La sicurezza cibernetica è strettamente legata alla dimensione subacquea, dove le infrastrutture digitali sono parte integrante della superficie d'attacco. Le minacce riguardano anche le intrusioni nei sistemi di controllo, l'esfiltrazione di dati e possibili forme di sabotaggio remoto. I punti più sensibili restano le stazioni di approdo e le reti di gestione, sempre più esposte alle tattiche ibride

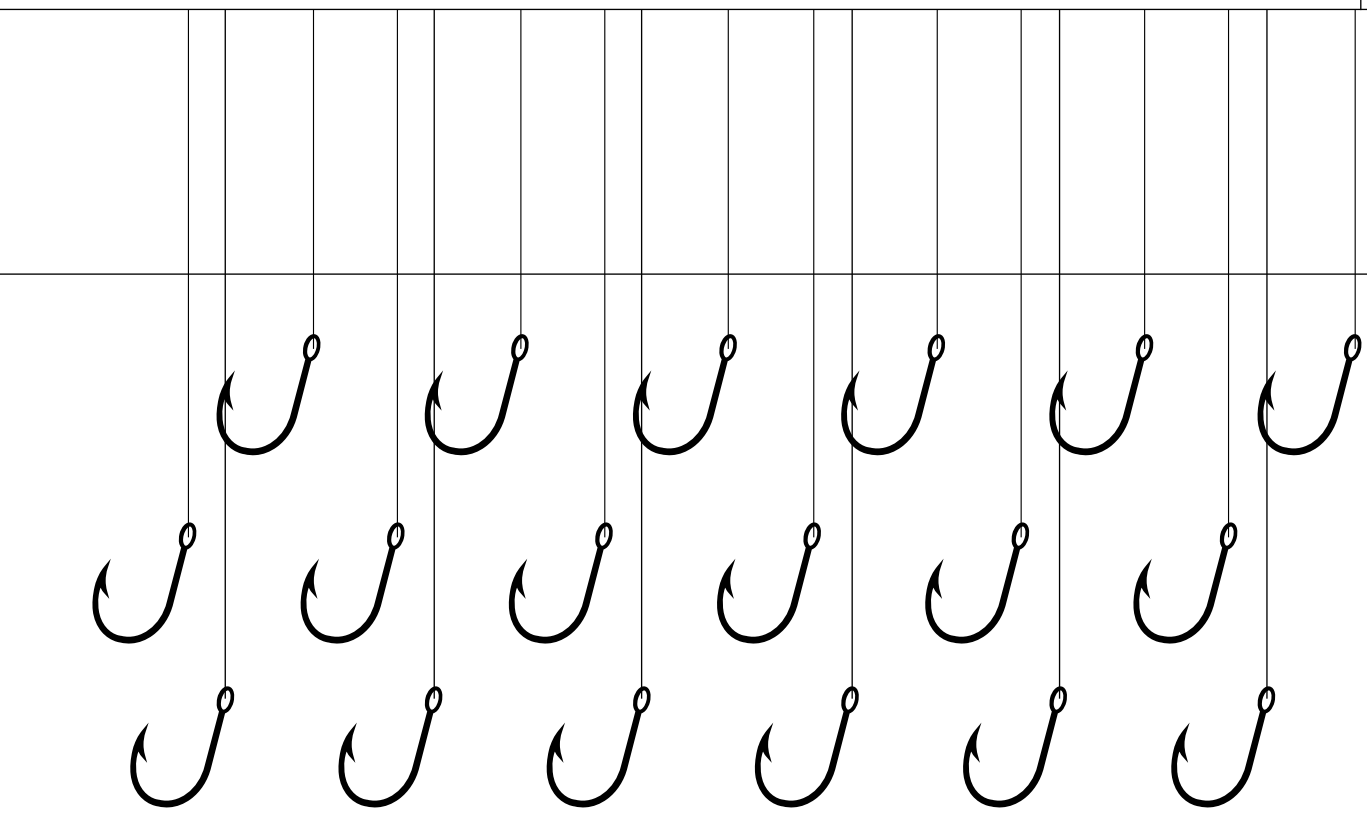
Quanta cyber-security passa dai cavi

MARCO BRACCIOLI
co-director Cybersec di Fondazione Icsa

Così come altri mondi anche l'ambiente subacqueo si sta fortemente antropizzando e in virtù di un confronto ibrido crescente tra potenze globali e regionali diventa terreno di scontro e confronto tra minaccia e deterrenza. Gli obiettivi son presto detti, a esclusione di quelli prettamente militari: piattaforme *offshore oil & gas*, reti di distribuzione ed alimentazione elettrica, fibre ottiche, campi eolici *offshore* (fissi e flottanti) e piattaforme innovative per le energie rinnovabili. La procedura di rilevamento danni segue un percorso ben preciso: rilevare e confermare il danno, localizzare, accedere all'area per l'investigazione, limitarne le conseguenze, reagire in emergenza e ripristinare. Fin qui tutto giusto, ma come prevedere o monitorare queste infrastrutture critiche? Per esempio, nel caso del gas le misure sono ben dettagliate dalla copertura anticorrosione, fino alla stesura in sottomarina di appesantimenti anti-flottaggio, mentre la pressione, la temperatura e il tasso di flusso vengono continuamente monitorati digitalmente attraverso un sistema di controllo remoto.

