondamentale importanza, infatti un ritardo di qualche secondo nella esecuzione di una transazione potrebbe costare milioni di dollari, e la perdita delle comunicazioni per qualche minuto potrebbe avere effetti catastrofici (20).

(15) Si veda: Francesco Bechis, «Undersea Cables: The Great Data Race Beneath the Oceans», Text, ISPI, 28 maggio 2021, <https://www.ispionline.it/en/pubblicazione/undersea-cables-great-data-race-beneath-oceans-30651>; Matteo Colombo, Federico Solfrini, e Arturo Varvelli, «Network Effects: Europe's Digital Sovereignty in the Mediterranean – European Council on Foreign Relations», ECFR (blog), 4 maggio 2021, <https://ecfr.eu/publication/network-effects-europes-digital-sovereignty-in-the-mediterranean/>; Valerio Francola e Gordon A. Mensah, «L'industria dei cavi sottomarini: qualche elemento introduttivo», ASTRID RASSEGNA (Laboratorio sull'Ecosistema Digitale Astrid, 2021);

(16) APEC Policy Support Unit, «Economic Impact of Submarine Cable Disruptions», 2012.

(17) Bryan Clark, «Undersea cables and the future of submarine competition», Bulletin of the Atomic Scientists 72, n. 4 (3 luglio 2016): 234–37, <https://doi.org/10.1080/00963402.2016.1195636>.

(18) Colombo, Solfrini, e Varvelli, «Network Effects».

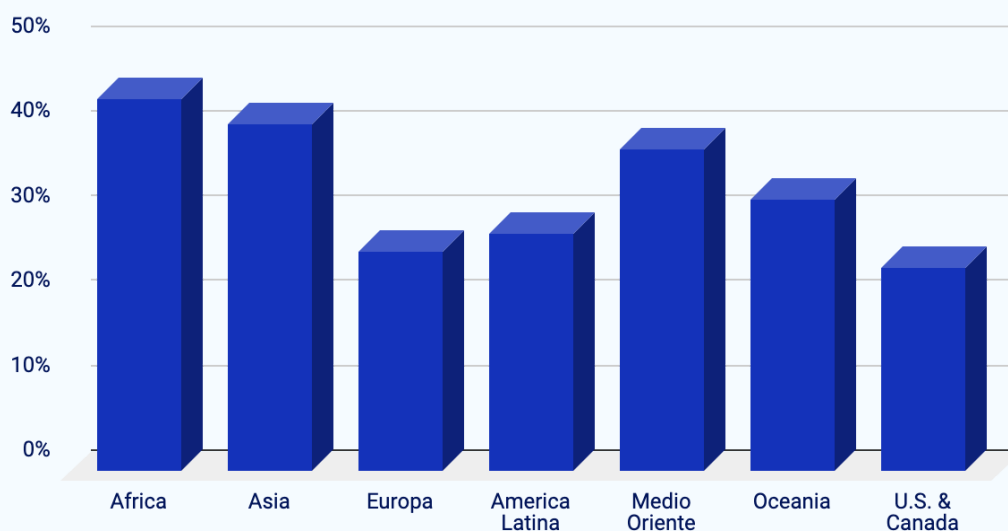
(19) APEC Policy Support Unit, «Economic Impact of Submarine Cable Disruptions».

(20) Clark, «Undersea cables and the future of submarine competition».

Considerando che maggiore è il numero di cavi a disposizione, più rapide saranno le comunicazioni e più rara l'ipotesi di una interruzione nelle comunicazioni, la messa in posa di cavi risulta essere cruciale (21). Nel periodo 2016-2020 sono stati messi in posa circa 67.000 chilometri di cavi sottomarini ogni anno (90.000 chilometri nel 2020) e si stima che, nel periodo 2021-2023, verranno messi in posa in media 113.000 chilometri di cavi ogni anno (22). **Questi cavi andranno a far parte di una rete che già si estende per oltre 1.3 milioni di chilometri.**

Inoltre, la dipendenza dai cavi è destinata ad aumentare se si tiene conto del crescente utilizzo di servizi cloud, video streaming, 5G, intelligenza artificiale e IoT, tutte tecnologie che richiedono un'alta intensità di larghezza di banda (23). Già nel 2012, infatti, APEC Policy Support Unit (24) stimava un *compound growth rate* della banda larga richiesta di circa il 40% annuo dal 2009 al 2018. I ritmi di crescita effettivamente realizzati sembrerebbero essere più bassi, ma tuttavia impressionanti. Il ritmo varia a seconda dell'area geografica di riferimento, con il continente africano ed asiatico in più vertiginosa crescita rispetto al continente europeo e nord-americano (25).

Tasso di crescita composto annuo 2015-2019



Fonte: Mauldin, Alan. 2019. «466 Tbps: The Global Internet Continues to Expand». 2019. <https://blog.telegeography.com/466-tbps-the-global-internet-continues-to-expand>.

(21) Colombo, Solfrini, e Varvelli, «Network Effects».

(22) Francola e Mensah, «L'industria dei cavi sottomarini: qualche elemento introduttivo».

(23) Christian Bueger e Tobias Liebetrau, «Protecting hidden infrastructure: The security politics of the global submarine data cable network», Contemporary Security Policy 42, n. 3 (3 luglio 2021): 391-413, <https://doi.org/10.1080/13523260.2021.1907129>.

(24) APEC Policy Support Unit, «Economic Impact of Submarine Cable Disruptions».

(25) Alan Mauldin, «466 Tbps: The Global Internet Continues to Expand», 2019, <https://blog.telegeography.com/466-tbps-the-global-internet-continues-to-expand>.

Altre tecnologie, quali le comunicazioni satellitari, seppur continuamente migliorate, non riescono al momento a fornire una valida alternativa ai cavi sottomarini in quanto più costose, meno efficienti e meno affidabili (26).

Fattore di confronto	Satelliti	Fibra in cavi sottomarini
Latenza	250 millisecondi	50 millisecondi
Vita media	10-15 anni	25 anni
Capienza	48.000 canali	160.000.000 canali
Costo dell'unità/mbps di capienza	737.316\$	14.327\$
Percentuale del traffico nel 1995	50%	50%
Percentuale del traffico nel 2014	0.4%	99.6%

Fonte: Spadaro Irene, e Pagnacco Anna., 2021. «Geostrategic value of submarine internet cables». Center for Cyber Security and International Relations Studies (CCSIRS).

La capacità di trasmettere, e processare, imponenti moli di dati è anche fondamentale per la **sicurezza nazionale** (27). Il danneggiamento dei cavi sottomarini ridurrebbe la capacità di comunicare con le operazioni militari all'estero; un esempio è stato il danneggiamento di tre cavi nel dicembre 2008 fra Italia e Egitto che ha ridotto dell'80% la connettività fra Europa e Medio Oriente (28). Tale evento pose seri problemi operativi per gli oltre 200.000 militari britannici ed americani in Iraq, i quali si affidavano alla infrastruttura dei cavi sottomarini commerciali per il 95% delle loro comunicazioni (29). Tali problemi operativi riguardarono soprattutto la U.S. Air Force la quale operava remotamente *unmanned aerial vehicles* (UAVs), i quali richiedevano 500 Mbps di banda larga per essere pilotati da remoto (30).

(26) Bueger e Liebetrau, «Protecting hidden infrastructure»; Clark, «Undersea cables and the future of submarine competition».

(27) Clark, «Undersea cables and the future of submarine competition».

(28) Rishi Sunak, «Undersea Cables, Indispensable, insecure» (Policy Exchange, 2017).

(29) Ibid.

(30) Ibid.

Inoltre, il ruolo dei dati assume sempre più importanza nel processo di *intelligence*, e *decision-making*, inoltre la digitalizzazione degli strumenti bellici causa un vertiginoso aumento dei dati a disposizione degli apparati di sicurezza. Non sorprende, dunque, che i siti di atterraggio e approdo dei cavi sottomarini siano stati inclusi dal U.S. State Department nell'elenco delle più critiche infrastrutture per gli Stati Uniti (31).

L'infrastruttura dei cavi sottomarini, per quanto fondamentale, risulta tuttavia essere fragile. Nonostante si affermi spesso che i cavi sottomarini operino ad una affidabilità "*cinque nove*", vale a dire del 99,999%, le interruzioni sono in realtà un fenomeno frequente a causa dell'estensione complessiva dell'infrastruttura (32). Infatti è stato osservato che, in media, nel Mondo **si rompa un cavo ogni tre giorni** (33). A tal proposito l'International Cable Protection Committee (ICPC) ha stimato il costo orario delle interruzioni delle comunicazioni sottomarine, che si attesta a 1,5 milioni di dollari (34). Assumono importanza, di conseguenza, eventi come il terremoto di Taiwan del 2006 durante il quale ben 9 cavi furono danneggiati, gli effetti furono avvertiti in tutto il Sud-Est asiatico per settimane, con oltre *seicento gigabytes di capacità offline* e l'interruzione del trading del Won Coreano (35).

