ANÁLISIS 3

LOS CABLES SUBMARINOS COMO PROBLEMA DE SEGURIDAD NACIONAL: HACIA EL DESACOPLE DIGITAL CON CENTRO EN EL INDO PACÍFICO

Silvana Elizondo

Resumen

En los últimos cinco años, el tendido de cables submarinos a través de los océanos ha comenzado a ser considerado como un problema de seguridad nacional. Aunque la mayoría de los cortes de cables, bastante habituales, son causados por catástrofes naturales o por accidentes vinculados a actividades marítimas, emergen al menos dos escenarios que sitúan a los cables submarinos dentro de la competencia estratégica: por un lado, la posibilidad de cortes intencionales como una modalidad de coerción o agresión ejecutada en forma anónima en el marco de una estrategia de zona gris, o en forma abierta, en el contexto de una escalada; por otro lado, la interceptación de los datos, que puede resultar de actividades de espionaje o ciberataques.

El primer escenario, que es relativamente fácil de ejecutar y tiene consecuencias sumamente gravosas para los afectados, ha incentivado la elaboración de estrategias de seguridad para la protección de infraestructura crítica submarina, que serán objeto de una investigación próxima. El segundo escenario ha llevado a un inédito avance hacia el desacople de infraestructuras de conectividad submarina, a partir de los temores de espionaje recíproco. Estados Unidos ha vetado en los últimos años el tendido de cables que vinculen sus costas con las de China, y ha comenzado a operar activamente para que empresas chinas (principalmente HMN Tech) queden excluidas de cualquier proyecto de tendido de cables submarinos, incluso cuando no tocan sus costas. El Indo Pacífico es el centro focal del esfuerzo, pero sus consecuencias son globales. Beijing responde obstaculizando los permisos para el tendido de cables por los espacios que controla, especialmente el Mar del Sur de China, por temor al espionaje. Ello está llevando a que los nuevos cables se desplacen por fuera de la primera cadena de islas, cambiando la geopolítica del suelo marino.

Estas tendencias convergen en un desacople digital creciente, que puede ocasionar dificultades en el manejo de las grandes economías, aun ampliamente interdependientes, y transformar el futuro del procesamiento de datos a nivel global. Mientras el fenómeno ya ha adquirido rasgos muy definidos en el Indo Pacífico, en necesario tomar en consideración las posibles implicancias de esta cuestión en el espacio sudamericano, donde ya ha impactado en los proyectos de conectividad de Chile a través del Pacífico.

Introducción

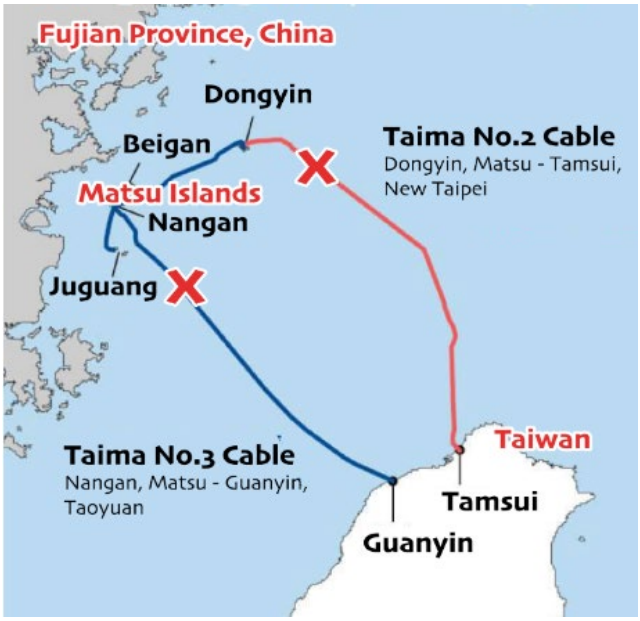
Entre el 2 y el 8 de febrero de 2023 la Isla de Matsu, perteneciente a Taiwán y cercana a China, se encontró súbitamente desconectada del mundo. Los dos cables submarinos de unos 50 kilómetros que la vinculan a la Isla de Taiwán fueron cortados una vez más, supuestamente por pesqueros chinos. Hasta tanto el gobierno taiwanés no logre su reparación, que llevará semanas y cientos de miles de dólares, los 13 mil habitantes de la isla viven un virtual bloqueo digital. La conexión vía satelital atiende solo las necesidades más urgentes [1].

