I cavi internet diventano obiettivi militari e preoccupano l'Occidente (seconda parte)

…Al contrario, gli stessi war games hanno concluso che la Russia, con limitate unità specializzate nel taglio dei cavi, *"non poteva sradicare rapidamente le fitte comunicazioni via cavo tra Nord America ed Europa".*

I governi occidentali si stanno affrettando a costruire difese migliori. La priorità è capire cosa sta realmente accadendo sott'acqua. Gli stati della **NATO** hanno già aumentato i pattugliamenti aerei e navali vicino alle infrastrutture critiche, compresi i percorsi dei cavi.

A maggio, l'alleanza ha convocato per la prima volta un nuovo **Critical Undersea Infrastructure Network,** con l'obiettivo di condividere più informazioni tra i governi e con le aziende private che solitamente gestiscono i cavi.

Un *"concetto di oceano digitale"* a ottobre ha anche previsto *"una rete di sensori su scala globale, dal fondale marino allo spazio"* per identificare le minacce.

Un'iniziativa dell'Unione Europea sta contemplando una rete di *"stazioni sottomarine"* sul fondale marino che potrebbero consentire ai droni di caricare le batterie e trasmettere dati su ciò che hanno visto.

Riparazioni complesse

Una volta che si è verificato un danno, ripararlo è difficile. Il mondo ha solo circa 60 navi di riparazione, il che significa che i guasti possono persistere per mesi. Molti non sono registrati né con gli Stati Uniti né con uno dei suoi alleati, nota **Evan D'Alessandro** del King's College di Londra, che studia i cavi sottomarini.

La sfida sarebbe aggravata in tempo di guerra, quando un taglio di cavi cinese si concentrerebbe in aree fortemente contese vicino alla costa di Taiwan.

Le navi di riparazione dei cavi dovevano essere scortate da navi da guerra nella prima e nella seconda guerra mondiale, nota D'Alessandro. In una guerra nel Pacifico, nota, le marine statunitensi e alleate avrebbero poche navi di riserva per questo compito.

In parte per mitigare questo problema, il Pentagono ha istituito una **Cable Security Fleet** nel 2021, in cui gli operatori di navi portacavi battenti bandiera americana e con equipaggio americano hanno ricevuto uno stipendio annuo di 5 milioni di dollari in cambio della prontezza a entrare in azione entro 24 ore durante una crisi e a prestare servizio in tempo di guerra.

La preoccupazione non è soltanto il sabotaggio, tuttavia, ma anche lo spionaggio. Gli Stati Uniti e i suoi alleati conoscono la minaccia meglio di chiunque altro visto che lo hanno fatto a loro volta. Negli anni '70, gli Stati Uniti hanno condotto operazioni audaci per intercettare i cavi militari sovietici utilizzando sottomarini appositamente equipaggiati in grado di posizionare e recuperare dispositivi sul fondale marino.

Spionaggio sottomarino cresciuto con Internet

Con la diffusione globale di Internet, le opportunità di spionaggio subacqueo sono aumentate rapidamente. Nel 2012, il **GCHQ**, il servizio di intelligence dei segnali del Regno Unito, aveva intercettato più di 200 cavi in □□fibra ottica che trasportavano traffico telefonico e Internet, molti dei quali raggiungevano comodamente la costa occidentale del paese.

L'agenzia avrebbe anche collaborato con l'Oman per intercettarne altri che attraversavano il Golfo Persico. La lezione, vale a dire il fatto che il percorso e la proprietà dei cavi possono essere vitali per la sicurezza nazionale, è stata appresa da altri.

Esplosione di cavi sottomarini in Asia

La paura dello spionaggio cinese è una delle ragioni per cui gli Stati Uniti hanno mostrato così tanto interesse per l'infrastruttura via cavo in rapida crescita dell'Asia.

Tra il 2010 e il 2023, nella regione sono stati lanciati circa 140 nuovi cavi, rispetto ai soli 77 nell'Europa occidentale. La Cina è diventata un attore importante nell'ondata di cavi tramite **HMN Technologies**, un'azienda precedentemente nota come **Huawei Marine Networks**, che dice di aver posato oltre 94.000 km di cavi in □□134 progetti.

Nel 2020, gli Stati Uniti, allarmati da questa tendenza, hanno bloccato il coinvolgimento di HMN in un cavo da 600 milioni di dollari da Singapore alla Francia, attraverso l'India e il Mar Rosso, noto come SeaMeWe-6, offrendo sussidi alle aziende concorrenti e minacciando sanzioni a HMN. Ciò avrebbe impedito alle aziende americane di utilizzare il cavo.

Questo è stato uno di almeno sei accordi sui cavi in Asia interrotti dagli Stati Uniti tra il 2019 e il 2023, secondo una recente indagine della *Reuters*.

Guai in paradiso

Gli alleati regionali degli Stati Uniti sono ugualmente desiderosi di contenere l'influenza cinese. Nel 2017, un progetto cinese per collegare l'Australia e le Isole Salomone nel Pacifico meridionale è stato ostacolato dal governo australiano, che ha avviato un progetto alternativo che coinvolgeva **Nokia**.

L'Australia sta ora finanziando altri due cavi per Palau e la Micronesia orientale, arcipelaghi in cui Cina, Stati Uniti e Australia si sono contesi l'influenza negli ultimi anni. Questi sforzi hanno ridotto drasticamente le ambizioni cinesi in materia di cavi.

HMN è ancora un pesce piccolo rispetto a **SubCom** degli Stati Uniti, **NEC Corporation** del Giappone e **Alcatel Submarine Networks** della Francia, il trio di aziende che domina il mercato globale dell'installazione di cavi.

Anche con una migliore sorveglianza subacquea e una maggiore ridondanza nei percorsi, è improbabile che la minaccia diminuisca. Il taglio dei cavi sottomarini in passato richiedeva ingenti investimenti navali. I droni navali sempre più capaci stanno cambiando le cose.

"La capacità di operare a profondità estreme potrebbe non essere più prerogativa esclusiva delle grandi potenze", dice **Sidharth Kaushal** del think-tank RUSI. La sfida per le potenze più piccole, dice, sarà spesso quella di identificare il percorso preciso dei cavi. Ciò potrebbe richiedere anni di sorveglianza in tempo di pace. Non c'è da stupirsi, quindi, che molti governi occidentali preferiscano tenere questi dettagli strettamente custoditi.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/i-cavi-internet-diventano-obiettivi-militari-e-preoccupano-loccidente-seconda-parte/500851/