Anche nel caso di Paesi ben collegati all'infrastruttura globale, la rottura di pochi cavi potrebbe causare molteplici complicazioni. Uno studio condotto sull'India, ad esempio, ha concluso che, seppure il Paese sia ben collegato, la rottura di soli tre cavi contemporaneamente causerebbe la perdita di oltre il 70% del suo traffico dati (36). Se finora si è parlato esclusivamente di rotture accidentali di cavi, va tenuto in considerazione che il danneggiamento intenzionale dei cavi durante una crisi o un conflitto armato potrebbe causare, oltre a danni economici, anche la parziale interruzione della catena di comando militare, la perdita di controllo sui propri *early-warning systems* e la potenziale perdita di efficienza di alcuni sistemi d'arma (37).

(31) Michael Sechrist, «New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems», Science, Technology, and Public Policy Program, (Belfer Center, 2012), <https://www.belfercenter.org/publication/new-threats-old-technology-vulnerabilities-undersea-communication-cable-network>.

(32) APEC Policy Support Unit, «Economic Impact of Submarine Cable Disruptions».

(33) Ryan Singel, «Cable Cut Fever Grips the Web», Wired, 2008, <https://www.wired.com/2008/02/who-cut-the-cab/>.

(34) Michael S. Matis, «The Protection of Undersea Cables: A Global Security Threat» (ARMY WAR COLL CARLISLE BARRACKS PA, 7 marzo 2012), <https://apps.dtic.mil/sti/citations/ADA561426>.

(35) Lixian Hantover, «The Cloud And The Deep Sea: How Cloud Storage Raises The Stakes For Undersea Cable Security And Liability», Ocean and Coastal Law Journal 19, n. 1 (17 maggio 2014), <https://digitalcommons.maine.gov/oelj/vol19/iss1/2>.

(36) Ibid.

(37) Clark, «Undersea cables and the future of submarine competition».

Vista l'importanza e la fragilità dell'infrastruttura dei cavi sottomarini sorprende che il tema sia relativamente poco esplorato. Bueger e Liebetrau (38) affermano, a tal proposito, che i cavi sottomarini soffrano di una **tripla invisibilità**. La prima invisibilità sarebbe quella propria di tutte le infrastrutture che, seppur fondamentali, sono spesso date per scontate. La seconda invisibilità sarebbe quella relativa alle infrastrutture non immediatamente visibili, mentre la terza invisibilità sarebbe quella relativa alla cosiddetta *sea blindness*, vale a dire l'errata percezione che il mare sia un dominio poco influenzato dall'attività umana.

Eppure, anche se il tema rimane criticamente poco esplorato dalla letteratura accademica e dal dibattito pubblico, esso è saldamente al centro di una rinnovata competizione geopolitica tra attori statali, quali Stati Uniti, Cina e Russia, ed attori non-statali quali le grandi aziende tecnologiche (39). La Cina, in particolare, nonostante sia entrata nella competizione dei cavi sottomarini solo di recente, può già vantare cinque delle sette maggiori aziende nel settore. I cavi sottomarini figurano spesso nei documenti strategici di Pechino, i quali fissano obiettivi come quello di aumentare la presenza cinese nella rete sottomarina del Mar Mediterraneo e conquistare oltre il 60% del mercato globale dei cavi sottomarini entro il 2025 (40).

Risulta evidente la necessità di avviare una riflessione non solo tecnica, ma anche politica e strategica sul ruolo dei cavi sottomarini nella competizione geopolitica. Bisogna, inoltre, conoscere in maniera approfondita quali sono i principali rischi ai quali i cavi sottomarini sono sottoposti. A tal proposito verranno ora analizzati **cinque principali minacce** alla stabilità di questa infrastruttura globale: *hybrid warfare*, attacchi cibernetici, terrorismo, danneggiamento accidentale e spionaggio.

(38) Bueger e Liebetrau, «Protecting hidden infrastructure».

(39) Ibid.

(40) Bechis, «Undersea Cables».

2.2

Hybrid warfare

Il danneggiamento dei cavi sottomarini quale tattica militare non è di certo una novità, la Royal Navy tagliò infatti tutti i cinque cavi che la Germania usava per le proprie comunicazioni trans-atlantiche poche ore dopo la dichiarazione di guerra nel 1914 (41). Non sorprende, quindi, che i cavi siano spesso elencati tra i principali obiettivi in caso di *hybrid warfare*. Schaub, Murphy, e Hoffman ad esempio affermano che tali infrastrutture sarebbero i bersagli primari durante una campagna di hybrid warfare, soprattutto nel **Mar Baltico**. La geografia di questa regione, infatti, permetterebbe alla Russia di compromettere le comunicazioni internazionali di Polonia, Lituania e Lettonia danneggiando anche solo pochi nodi strategici (42).



Fonte: Schaub Gary, Martin Murphy, Frank G Hoffman, 2017. «Hybrid Maritime Warfare». The RUSI Journal 162 (1): 32–40. <https://doi.org/10.1080/03071847.2017.1301631>.

Una simile operazione potrebbe essere condotta usando sottomarini a comando remoto dotati di sonar ed equipaggiati con esplosivi (43). La tecnologia necessaria risultagà facilmente reperibile (44), con barriere all'ingresso basse al punto da spingere Martinage ad affermare che non solo gli Stati, ma anche gruppi terroristici potrebbero dotarsene (45).

(41) Sunak, «Undersea Cables, Indispensable, insecure».

(42) Gary Schaub, Martin Murphy, e Frank G Hoffman, «Hybrid Maritime Warfare», The RUSI Journal 162, n. 1 (2 gennaio 2017): 32–40, <https://doi.org/10.1080/03071847.2017.1301631>.

(43) Robert Martinage, «Under the Sea», 26 ottobre 2015, <https://www.foreignaffairs.com/articles/commons/under-sea>.

(44) Sunak, «Undersea Cables, Indispensable, insecure».

(45) Martinage, «Under the Sea».

In un recente articolo, Carrer e Rossi (46) hanno evidenziato l'interesse russo verso i cavi sottomarini, sottolineando la frequente presenza di navi oceanografiche nei pressi di importanti dorsali di questa infrastruttura e l'esistenza di sottomarini dotati di braccia meccaniche capaci di agire sul fondale, anch'esse spesso localizzati nei pressi di importanti dorsali nella regione artica.

Concludendo, i cavi sottomarini rappresentano un potenziale obiettivo per campagne di *hybrid warfare*. Tali operazioni potrebbero danneggiare l'economia di uno stato, isolarlo e comprometterne la capacità di reazione. Descrivendo il caso russo, si è illustrato come una simile operazione sarebbe non solo vantaggiosa, ma anche facilmente realizzabile visto che gli strumenti necessari sono già a disposizione o in ogni caso facilmente reperibili.

(46) Gabriele Carrer e Emanuele Rossi, «Che cos'è il Gugi, l'unità russa sospettata di sabotare i cavi sottomarini», Formiche.net, 6 novembre 2021, <https://formiche.net/2021/11/cavi-sottomarini-gugi/>.



2.3 Cybersecurity

La crescente complessità dell'infrastruttura sottomarina e il bisogno di mantenere la profittabilità hanno spinto i principali attori in questo settore ad adottare *remote network management systems*. Tali sistemi utilizzano software capaci di rendere più efficiente il funzionamento dei cavi, di ridurre la forza lavoro necessaria e di fornire agli operatori maggiore *operational awareness* (47).

L'utilizzo di tali software, tuttavia, introduce un nuovo rischio per la connettività globale, vale a dire quello di **attacchi cibernetici**. Un hacker avrebbe la possibilità di guadagnare il controllo su questi sistemi connessi all'Internet, oltre che controllare e manipolare il traffico di dati (48). Lo scenario peggiore secondo Sechrist sarebbe quello di un hacker capace di forzare un *presentation server*, i quali ospitano *web-based management systems* di multipli cavi. In una simile situazione un hacker potrebbe avere accesso ad una moltitudine di dati e, tramite l'utilizzo di funzionalità ROADM (Reconfigurable Optical Add/Drop Multiplexing) sarebbe in grado di bloccare importanti porzioni di traffico dati (49).

In altri scenari, inoltre, è possibile immaginare hacker capaci di tenere in ostaggio intere infrastrutture utilizzando *ransomware*, o raccogliendo dati sfruttando la vulnerabilità dei *network management systems* (50).

In conclusione, le minacce ai cavi sottomarini non sono solo di natura fisica, ma anche cibernetica.

(47) Sechrist, «New Threats, Old Technology».

(48) Justin Sherman, «The U.S. Should Get Serious About Submarine Cable Security», Council on Foreign Relations, 2021, <https://www.cfr.org/blog/us-should-get-serious-about-submarine-cable-security>.

(49) Sechrist, «New Threats, Old Technology».

(50) Sherman, «The U.S. Should Get Serious About Submarine Cable Security».

2.4

Terrorismo

Un terzo rischio è quello di azioni da parte di gruppi terroristici ai danni dell'infrastruttura sottomarina e delle sue *landing stations*. Simili eventi sono già accaduti, ad esempio nel 2007 in Vietnam quando il danneggiamento di alcuni cavi fu attribuito a gruppi di pirati e nel 2010, quando un cavo internazionale fu danneggiato da gruppi terroristici nelle Filippine (51).