Otros fenómenos de similares consecuencias tuvieron lugar en la región en años anteriores, con la ocurrencia de terremotos, tsunamis (Taiwán en 2006; Japón en 2011) y

erupciones volcánicas, como la ocurrida en Tonga en 2022, que la dejó aislada por meses.

Pero el episodio de Matsu es un ejemplo de un fenómeno ya evidente, en el que la conectividad - ahora de fibra óptica- vuelve a ser un objetivo militar accionable, aunque por el momento se mantenga dentro de los parámetros de no atribución y uso de medios civiles de coerción, propios de la estrategia de zona gris [2].

Este evento presenta similitudes con el sucedido en el Ártico hace algunos meses, cuando desaparecieron kilómetros de cables de una red de observación ambiental, de uso dual, desplegada por un centro de investigaciones marinas de Noruega, cuyos anclajes fueron además intencionalmente desplazados [3]. Según reportan fuentes occidentales, la preparación de este tipo de operaciones de coerción no militar podría explicar además el comportamiento que más de 50 buques civiles rusos despliegan actualmente en el Mar Báltico y en el Mar del Norte, alrededor de objetivos militares como cables de fibra



Fuente: The Diplomat, 5-4-23.

óptica, granjas eólicas y tuberías de gas [4]. No puede dejar de mencionarse, dentro de este paquete de nuevos escenarios submarinos, el caso del gasoducto de Nord Stream saboteado en septiembre de 2022, sin que aún se conozcan con certeza sus responsables y su propósito. Las últimas versiones, provenientes de la Armada danesa, sostienen que el barco de rescate submarino SS-750 de la armada rusa, que transportaba un minisubmarino con capacidad de sumergirse 80 metros, fue visto cerca de los oleoductos Nord Stream cuatro días antes de que explotaran, por lo cual se sospecha que podría ser el responsable del sabotaje [5].

Todos estos eventos, ocurridos en lugares distantes del planeta, permiten confirmar que la protección de las infraestructuras submarinas ya no puede estar limitada a la prevención de accidentes derivados de actividades como la pesca o la draga, o a la mitigación de efectos de desastres provocados por la naturaleza. La protección de la infraestructura crítica submarina es hoy una cuestión de seguridad que las estrategias nacionales abordan especialmente [6].

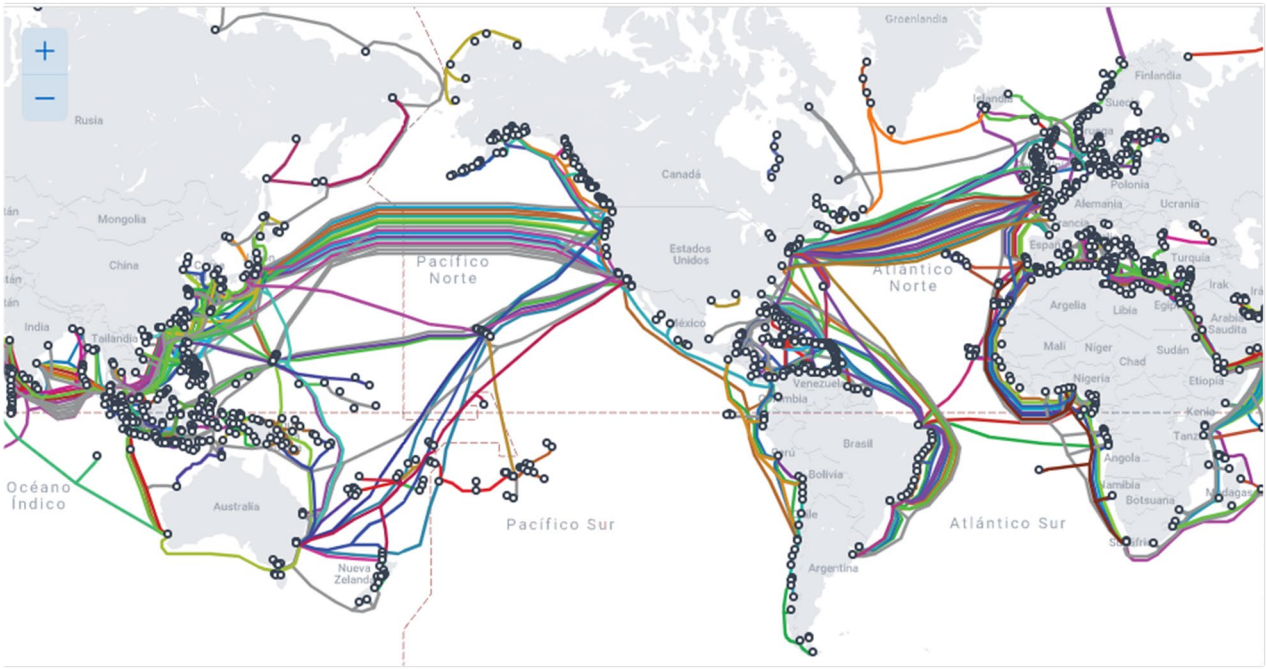
El propósito de este artículo es analizar uno de los principales componentes de la infraestructura crítica submarina, los cables submarinos, y su relación con la seguridad