Secondo uno studio recente esistono globalmente 2,7 milioni di chilometri di cavi per dati ed energia e 1,2 milioni di chilometri di *pipeline oil & gas*. Il mercato *underwater* è stimato al 2050 in 400 miliardi di euro, oltre 30 miliardi in valore di soluzioni innovative e 10 miliardi in soluzioni di comunicazione subacquea. Soprattutto la spesa per l'innovazione riguarderà *data collection* e analisi, droni subacquei per monitoraggio e riparazione infrastrutture, nodi *multi-sensor* con *modem* acustici, *gateway* subacquei integrati anche alle reti *telco* e spaziali. Le principali necessità di comunicazione sia per il settore civile (infrastrutture critiche) che per quello militare (operazioni multi-dominio) sono: comunicazioni strategiche per unità subacquee che operano in profondità, scambio di dati ad alta velocità in emersione, comunicazioni tattiche bi-direzionali e a bassa latenza con unità subacquee in tutti gli scenari operativi, monitoraggio e controllo delle infrastrutture critiche sottomarine e Internet of underwater things. La sfida tecnologica è sicuramente legata alla trasmissione subacquea che può essere di tre tipi.

INTERNET OF UNDERWATER THINGS L'espressione descrive reti di sensori, *modem* acustici, *gateway* e piattaforme autonome distribuite sotto la superficie del mare e capaci di scambiarsi dati in modo continuo. È l'equivalente subacqueo dell'Internet delle cose, ma in un ambiente molto più ostile, dove comunicare è difficile e costoso. Il suo valore strategico sta nel fatto che permette di trasformare il fondale da spazio opaco a spazio monitorato, collegando infrastrutture energetiche, cavi, droni e sistemi di allerta dentro una stessa architettura digitale.



La prima è la radiofrequenza che attraversa facilmente i confini aria/acqua e non è influenzata da torbidità, salinità e gradienti di pressione. Inoltre è immune al rumore acustico, ha elevata larghezza di banda (fino a 100 Mb/s) a distanza molto ravvicinata ma è sensibile alle interferenze elettromagnetiche con una portata limitata in acqua, prediligendo quelle poco profonde. Successivamente, l'acustica è una tecnologia collaudata, con distanze fino a circa 20 chilometri, ma che presenta forti riflessioni e attenuazione durante la trasmissione attraverso il confine acqua/aria e scarse prestazioni in acque poco profonde. Inoltre, viene influenzata negativamente da torbidità, rumore ambientale, salinità e gradienti di pressione con una larghezza di banda limitata (qualche b/s fino a 20 kb/s).
Infine, l'ottica che presenta larghezza di banda ultraelevata (nel ordine di gigabit al secondo), ma non attraversa facilmente il confine acqua/aria, è sensibile a torbidità, particelle e incrostazioni marine e richiede una linea di vista diretta, un allineamento preciso dei nodi con raggio d'azione molto breve.

Venendo invece alla parte *cyber* relativa alle minacce ai cavi sottomarini, esse si possono condensare in macroaree: esfiltrazione di dati, dirottamento e presa di controllo degli *unmanned asset* per azioni malevole, *fishing*, attacco ai *data center* sottomarini e alle *pipeline*, interruzione delle comunicazioni. Un recente studio dell'International cable protection committee, tra il 2010 e il 2024, definisce che circa il 42% dei guasti ai cavi sottomarini è stato causato dall'attività di pesca e dall'ancoraggio, mentre un ulteriore 44% è in parte attribuito a sabotaggi volontari.
L'Unione europea ha istituito intorno alla struttura dei cavi sottomarini un quadro di sicurezza costituito dalle direttive Cer e Nis 2. La prima, in particolare, richiama gli Stati membri a adottare misure per rafforzare la resilienza dei soggetti critici e la protezione delle infrastrutture critiche. La seconda, invece, richiede ai soggetti che sono fornitori di infrastrutture e servizi digitali che gestiscono cavi sottomarini di proteggere i loro sistemi informatici e di rete, nonché il loro ambiente fisico da qualsiasi evento (*all-hazards*). È