Uno svantaggio, a tal proposito, risiede nel fatto che, per ottimizzare i costi e facilitarne la gestione, **le landing stations tendono a concentrarsi nelle stesse zone geografiche o, in altri casi, diversi cavi approdano nella stessa landing station** (52). In Italia, ad esempio, la maggior parte dei cavi sottomarini che connettono il Paese emergono nei pressi di soltanto quattro località: Bari, Catania, Mazara del Vallo e Palermo (53). Tale vulnerabilità affligge allo stesso modo anche altri paesi, come gli Stati Uniti, dove Sechrist afferma che la maggior parte dei cavi transatlantici emergano in un raggio di 50 chilometri attorno New York (54). Ciò facilita lo svolgimento di operazioni coordinate ai danni delle landing stations o permette di danneggiare il funzionamento di diversi cavi tramite un attacco a una singola landing station (55).

Queste landing stations sono, quindi, componenti fisiche, ben visibili e geograficamente concentrate dell'infrastruttura dei cavi sottomarini. In quanto tali, esse rappresentano validi obiettivi per operazioni terroristiche. A tal proposito, infatti, Burnett ha sottolineato che “sarebbe naïve pensare che le *landing stations* dei cavi sottomarini [...] possano sfuggire ad attacchi terroristici asimmetrici” (56). Tale rischio risulta amplificato nel caso di stati fragili che non hanno il completo controllo del loro territorio e, quindi, non del tutto capaci di proteggere questi importanti nodi della infrastruttura globale (57).

(51) Hantover, «The Cloud And The Deep Sea».

(52) Margaret Ross, «Understanding Interconnectivity of the Global Undersea Cable Communications Infrastructure and its Implications for International Cyber Security», *The SAIS Review of International Affairs* 34, n. 1 (2014): 141–55, <https://www.jstor.org/stable/27000949>.

(53) TeleGeography, «Submarine Cable Map», 2021, <https://www.submarinecablemap.com/>.

(54) Sechrist, «New Threats, Old Technology».

(55) Hantover, «The Cloud And The Deep Sea».

(56) Douglas R. Burnett, «Cable Vision», *U.S. Naval Institute Proceedings*, 1 agosto 2011, <https://www.usni.org/magazines/proceedings/2011/august/cable-vision>.

(57) Colombo, Solfrini, e Varvelli, «Network Effects».

2.5

Danno accidentale

Come si è già affermato, standard di affidabilità “cinque nove”, vale a dire di una affidabilità del 99,999%, fanno sì che i cavi siano soggetti a pochi incidenti in proporzione alla loro distribuzione globale (58). Tuttavia, tale infrastruttura risulta comunque esposta a danni accidentali, infatti **si registrano annualmente circa cento interruzioni a seguito di fenomeni naturali e antropici** (59).

I cavi sottomarini possono essere soggetti ad abrasioni o altri fenomeni naturali, seppure questi eventi rappresentino una porzione ristretta del totale delle interruzioni di servizio. Tuttavia, quest’ultimi sarebbero una delle principali cause di danneggiamento in quelle porzioni di cavo ad oltre 1000 metri di profondità. Inoltre, seppur tali eventi siano improbabili, di solito il danno causato da essi andrebbe a colpire molteplici cavi simultaneamente (60). Basti pensare al terremoto del 2006 al largo delle coste di Taiwan, durante il quale nove cavi furono danneggiati, compromettendo comunicazioni, mercati e scambi finanziari non solo di Taiwan, ma dell’intera regione. Per riparare il danno furono necessarie 11 navi e 49 giorni (61).



Fonte: Sunak, Rishi. 2017. «Undersea Cables, Indispensable, insecure». Policy Exchange.

(58) Bueger e Liebetrau, «Protecting hidden infrastructure».

(59) Francola e Mensah, «L’industria dei cavi sottomarini: qualche elemento introduttivo».

(60) Ibid.

(61) Martinage, «Under the Sea».

Quando si parla di fenomeni naturali non ci si deve limitare ai soli terremoti, ma anche alle eruzioni vulcaniche, tempeste, tsunami e frane. Bueger e Liebetrau affermano che, visto il **cambiamento climatico** e il prevedibile aumento di fenomeni meteorologici estremi, tale rischio per i cavi andrà probabilmente ad intensificarsi (62).

Le attività di pesca e navigazione risultano essere un'ulteriore fonte di danni accidentali, infatti si stima che circa il 40% dei danni a questa infrastruttura sottomarina derivino da simili attività, in particolare dalla pesca a strascico, dragaggio e calata di ancore (63). Infatti, nelle porzioni di cavo a meno di 200 metri di profondità, la pesca e la calata di ancore sarebbero responsabili per oltre il 70% dei danni riportati (64). Il danno accidentale causato dall'attività umana sarebbe quindi una più frequente fonte di deterioramento, ma genericamente colpirebbe singoli cavi, non andando ad influenzare massicciamente la performance del network (65).

Per proteggere i cavi dai danni accidentali di natura antropica si è spesso proposto di creare dei perimetri di sicurezza attorno ai cavi per evitare attività potenzialmente pericolose (66), seppure tali iniziative siano difficilmente applicabili fuori dalle acque territoriali (67).

(62) Bueger e Liebetrau, «Protecting hidden infrastructure».

(63) Ibid.

(64) APEC Policy Support Unit, «Economic Impact of Submarine Cable Disruptions»; Kent Bressie, «Submarine Cable Protection and Resilience», 2021.

(65) APEC Policy Support Unit, «Economic Impact of Submarine Cable Disruptions».

(66) Francola e Mensah, «L'industria dei cavi sottomarini: qualche elemento introduttivo».

(67) Bueger e Liebetrau, «Protecting hidden infrastructure».

2.6 Spionaggio

I cavi veicolano, come già affermato, un' imponente mole di dati, fra i quali informazioni sensibili e strategiche. Accedere a esse fornirebbe un immenso vantaggio informativo.

Ciò che preoccupa, di conseguenza, è il fatto che imprese e stati possano spesso accedere ai dati transitanti nei cavi che essi gestiscono (68). Infatti, gli Stati Uniti hanno più volte evidenziato l'attivismo cinese e russo palesando il loro timore che Pechino possa usare le aziende statali nel settore per accedere a informazioni sensibili e classificate (69).

La proprietà del cavo non sarebbe neanche una condizione necessaria, visto che l'intercettazione del segnale può avvenire anche grazie a **recettori** che, applicati in particolari punti del cavo detti di rigenerazione, permettono di registrare e salvare i dati (non solo metadati, ma anche contenuti) ivi transitanti (70).

La diffusione di servizi in *cloud* per settori strategici quali energia, finanza, difesa e sanità aumenta costantemente il volume di **dati sensibili** in transito lungo i cavi, incentivando sempre più attività di spionaggio lungo l'infrastruttura di comunicazione (71).

(68) Colombo, Solfrini, e Varvelli, «Network Effects».

(69) Sherman, «The U.S. Should Get Serious About Submarine Cable Security».

(70) Francola e Mensah, «L'industria dei cavi sottomarini: qualche elemento introduttivo».

(71) Sherman, «The U.S. Should Get Serious About Submarine Cable Security»

3. CAVI SOTTOMARINI TRA ECONOMIA E GEOPOLITICA

Sebbene, ad oggi, i cavi sottomarini restino materia formalmente privata, con imprese che spesso formano consorzi per la costosa costruzione dell'infrastruttura, non si può ignorare l'importante ruolo svolto dagli Stati che trascende quello di mero vagliatore "passivo" del business condotto dalle aziende del settore. Al contrario, i governi hanno un ruolo fondamentale in tutti gli *step* della realizzazione e uso di un cavo, fino alla sorveglianza degli stessi. Il rapporto fra Stati e imprese del settore si concretizza in varie forme, lasciando più spazio all'uno o all'altro attore a seconda dell'entità delle esigenze securitarie che investono l'operazione.

Tuttavia, i cavi sottomarini sono un mercato che più di altri si può definire strategico per gli Stati moderni: la loro natura infrastrutturale li rende di cruciale importanza per due ragioni principali. In primo luogo, per i benefici che garantiscono ai loro fruitori. Sarebbe lapalissiano ricordare il fondamentale ruolo di comunicazione che essi svolgono con la trasmissione di dati e voce permettendo a due centri di un sistema (sia questo *inter* o intranazionale) di lavorare insieme, come la radice latina del verbo (**cum-munis**) prevede.

Non a caso, fin dall'avvento dei primi cavi sottomarini, a metà Ottocento, fu discussa la loro rilevanza per l'interesse nazionale, soprattutto per via degli indiscutibili vantaggi che tale infrastruttura comportava (72). In tal senso, il ruolo dello Stato è da intendersi come promotore di una politica industriale volta a creare valore per il sistema-paese e le aziende operanti nel settore. Inoltre, obiettivo meno evidente all'opinione pubblica, **il rapporto delle amministrazioni con il settore è a volte orientato alla collezione strategica dell'enorme mole di dati che i cavi trasportano** (73).

La seconda ragione per cui l'industria dei cavi sottomarini attira le attenzioni degli apparati statali è legata ai rischi e vulnerabilità menzionate nel capitolo precedente. Ciò implica, quindi, molteplici azioni da prendere in considerazione che spaziano dal garantire l'ordinario funzionamento delle funzioni digitali di base al mantenere l'indipendenza della rete nazionale con le fondamentali informazioni che vi scorrono da potenziali minacce esterne (sia di carattere *cyber-terroristico* che di spionaggio). È chiaro, poi, che queste due ragioni possono inevitabilmente incrociarsi.

(72) T. Twiss, "Submarine telegraph Cables" (november 1880) *XIIX: XI The Nautical Magazine* at 883-884.

(73) Fabbri, D. (2018). L'impero informatico americano alla prova cinese. *Limes*, rivista italiana di Geopolitica 10/2018 <https://www.limesonline.com/cartaceo/limpero-informatico-americano-alla-prova-cinese>

Per una grande potenza “sicurezza” e “protezione” sono concetti dal significato ben più ampio della loro classica interpretazione “difensiva”. Negli Stati Uniti, ad esempio, è ricorrente il riferimento all’avanzata tecnologia come il raggiungimento di una **“frontiera infinita”** (secondo la terminologia di Vannevar Bush (74), consigliere di F.D. Roosevelt) che va naturalmente difesa. È un concetto automaticamente applicabile anche ai cavi sottomarini, tramite il quale l’assertività politica americana si dirada nel globo sotto forma di *World Wide Web*. **Si tratta di un ruolo egemonico da mantenere e proteggere, non senza costi sia economici che di immagine** (non è facile predicare libertà informatica la mattina e difendersi dalle rivelazioni di Snowden la sera).

Inoltre, i cavi sottomarini e il loro peso nella trasmissione dei dati sono la dimostrazione dell’**innegabile fisicità dell’Internet**, spesso visto come abitante di uno spazio evaporato in *cloud* e smaterializzato in *bits*. Le tecnologie che occupano il dibattito contemporaneo come il 5G, l’intelligenza artificiale, l’*Internet of Things* e il *cloud computing* si basano, al contrario, tutte su componenti hardware da cui e verso cui i dati vengono trasportati niente di meno che da cavi.

È, quindi, evidente che queste ragioni collocano i cavi sottomarini in molteplici zone conflittuali a livello geopolitico con ripercussioni sia nei **rapporti internazionali** tra Stati sia nelle dinamiche interne ai sistemi-paese. Dunque, analizzare lo stato dell’arte dei cavi sottomarini significa porre l’analisi su diversi livelli che si influenzano reciprocamente.

Nella sezione seguente analizzeremo il mondo dei cavi sottomarini da due punti di vista che sono intimamente collegati: quello economico che guarda al mercato dei cavi con i vari attori in gioco a diversi livelli della catena del valore e, infine, quello geopolitico, prendendo in esame i conflitti di potere esistenti in questo sistema.

(74) Bush, V. “Science, The Endless Frontier”, 1945

3.1 L'economia dei cavi

Il business dei cavi sottomarini non è semplice. Infatti, il costo di un cavo, dalla manifattura alla posa e ai permessi, parte dalle centinaia di milioni di dollari (per quelli più corti) fino al miliardo di dollari per i cavi transpacifici. Molte realtà diverse concorrono alla realizzazione dell'infrastruttura, Colombo et al. (75), ad esempio, identificano tre principali attori nell'industria dei cavi sottomarini: compagnie di telecomunicazioni, compagnie *Big-tech* e aziende specializzate nella manifattura, operazione e mantenimento dell'infrastruttura. Trasversalmente a queste tre categorie, è possibile individuarne altre due: i possessori veri e propri di cavi (**cable owners**) e i fornitori (**cable suppliers**). Le tre realtà si relazionano, quindi, in rapporti mutevoli rispetto alle due dimensioni: le imprese manifatturiere sono gli attori principali per la progettazione e l'installazione di tutti gli elementi del sistema, dai cavi stessi ai ripetitori e le stazioni di approdo. Tuttavia, compagnie di telecomunicazioni e aziende Big-Tech possono cimentarsi direttamente in alcune operazioni delle imprese manifatturiere. Possono agire singolarmente o in consorzi con altre compagnie del settore (o anche di un altro settore).

La proprietà del cavo viene solitamente usata dagli operatori di telecomunicazioni o servizi internet per fini di traffico proprio, mentre la capacità di trasmissione restante può essere venduta ad altri operatori. Tra i proprietari di alcune quote di cavi sottomarini sono da menzionare anche le banche d'investimento, che possono perfino detenere una quota di *capacity* di trasmissione come collaterale per il credito fornito. Menzione a parte, nella catena del valore, meritano poi i *provider* dei servizi più strettamente "marittimi", che forniscono le imbarcazioni e il personale specializzato per la messa a fondo dei cavi.

Il principale e più tradizionale modello di business nel settore si basa su **consorzi di aziende** interessate all'utilizzo del cavo. Queste formano accordi tra le parti per la divisione delle ingenti quantità di capitale richiesto. Tali accordi si concretizzano intorno al "Construction & Maintenance Agreement", dove vengono anche stabilite le rispettive quote di capacità assegnata. Le aziende, invece di impegnarsi direttamente, possono a volte cimentarsi nella creazione congiunta di società di progetto (**Special Purpose Vehicles**) per la partecipazione al progetto. In tal modo, il finanziamento è reso più agevole al prezzo, però, di una minore autonomia nel *management* dell'infrastruttura. In ogni caso, l'investimento in un consorzio è un procedimento che l'azienda valuta attentamente, dati l'ammontare di capitale coinvolto e i tempi non brevi da aspettare prima di un ritorno, che è comunque costituito principalmente dall'utilizzo di capacità e non di rivendita.

(75) Colombo, Solfrini, e Varvelli, «Network Effects».

Un altro modello di business è quello dei “**cavi privati**”, che hanno come primo obiettivo il mercato all'ingrosso e la rivendita di capacità piuttosto che l'utilizzo da parte delle parti. In questo modello possono anche agire uno o più investitori istituzionali (come, ad esempio, fondi sovrani). Reverdy e Skenderoski (76) definiscono gli abituali requisiti di finanziamento per la costruzione di cavi sottomarini a fronte di investimenti corposi in capitale fisso (CAPEX) comparati con una spesa operativa (OPEX) nettamente minore (in media appena il 6% del CAPEX), che viene più che finanziata dai flussi di cassa derivanti dall'eventuale vendita di capacità. Come in ogni infrastruttura, quindi, un progetto di costruzione e messa in posa di cavo sottomarino deve far fronte a notevoli spese preventive prima che sia *ready-for-service* e che generi, di conseguenza, ricavi: un periodo che può durare 2-3 anni, al netto di complicazioni regolatorie o geopolitiche. A causa di queste ragioni di necessità di raccolta fondi, l'iniziatore del progetto spesso ricerca la partecipazione di stakeholders interessati per ragioni politiche o commerciali, come **banche di sviluppo** o **agenzie di credito all'esportazione**. In ogni caso, il modello di costruzione di cavi mirato al profitto ha subito un rallentamento dopo il *boom* dei primi anni Duemila, il quale ha portato a sospetti di una bolla speculativa nel settore (77).

Nell'ultimo periodo si è assistito a un incremento del modello “cavo privato” costruito per fini propri. L'accresciuta popolarità di esso è dovuta alle diverse necessità dei gruppi Big Tech rispetto alle tradizionali imprese di telecomunicazioni: i primi, infatti, necessitano di una mole maggiore di capacità e di elevati *standard* di qualità per la fornitura dei loro contenuti e preferiscono più semplicemente sviluppare i cavi per le proprie necessità, utilizzandone la capacità quasi totalmente. Infatti, **Microsoft, Apple, Meta e Google insieme utilizzano oltre il 66% della capacità totale della rete di cavi sottomarini** (78). Nel 2010 Google era l'unica società possedente una quota in un solo cavo, invece si prevede che per il 2024 questi quattro giganti statunitensi possiederanno delle quote in oltre 30 cavi (79), non pochi dei quali a proprietà unica. L'alta competitività di questo modello, che non prevede la stretta necessità di fare profitti dall'infrastruttura, ha progressivamente eroso i ricavi degli operatori *wholesale*, tramite un evidente calo della domanda.

(76) Reverdy, D. & Skenderoski I. (2015) Submarine Cables: Structuring and Financing Options. Salience Consulting White Paper [https://salienceconsulting.ae/wp-content/uploads/2018/09/Submarine Cables Structuring and Financing Options Jan 2015.pdf](https://salienceconsulting.ae/wp-content/uploads/2018/09/Submarine-Cables-Structuring-and-Financing-Options-Jan-2015.pdf)

(77) Miller, J. (2017). Submarine Cables: Are We in a New Bubble?. Telegeography Blog <https://blog.telegeography.com/ptc-submarine-cable-bubble-presentation-2017-market-summary>.

(78) Mims, C. (2022) Google, Amazon, Meta and Microsoft Weave a Fiber-Optic Web of Power <https://www.wsj.com/articles/google-amazon-meta-and-microsoft-weave-a-fiber-optic-web-of-power-11642222824>

(79) Submarine Telecom Forum: Industry Report 2021

Ciò ha sollevato un dibattito (80) sulle eventuali implicazioni socio-economiche della “privatizzazione dell'infrastruttura digitale”. Seguendo un'azzeccata similitudine del giornalista Christopher Mims: **“immaginiamo se Amazon possedesse le strade su cui consegna i suoi pacchi”**.