stata inoltre pubblicata la Raccomandazione 2024/779 della Commissione europea per migliorare la sicurezza e la resilienza dei cavi sottomarini attraverso la mappatura di quelli esistenti (con aggiornamento almeno annuale), una valutazione di rischi, vulnerabilità e dipendenze, con specifica attenzione alla *supply chain*. Anche in tale logica si inserisce la definizione di un Cable security toolbox che definisca misure di mitigazione dei rischi, soprattutto rispetto ai fornitori ad alto rischio, lo scambio regolare di informazioni su incidenti, awareness e pratiche applicate e l'impiego di soluzioni innovative per l'individuazione e la deterrenza delle minacce contro le infrastrutture dei cavi sottomarini. Sempre più episodi recenti nel Baltico, nel Mediterraneo e nel mar Rosso sono sospettati di essere sabotaggi deliberati contro cavi di comunicazione o gasdotti, difficili da attribuire ma compatibili con operazioni di *seabed warfare*. Attori statali possono usare sottomarini, mini-sottomarini, Auv e navi civili di facciata per tagliare o danneggiare i cavi in punti strategici, creando interruzioni mirate o dimostrative nell'ambito della guerra ibrida. Oltre al taglio, una minaccia chiave è l'intercettazione clandestina del traffico: capacità militari profonde consentono di installare sonde o dispositivi lungo il cavo o nei ripetitori per leggere o deviare i flussi. In parallelo, campagne di *cyber*-spionaggio contro gli operatori mirano a ottenere accesso alle reti di gestione per monitorare o copiare comunicazioni sensibili senza interrompere il servizio. I punti più esposti sono le stazioni di approdo: qui convergono alimentazione, apparati ottici, *router* e sistemi Scada/Noc, spesso raggiungibili via rete dalle sedi centrali. Le vulnerabilità in questi sistemi possono permettere ad un attore di alterare configurazioni, spegnere segmenti di cavo, manipolare instradamenti o preparare sabotaggi fisici più precisi. I principali vettori di rischio sono: attacchi ai sistemi di controllo e supervisione della rete (con impatti sul bilanciamento e sulla continuità del servizio); sabotaggio fisico del cavo o dei punti di approdo (spesso difficile da attribuire con certezza); dipendenze da *data center*, consorzi e fornitori terzi, che ampliano la superficie d'attacco. Le misure di difesa principali sono: *asset discovery* e mappatura completa delle tratte e dei punti sensibili; centralizzazione dei controlli e monitoraggio continuo dei sistemi di sicurezza; sorveglianza marittima e capacità di risposta rapida, incluse riparazioni e ridondanza di rete; collaborazione tra Stati, Ue e operatori privati (perché la protezione non è solo tecnica ma anche organizzativa e strategica). Per la difesa fisica dei cavi, invece, si va verso una sensoristica sofisticata, che si può aggregare in questo modo: sensori in fibra ottica distribuiti (utili per rilevare vibrazioni, deformazioni e disturbi lungo la tratta); sensori di tensione e *strain* (per intercettare trazioni anomale sul cavo); sensori acustici e vibrazionali nei punti critici (soprattutto vicino agli approdi); sensori perimetrali e Cctv nelle *landing station* (per rilevare accessi o manomissioni fisiche); e, per ultimo vista l'attualità del tema, veniamo a Hormuz e ai cavi che passano nello stretto, questa è davvero la bomba nucleare nelle mani degli iraniani: la vulnerabilità dei cavi sottomarini. Le fonti citano sistemi come Aae-1, Falcon, Gulf Bridge International, Sea-Me-We e Tgn-Gulf tra quelli potenzialmente esposti nell'area. Un danno a questi collegamenti potrebbe rallentare Internet, disturbare le transazioni bancarie, la logistica, la telemedicina e le comunicazioni d'emergenza. In pratica, la crisi di Hormuz sui cavi sottomarini significa una vulnerabilità da guerra ibrida: il danno più probabile non è il collasso totale di internet, ma una degradazione seria e localizzata delle reti con impatti economici e finanziari importanti, e questa è un'altra delle cose che non ci possiamo certo permettere di questi tempi.

GATEWAY SUBACQUEI Sono i nodi che raccolgono, elaborano e instradano i dati provenienti da sensori e sistemi underwater verso reti più ampie, comprese quelle terrestri, telco o satellitari. In pratica fanno da ponte tra il mondo sommerso e quello emerso. La loro importanza cresce perché senza questi punti di raccordo i sensori restano isole separate, utili solo localmente. Con i *gateway*, invece, il monitoraggio dei fondali diventa una capacità integrata, che può sostenere manutenzione, sorveglianza, risposta alle emergenze e persino operazioni multi-dominio.