L'ultimo Industry Report (81) svolto dal Submarine Telecom Forum prevede che questa crescente prevalenza dei *provider OTT* come Amazon, Google e Facebook porterà a una nuova definizione delle tratte dei cavi sottomarini. Questi, infatti, non saranno più pensati per far comunicare grandi centri abitati tramite i servizi di telecomunicazione, ma per connettere i data center di tali compagnie e l'ingente mole di *capacity* che richiedono.

Le aziende che valutano la posa di un nuovo cavo sono, generalmente, spinte da tre fattori (82): la domanda di ulteriore **capacità** all'interno di una tratta preesistente e di **connettività** ulteriore tra due punti già connessi per garantire una diversificazione delle tratte che prevenga i rischi e, infine, la domanda, prettamente politica, di **connessione di una Nazione al network di rete per fini di sviluppo economico**. Per quest'ultimo punto si prenda come esempio il progetto EASSy, un sistema mirato a collegare tra loro i Paesi della costa africana orientale. Questi sono progetti che vedono più spesso la partecipazione di banche di sviluppo, come la Banca Mondiale, nel finanziamento del progetto.

(80) Cooper, T. (2019) “Google and other tech giants are quietly buying up the most important part of the internet”. Venturebeat

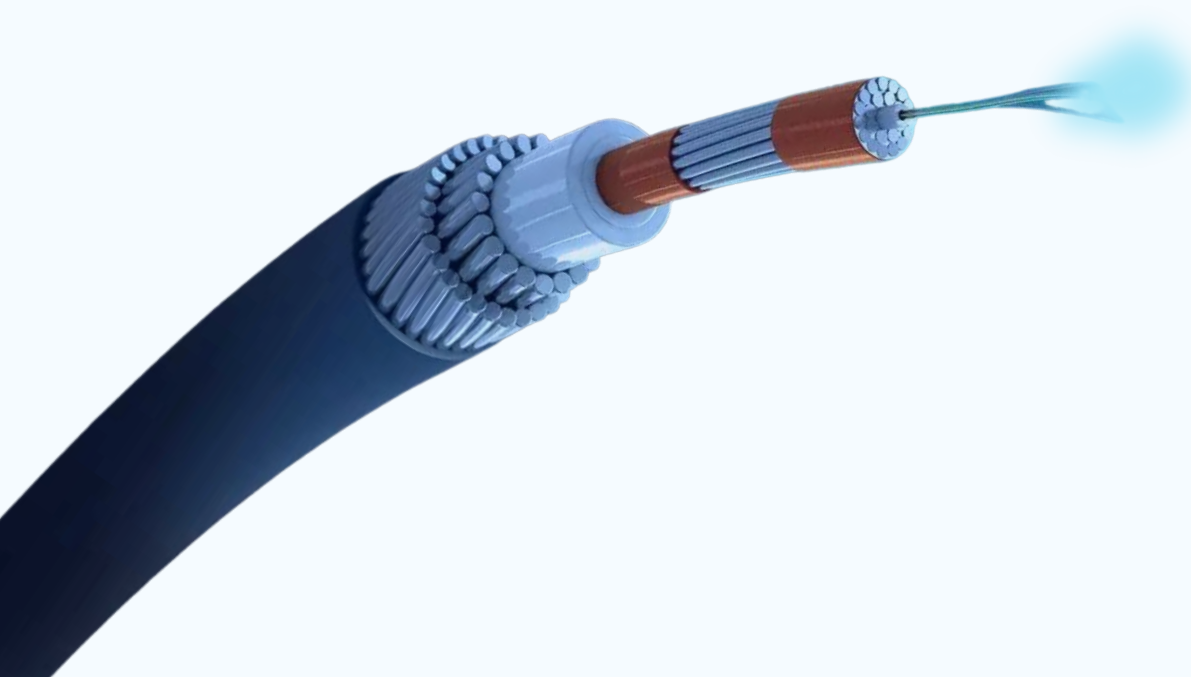
<https://venturebeat.com/2019/04/06/google-and-other-tech-giants-are-quietly-buying-up-the-most-important-part-of-the-internet/>

(81) Submarine Telecom Forum: Industry Report 2021

(82) Burnett, D. R., Beckman, R., & Davenport, T. M. (Eds.). (24 Oct. 2013). Submarine Cables. Leiden, The Netherlands: Brill | Nijhoff. doi: <https://doi.org/10.1163/9789004260337>

	Fornitori/Possessori
Aziende di telecomunicazioni	AT&T(US) BT (UK) Telecom Italia Sparkle (IT) Orange Marine (FR)
Aziende fornitrici di servizi Internet	Google (US) Meta (US) Amazon (US) Microsoft (US)
Aziende specializzate	Alcatel Submarine Networks (FR) Subcom (US) NEC (JP) Hengtong/ Huawei Marine (CN) Global Marine Systems (UK) Prysmian (IT)

Alcuni esempi di imprese coinvolte nel settore dei cavi sottomarini



3.2 Geopolitica dei cavi sottomarini

Come accennato in precedenza, le azioni degli attori menzionati nel paragrafo sopraindicato sono inevitabilmente influenzate dalle dinamiche geopolitiche. Se la geopolitica si occupa dei conflitti di potere in spazi determinati, i cavi sottomarini non possono sottrarsi a tali conflitti per due principali ragioni tra loro connesse. **I cavi sono immersi nel potere grazie a (o a causa di) le merci che viaggiano su tale infrastruttura: i dati.** Il loro accesso o libero fluire, infatti, risultano vitali per i due centri che l'infrastruttura connette, anche se in un rapporto impari. Le Nazioni, inoltre, fanno grande affidamento sui cavi sottomarini anche per le comunicazioni più sensibili legate alla sicurezza nazionale: i sistemi di radiofrequenza dei satelliti non possiedono ancora la larghezza di banda necessaria a gestire l'immensa mole di dati richiesta dalle operazioni militari o di *intelligence* (83). In secondo luogo, i cavi sono componente fisica del mondo digitale e ne rappresentano, appunto, lo spazio. Essi seguono rotte predeterminate, passano per colli di bottiglia sensibili e approdano in punti specifici, in tutti luoghi e territori dove le autorità politiche possono agire per svariati interessi con la forza o le leggi. **Quindi quali sono le azioni dei diversi Stati nello scacchiere globale? Quali interessi perseguono o con quali modalità?** Questa sezione si propone di rispondere a queste domande facendo riferimento ai principali soggetti geopolitici mondiali.

È doveroso iniziare col conflitto Cina-Stati Uniti, nel quale la prima potenza cerca di contrastare la posizione egemonica di Washington nei mercati progettando una globalizzazione "con caratteristiche cinesi". Si tratta della **Belt & Road Initiative**, l'ultra-dibattuto progetto di Pechino per una connessione commerciale con l'Eurasia, resa tramite infrastrutture di trasporti, collaborazioni industriali, reti energetiche e molto altro (84). Il tutto permeato da una retorica opposta a quella, considerata paternalistica, del "Washington Consensus". È una sfida che ha visto gli Stati Uniti impegnati su molti fronti (militare, telecomunicazioni, finanziario) e con diverse armi, dalla minaccia militare all'interruzione di procedure di fusione e acquisizione, anche al di fuori del territorio americano. In tale braccio di ferro l'industria delle telecomunicazioni gioca un ruolo fondamentale per motivi già citati, come l'importanza di dati e informazioni a fronte del loro ampio utilizzo nelle tecnologie del domani (85).

(83) Bryan Clark (2016) Undersea cables and the future of submarine competition, Bulletin of the Atomic Scientists, 72:4, 234-237, DOI: 10.1080/00963402.2016.1195636

(84) Amighini, A. e Sciorati, G. (2019) "Fact Checking: BRI, la nuova via della seta". Ispionline <https://www.ispionline.it/it/pubblicazione/fact-checking-bri-la-nuova-della-seta-23784>

(85) Ne abbiamo già parlato in Crivellaro e Wilegoda (2020). 5G: opportunità di investimento ed implicazioni geopolitiche delle reti di quinta generazione. AWARE Think Tank

L'importanza dei cavi sottomarini in queste dinamiche deriva proprio dal fatto che essi rappresentano le autostrade su cui viaggiano i dati, oro del nuovo millennio. Esempio lampante di tale inevitabile conflittualità è il caso del **Pacific Light Cable Network** (PLCN), progetto di cavo da tredicimila chilometri patrocinato da Facebook e Google che avrebbe dovuto collegare Los Angeles e Hong Kong, passando anche per Filippine e Taiwan. "Avrebbe dovuto", appunto. Fin dalla sua proposta nel 2016, il progetto ha, infatti, destato l'attenzione del "Team Telecom". Quest'ultimo è stato per anni un processo informale interagenzia che informava e consigliava la famosa *Federal Communications Committee* (FCC) di Washington, responsabile delle licenze ad operare, su possibili minacce alla sicurezza nazionale dovute alla presenza estera nel settore telco statunitense. Nel 2020, tale processo è stato rinominato e formalizzato con ordine esecutivo (86) della Casa Bianca come *"Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector"* e lo stesso Dipartimento di Giustizia (87) ne evidenzia i parallelismi con il potente *"Committee on Foreign Investment in the United States"* (CFIUS).

Nel 2016, appunto, il Team Telecom raccomandò subito alla FCC di non autorizzare le operazioni di collegamento digitale, nonostante il cavo fosse già stato posato. Alla sua costruzione e messa in posa parteciparono la statunitense TE SubCom e la Pacific Light Data Communication Company (PLDC), braccio di Hong Kong della Compagnia China Soft Power Technology Holdings LTD (poi acquistato dal gigante dei media telco cinese Dr. Peng Group (88)). Gli apparati che costituiscono il Team Telecom (tra cui il Pentagono stesso) erano chiaramente preoccupati sia della porzione di cavo che arrivava nella baia di Hong Kong, sia della già citata sussidiaria e degli stretti legami tra Dr. Peng e Huawei. Dopo richieste dai toni imploranti (89) di Google e Facebook e le successive verifiche delle varie agenzie, il cavo è entrato in funzione nel gennaio del 2022, ma solo per la parte tra California, Filippine e Taiwan, con la promessa delle aziende della Silicon Valley di non autorizzare alcuna

(86) White House. Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (2020) <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-establishing-committee-assessment-foreign-participation-united-states-telecommunications-services-sector/>

(87) Department of Justice (2020). The Committee for the assessment of Foreign Participation in the United States Telecommunications Services Sector - Frequently Asked Questions. <https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector#11>

(88) Submarine Cable Networks. (2022). PLCN.

(89) Reuters riporta frammenti della richiesta di Google che parlano di una "necessità immediata di soddisfare la domanda interna di collegamento tra i data center di Taiwan e quelli in USA", di un impegno da parte della compagnia di "perseguire la diversificazione dei collegamenti con l'Asia" e di un ringraziamento (sic!) alla FCC per aver consentito le operazioni in tal senso. <https://www.reuters.com/article/us-usa-trade-china-telecommunications-idUSKCN21Q2TP>

operazione sul cavo della sussidiaria di Hong Kong (90). La notizia non è stata accolta benissimo in Cina: un mese dopo, il 21 febbraio 2022, Dr.Peng vende il 100% delle sue quote in PLDC a Meister United Limited, compagnia spalleggiata da un fondo di *private equity* canadese.

È poi rilevante menzionare il blocco, nel 2019, da parte del governo australiano al progetto (già accordato tra le parti tre anni prima) di cavo di **Huawei Marine**, che avrebbe collegato l'Australia alla Papua Nuova Guinea e Isole Salomone, sulle basi di possibili minacce alla sicurezza nazionale (91).

Di conseguenza, non dovrebbero sorprendere i punti di approdo del già menzionato progetto **PEACE**, progetto di una rete di cavi a trazione cinese (Hengtong), che già connette il Pakistan all'Africa orientale e mira ad estendersi fino alle coste francesi. Il progetto, secondo il responsabile operativo Xiaohua Sun (92), è un elemento centrale dell'iniziativa di sviluppo infrastrutturale One Belt, One Road, adottata da Pechino nel 2013. L'iniziativa PEACE si inserisce quindi agilmente nel progetto che negli ultimi tempi ha visto avvicinarsi proprio Pechino con Islamabad e i paesi dell'Africa centro-orientale, sollevando pertanto non poche preoccupazioni negli Stati Uniti (93).

Infine, osserviamo come il processo di intelaiatura dei network sottomarini sia notevolmente complicato per le motivazioni geopolitiche che si moltiplicano con i rischi menzionati nel capitolo precedente: un'azienda non può attraccare a una qualsiasi sponda senza preoccuparsi delle implicazioni politiche, ma al tempo stesso non è da escludere che a monte di alcune scelte di business ci sia un progetto politico.

Tutto ciò delinea un assetto di compenetrazione tra **poteri pubblici e interessi economici privati** che interessa sostanzialmente ogni attore statale in competizione per un ruolo nello scacchiere internazionale (94).

(90) Khalili, J. (2020). Google, Facebook to activate undersea web cable, excluding China and Hong Kong. Techradar. <https://www.techradar.com/news/google-facebook-to-activate-undersea-web-cable-excluding-china-and-hong-kong>

(91) Smyth, J. (2017). Huawei's undersea cable project raises red flag in Australia. Financial Times. <https://www.ft.com/content/96513f58-d959-11e7-a039-c64b1c09b482>

(92) Peacecable.net. News del 29.11.2018 <http://www.peacecable.net/news/Detail/16600>

(93) Nyabiage, J. (2022). China's Peace cable linking Europe and Africa arrives in Kenya. South China Morning Post <https://www.scmp.com/news/china/diplomacy/article/3172463/chinas-peace-cable-linking-europe-and-africa-arrives-kenya>

(94) Si veda Aresu, A. (2020). Le potenze del capitalismo politico. Stati Uniti e Cina. La Nave di Teseo

4. IL CASO ITALIANO

Alla luce delle dinamiche menzionate nelle sezioni precedenti, resta da chiedersi cosa possa fare il sistema-paese Italia per adottare una strategia che minimizzi i rischi e valorizzi le opportunità derivanti dall'infrastruttura dei cavi sottomarini.

4.1 Mitigazione dei rischi

Quando si parla della mitigazione dei rischi, purtroppo, non esiste una singola misura che, implementata, garantirebbe un'effettiva protezione a questa infrastruttura rispetto ai vari rischi. Infatti, la differente natura dei rischi possibili richiede un approccio multidimensionale al problema.

Se è, infatti, vero che parte dei problemi, soprattutto in riferimento al danno accidentale, potrebbero essere risolti focalizzandosi sul rafforzamento fisico di questa infrastruttura, è altrettanto giusto affermare che fenomeni più complessi e intrinsecamente transnazionali, quali *hybrid warfare*, spionaggio e instabilità derivante dal condividere infrastrutture con paesi e regioni politicamente instabili, richiedono un approccio diverso.

La necessità di un approccio congiunto in seno alla NATO in merito alla difesa delle infrastrutture sottomarine è emersa durante la riunione dei Ministri della Difesa, tenutasi il 22 e 23 Ottobre 2020 (95). La discussione, seguita alla distribuzione di un *report* confidenziale sulle vulnerabilità dell'infrastruttura sottomarina (96), ha ricordato agli alleati la necessità di cooperare e sviluppare capacità moderne nel dominio marittimo. Un mese dopo, il Segretario Generale Stoltenberg ha affermato che l'Alleanza Atlantica valuta positivamente investimenti in capacità navali, in aerei per il pattugliamento marittimo e l'organizzazione di esercitazioni congiunte (98).

(95) Mattia Patriarca, «La sicurezza dei cavi sottomarini: una sfida per l'Europa», Geopolitica.info (blog), 14 ottobre 2021, <https://www.geopolitica.info/cavi/>.

(96) NATO, «Online Press Conference by NATO Secretary General Jens Stoltenberg Following the First Day of the Meetings of NATO Defence Ministers», NATO, 2020, http://www.nato.int/cps/en/natohq/opinions_178946.htm.

(97) Alexandra Brzozowski, «NATO Seeks Ways of Protecting Undersea Cables from Russian Attacks», www.euractiv.com, 23 ottobre 2020, <https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/>.

(98) NATO, «Adapting NATO for 2030 and beyond - Speech by NATO Secretary General Jens Stoltenberg at the 66th Annual Session of the NATO Parliamentary Assembly», NATO, 2020, http://www.nato.int/cps/fr/natohq/opinions_179665.htm.

Inoltre, l'istituzione di un NATO Command for North Atlantic in Norfolk incaricato, fra le altre cose, di approfondire la protezione e il monitoraggio dell'infrastruttura sottomarina (99), sottolinea l'importanza che la NATO dedica a questa tematica.

Sebbene le iniziative della NATO siano cruciali, è altrettanto necessario notare che, per quanto concerne la protezione dei cavi sottomarini, il *focus* dell'Alleanza è nell'Oceano Atlantico, in particolare nel Nord Atlantico (100). **Potrebbe, quindi, essere necessario, dal punto di vista nazionale, ribadire l'importanza del Mediterraneo per la connettività globale e sicurezza.**

E' da notare, inoltre, il crescente attivismo dell'Unione Europea in merito alla protezione delle infrastrutture sottomarine e alla reazione ad aggressioni ibride. L'Alto rappresentante Borrell ha, infatti, parlato di un *hybrid toolbox* per fornire agli Stati Membri gli strumenti necessari a fronteggiare varie tipologie di aggressione (101).

Nel 2021, inoltre, nell'ambito del Digital Day, la Commissione europea ha elencato gli elementi necessari per raggiungere gli obiettivi comunitari in termini di connettività. Essi includono rafforzamento delle *partnership*, miglioramento dell'infrastruttura dei cavi sottomarini, sicurezza dei network e connettività satellitare (102). Contestualmente, una Dichiarazione Ministeriale del 2021 invitava a includere i cavi sottomarini nell'elenco delle infrastrutture critiche per l'UE (103).

Tali sviluppi sono interessanti, soprattutto se si considera che nel nuovo "Strategic Compass" dell'Unione, si fa menzione a una nuova normativa europea sulla *cyber-resilienza* e si manifesta la volontà di sfruttare la cooperazione strutturata permanente, le presenze marittime coordinate e la condivisione di informazioni, al fine di fornire agli Stati Membri una migliore conoscenza situazionale per la protezione delle infrastrutture marittime critiche (104).

(99) NATO, «Online Press Conference by NATO Secretary General Jens Stoltenberg Following the First Day of the Meetings of NATO Defence Ministers».

(100) NATO, «Adapting NATO for 2030 and beyond - Speech by NATO Secretary General Jens Stoltenberg at the 66th Annual Session of the NATO Parliamentary Assembly».

(101) Flavio Fabbri, «Borrell: "L'UE deve diventare un provider di sicurezza ibrida, anche cyber"», CyberSecurity Italia (blog), 12 novembre 2021, <https://www.cybersecitalia.it/borrell-ue-leuropa-deve-diventare-un-provider-di-sicurezza-ibrida-anche-cyber/15173/>.

(102) Commissione europea, «Digital Day 2021: Europe to Reinforce Internet Connectivity with Global Partners | Shaping Europe's Digital Future», 19 marzo 2021, <https://digital-strategy.ec.europa.eu/en/news/digital-day-2021-europe-reinforce-internet-connectivity-global-partners>.

(103) Ministerial Declaration, «European Data Gateways as a key element of the EU's Digital Decade», 19 marzo 2021.

(104) Consiglio dell'Unione europea, «Una bussola strategica per la sicurezza e la difesa», 21 marzo 2022, <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/it/pdf>.

Viene spesso affermato, inoltre, che la protezione dei cavi sottomarini sarà forse un elemento incluso nell'aggiornamento della direttiva NIS (105), a riguardo del quale sono iniziate, il 13 Gennaio 2022, le negoziazioni interistituzionali (106). A tal proposito, riteniamo sia necessario adottare una posizione nazionale che incentivi e incoraggi tali iniziative e ne assicuri la piena implementazione.

Tuttavia, la dimensione transnazionale dei cavi non esonera dal prendere in considerazione misure nazionali per la protezione dell'infrastruttura. In particolare, il NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) afferma che le *cable landing stations* siano spesso poco protette e che potrebbero essere implementate misure ulteriori per garantirne la sicurezza (107). Inoltre, riporta anche che tali stazioni siano meno protette, dal punto di vista fisico, di una comune banca (ne sarebbe una prova l'intromissione di un giornalista in una cable landing station in Cornovaglia nel 2018 (108)), invitando, quindi, un investimento in sorveglianza e perimetri di sicurezza. Inoltre, **risulta necessario anche valutare la diversificazione geografica delle landing stations**, in modo da evitare eventuali colli di bottiglia, garantire la ridondanza e mantenere la connettività anche in caso di catastrofi naturali.

(105) Patriarca, «La sicurezza dei cavi sottomarini».

(106) Parlamento Europeo, «Review of the Directive on security of Network and information systems», European Parliament, 2022, <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive>.

(107) CCDCOE, «Strategic importance of, and dependence on, undersea cables», 2019, <https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf>.

(108) Mark Hookham e Gabriel Pogrud, «Revealed: How Reporter Strolled into UK's 'Secure' Data-cable Sites», The Sunday Times, 4 febbraio 2018, par. news, <https://www.thetimes.co.uk/article/revealed-how-reporter-strolled-into-uks-secure-data-cable-sites-f6fx2hndv>.

4.2 Valorizzazione delle opportunità

Una valorizzazione del settore è materia di politica industriale che, per sua natura, deve tenere conto delle peculiarità dell'industria di riferimento e di cosa si intenda per "valorizzazione". Chiaramente, il caso dell'infrastruttura è particolare: una buona infrastruttura digitale si valuta, oltre che in base alla sua sicurezza e resistenza agli shock, anche dalla sua qualità nel senso di velocità, capacità etc.

La questione della formulazione di una politica infrastrutturale relativa ai cavi richiede una precisa riflessione su quali margini di azione adottare.

Un aspetto da considerare è sicuramente quello della *redundancy*, ovvero la diversificazione dell'infrastruttura in modo da avere più *capacity* potenziale rispetto a quella effettivamente utilizzata per far fronte a eventuali interruzioni. **Tuttavia, appare evidente che una strategia di valorizzazione del settore non può prescindere dalla considerazione più ampia di valorizzazione delle tecnologie,** che di questa infrastruttura fanno grande uso, come per esempio il Cloud.

Per quanto riguarda l'azione all'interno dell'Unione europea, va tenuto di conto che la natura dell'Unione, sebbene diversa da quella di ogni altra organizzazione internazionale, impone ancora di pensarla più come un *forum* di compensazione di interessi diversi, piuttosto che come entità di indirizzo autonomo. La politica industriale è uno dei campi in cui questo aspetto meglio si apprezza, soprattutto quando questa concerne settori strategici, spazi in cui la sovranità trattenuta dagli Stati Membri è ancora elevata. Anche nei cavi, quindi, l'Unione è incapace (109) di imporre una politica propria riguardo alla discrezionalità della concessione delle licenze o alla formazione e composizione dei consorzi, per esempio. Ciononostante, esistono dei margini di manovra. La sezione digital dell'iniziativa **Connecting Europe Facility** (CEF) per il 2021-2027 prevede il co-finanziamento per progetti di infrastrutturazione digitale europea, fra i quali proprio i cavi sottomarini (110).

La Commissione ha agito, inoltre, quale investitore diretto contribuendo a metà del *budget* del Consorzio BELLA per la costruzione del cavo **EllaLink**, che collega Portogallo e Brasile.

(109) Colombo, Solfrini, e Varvelli, «Network Effects».

(110) Commissione Europea, Press Corner del 16 dicembre 2021:

https://ec.europa.eu/commission/presscorner/detail/en/IP_21_6830

Guardando alla politica internazionale, l'infrastruttura sottomarina rappresenta sia una sfida che un possibile volano per la proiezione estera nazionale. Come notato da Ross, **l'Italia è il secondo paese al mondo per "betweenness centrality score" nell'infrastruttura dei cavi sottomarini** (111). Preceduta solo dagli Stati Uniti, l'Italia avrebbe ottenuto questo risultato grazie alla sua centralità geografica nell'infrastruttura globale e, quindi, alla sua natura di snodo cruciale per connettere diverse regioni.

Tale connettività ha importanti conseguenze politiche, visto il potenziale che le infrastrutture hanno di integrare regioni e di creare importanti relazioni politiche (112). La connessione e l'interdipendenza infrastrutturale incentiva i governi a mantenere e approfondire relazioni diplomatiche, come nel caso dell'Italia con la **Libia**, in cui il fitto network di infrastrutture condivise rappresenta un importante elemento nelle relazioni politiche fra gli Stati (113).

Di conseguenza, **vista la posizione e il ruolo dell'Italia nell'area Mediterranea, risulta necessario analizzare il legame fra infrastrutture digitali e stabilizzazione politica in paesi vulnerabili**. Tale approccio è stato anche proposto da Bueger e Liebetrau, i quali hanno invitato ad approfondire tematiche quali il legame fra conflitti interni e infrastrutture digitali e indagare come includere obiettivi di connettività nell'ambito di operazioni di state-building o di *security sector reforms*. Un approccio alla connettività globale attento alle regioni vulnerabili potrebbe, inoltre, permettere una più veloce e duratura ripresa economica laddove conflitti hanno degradato le infrastrutture del paese. Inoltre, potrebbe garantire l'affidabilità di un mezzo attraverso il quale veicolare la **partecipazione della società civile alla transizione democratica** (114).

(111) Ross, «Understanding Interconnectivity of the Global Undersea Cable Communications Infrastructure and its Implications for International Cyber Security».

(112) Bueger e Liebetrau, «Protecting hidden infrastructure».

(113) Colombo, Solfrini, e Varvelli, «Network Effects».

(114) Bueger e Liebetrau, «Protecting hidden infrastructure».

BIBLIOGRAFIA

- APEC Policy Support Unit. «Economic Impact of Submarine Cable Disruptions», 2012.
- Amighini, A. e Sciorati, G. (2019) "Fact Checking: BRI, la nuova via della seta". Ispionline <https://www.ispionline.it/it/pubblicazione/fact-checking-bri-la-nuova-della-seta-23784>
- Aresu, A. Le potenze del capitalismo politico. Stati Uniti e Cina. La Nave di Teseo, 2020
- Bechis, Francesco. «Undersea Cables: The Great Data Race Beneath the Oceans». Text. ISPI, 28 maggio 2021. <https://www.ispionline.it/en/pubblicazione/undersea-cables-great-data-race-beneath-oceans-30651>.
- Bressie, Kent. «Submarine Cable Protection and Resilience», 2021.
- Brzozowski, Alexandra. «NATO Seeks Ways of Protecting Undersea Cables from Russian Attacks». www.euractiv.com, 23 ottobre 2020. <https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/>.
- Bueger, Christian, e Tobias Liebetrau. «Protecting hidden infrastructure: The security politics of the global submarine data cable network». Contemporary Security Policy 42, n. 3 (3 luglio 2021): 391–413. <https://doi.org/10.1080/13523260.2021.1907129>.
- Burnett, Douglas R. «Cable Vision». U.S. Naval Institute Proceedings, 1 agosto 2011. <https://www.usni.org/magazines/proceedings/2011/august/cable-vision>.
- Bush, Vannevar. "Science, The Endless Frontier: A Report to the President by Vannevar Bush, Director of the Office of Scientific Research and Development". July 1945
- Carrer, Gabriele, e Emanuele Rossi. «Che cos'è il Gugi, l'unità russa sospettata di sabotare i cavi sottomarini». Formiche.net, 6 novembre 2021. <https://formiche.net/2021/11/cavi-sottomarini-gugi/>.
- Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans – Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC.
- CCDCOE. «Strategic importance of, and dependence on, undersea cables», 2019. <https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf>.
- Clark, Bryan. «Undersea cables and the future of submarine competition». Bulletin of the Atomic Scientists 72, n. 4 (3 luglio 2016): 234–37. <https://doi.org/10.1080/00963402.2016.1195636>.

- Colombo, Matteo, Federico Solfrini, e Arturo Varvelli. «Network Effects: Europe's Digital Sovereignty in the Mediterranean – European Council on Foreign Relations». ECFR (blog), 4 maggio 2021. <https://ecfr.eu/publication/network-effects-europes-digital-sovereignty-in-the-mediterranean/>.
- Commissione europea. «Digital Day 2021: Europe to Reinforce Internet Connectivity with Global Partners | Shaping Europe's Digital Future», 19 marzo 2021. <https://digital-strategy.ec.europa.eu/en/news/digital-day-2021-europe-reinforce-internet-connectivity-global-partners>.
- Consiglio dell'Unione europea. «Una bussola strategica per la sicurezza e la difesa», 21 marzo 2022. <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/it/pdf>.
- Cooper, T. (2019) "Google and other tech giants are quietly buying up the most important part of the internet". Venturebeat <https://venturebeat.com/2019/04/06/google-and-other-tech-giants-are-quietly-buying-up-the-most-important-part-of-the-internet/>
- Crivellaro Edoardo e Wilegoda Lucas. 5G: opportunità di investimento ed implicazioni geopolitiche delle reti di quinta generazione. AWARE Think Tank. 2020
- Department of Justice (2020). The Committee for the assessment of Foreign Participation in the United States Telecommunications Services Sector - Frequently Asked Questions. <https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector#11>
- Fabbri, Dario. L'impero informatico americano alla prova cinese. Limes, rivista italiana di Geopolitica 10/2018 <https://www.limesonline.com/cartaceo/limpero-informatico-americano-alla-prova-cinese>
- Fabbri, Flavio. «Borrell: "L'UE deve diventare un provider di sicurezza ibrida, anche cyber"». CyberSecurity Italia (blog), 12 novembre 2021. <https://www.cybersecitalia.it/borrell-ue-leuropa-deve-diventare-un-provider-di-sicurezza-ibrida-anche-cyber/15173/>.
- Francola, Valerio, e Gordon A. Mensah. «L'industria dei cavi sottomarini: qualche elemento introduttivo». ASTRID RASSEGNA. Laboratorio sull'Ecosistema Digitale Astrid, 2021.
- Hantover, Lixian. «The Cloud And The Deep Sea: How Cloud Storage Raises The Stakes For Undersea Cable Security And Liability». Ocean and Coastal Law Journal 19, n. 1 (17 maggio 2014). <https://digitalcommons.maine.law.maine.edu/oclj/vol19/iss1/2>.
- Headrick D.R (1981) The Tools of Empire. Technology and European Imperialism in the Nineteenth Century, New York, Oxford: Oxford University Press

- Hookham, Mark, e Gabriel Pogrand. «Revealed: How Reporter Strolled into UK's 'Secure' Data-cable Sites». The Sunday Times, 4 febbraio 2018, par. news. <https://www.thetimes.co.uk/article/revealed-how-reporter-strolled-into-uks-secure-data-cable-sites-f6fx2hndv>.
- Martinage, Robert. «Under the Sea», 26 ottobre 2015. <https://www.foreignaffairs.com/articles/commons/under-sea>.
- Matis, Michael S. «The Protection of Undersea Cables: A Global Security Threat». ARMY WAR COLL CARLISLE BARRACKS PA, 7 marzo 2012. <https://apps.dtic.mil/sti/citations/ADA561426>.
- Mauldin, Alan. «466 Tbps: The Global Internet Continues to Expand», 2019. <https://blog.telegeography.com/466-tbps-the-global-internet-continues-to-expand>.
- McGillem, C. D. (2020, March 2). telegraph. Encyclopedia Britannica. <https://www.britannica.com/technology/telegraph>
- Miller, J. (2017). Submarine Cables: Are We in a New Bubble?. Telegeography Blog <https://blog.telegeography.com/ptc-submarine-cable-bubble-presentation-2017-market-summary>.
- Mims, C. (2022) Google, Amazon, Meta and Microsoft Weave a Fiber-Optic Web of Power. Wall Street Journal. <https://www.wsj.com/articles/google-amazon-meta-and-microsoft-weave-a-fiber-optic-web-of-power-11642222824>
- Ministerial Declaration. «European Data Gateways as a key element of the EU's Digital Decade», 19 marzo 2021.
- NATO. «Adapting NATO for 2030 and beyond - Speech by NATO Secretary General Jens Stoltenberg at the 66th Annual Session of the NATO Parliamentary Assembly». NATO, 2020. http://www.nato.int/cps/fr/natohq/opinions_179665.htm.
- ———. «Online Press Conference by NATO Secretary General Jens Stoltenberg Following the First Day of the Meetings of NATO Defence Ministers». NATO, 2020. http://www.nato.int/cps/en/natohq/opinions_178946.htm.
- Nyabiage, J. (2022). China's Peace cable linking Europe and Africa arrives in Kenya. South China Morning Post <https://www.scmp.com/news/china/diplomacy/article/3172463/chinas-peace-cable-linking-europe-and-africa-arrives-kenya>
- Parlamento Europeo. «Review of the Directive on security of Network and information systems». European Parliament, 2022. <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive>.
- Patriarca, Mattia. «La sicurezza dei cavi sottomarini: una sfida per l'Europa». Geopolitica.info (blog), 14 ottobre 2021. <https://www.geopolitica.info/cavi/>.

- Reverdy, D. & Skenderoski I. (2015) Submarine Cables: Structuring and Financing Options. Saliency Consulting White Paper https://saliencyconsulting.ae/wp-content/uploads/2018/09/Submarine_Cables_Structuring_and_Financing_Options_Jan_2015.pdf
- Ross, Margaret. «Understanding Interconnectivity of the Global Undersea Cable Communications Infrastructure and its Implications for International Cyber Security». The SAIS Review of International Affairs 34, n. 1 (2014): 141-55. <https://www.jstor.org/stable/27000949>.
- Schaub, Gary, Martin Murphy, e Frank G Hoffman. «Hybrid Maritime Warfare». The RUSI Journal 162, n. 1 (2 gennaio 2017): 32-40. <https://doi.org/10.1080/03071847.2017.1301631>.
- Sechrist, Michael. «New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems». Science, Technology, and Public Policy Program,. Belfer Center, 2012. <https://www.belfercenter.org/publication/new-threats-old-technology-vulnerabilities-undersea-communication-cable-network>.
- Sherman, Justin. «The U.S. Should Get Serious About Submarine Cable Security». Council on Foreign Relations, 2021. <https://www.cfr.org/blog/us-should-get-serious-about-submarine-cable-security>.
- Singel, Ryan. «Cable Cut Fever Grips the Web». Wired, 2008. <https://www.wired.com/2008/02/who-cut-the-cab/>.
- Smyth, Jamie (2017). Huawei's undersea cable project raises red flag in Australia. Financial Times. <https://www.ft.com/content/96513f58-d959-11e7-a039-c64b1c09b482>
- Spadaro, Irene, e Anna Pagnacco. «Geostrategic value of submarine internet cables». Center for Cyber Security and International Relations Studies (CCSIRS), 2021.
- Submarine Cable Networks. (2022). PLCN. <https://www.submarinenetworks.com/systems/trans-pacific/plcs>
- Submarine Telecom Forum: Industry Report 2021 <https://subtelforum.com/products/submarine-telecoms-industry-report/>
- Sunak, Rishi. «Undersea Cables, Indispensable, insecure». Policy Exchange, 2017.
- TeleGeography. «Submarine Cable Map», 2021. <https://www.submarinecablemap.com/>.
- The White House. (2022) Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector – . Retrieved 8 April 2022, from <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-establishing-committee-assessment-foreign-participation-united-states-telecommunications-services-sector/>

-

2022 Submarine Cable Map, TeleGeography & TelecomEgypt. Sono raffigurati 486 cavi e 1,306 landing stations.



AWARE

www.awarethinktank.it

info@awarethinktank.it