nacional en el contexto de la competencia estratégica global. En este marco surgen al menos dos posibilidades: por un lado, que el tendido de cables, que está en manos de empresas civiles, pueda ser objeto de espionaje, manipulación y ciberataques por parte de actores hostiles; por otro lado, es posible que los cables sean deliberadamente cortados, ya sea en forma abierta o en el contexto de la no atribución, propia de la zona gris. Esta posibilidad está llevando a un claro desacople de infraestructuras. Aunque el fenómeno nace en el Indo Pacífico, ningún país, por distante que se encuentre, va a quedar al margen de sus consecuencias.

Analizaremos para ello la relevancia de los cables submarinos, el marco normativo y los riesgos y amenazas que se presentan alrededor de ellos, en el contexto de la competencia entre potencias. Luego describiremos las dinámicas del desacople digital entre Estados Unidos y China, con centro en el Indo Pacífico. Reflexionaremos, finalmente, acerca de las implicancias que estas dinámicas pueden tener para nuestra región.

Importancia de los cables submarinos

Como muestran los mapas globales elaborados por TeleGeography, una empresa de



: Telegeography. https://www.submarinecablemap.com/

Nota: Este mapa muestra los cables comerciales y no incluye todos los cables propiedad del gobierno, como los que se utilizan con fines militares y de inteligencia.

consultoría e investigación de mercado de telecomunicaciones radicada en Washington, los fondos marinos están atravesados por una red de cables de fibra óptica que conforma la dimensión física del ciberespacio, lo que la convierte en la infraestructura crítica central de la era digital. Transportan el 98% del tráfico global de internet y el 95% de las comunicaciones, sosteniendo el funcionamiento de los sistemas financieros, militares, de gobierno, comerciales, de seguridad, educativos, alcanzando prácticamente todos los ámbitos de la vida cotidiana. Las transacciones financieras que se realizan por esta vía, de unos 10 billones de dólares diarios, conforman la columna vertebral de la economía global.

Se registran actualmente 550 cables submarinos, que suman 1,4 millones de kilómetros de largo, uniendo a todos los continentes, menos la Antártida [7]. Estas cifras crecen año a año, ya que el crecimiento de la demanda, especialmente centrado en Asia, y la virtualización incentivada con la pandemia COVID 19 no han hecho más que multiplicar la presión sobre una capacidad bastante inelástica para fabricar y desplegar cables. “Con la tendencia actual hacia el trabajo remoto, el uso cada vez mayor del almacenamiento en la nube y la llegada de 5G e Internet de las cosas, la producción industrial, los servicios públicos y la vida de los ciudadanos dependerán aún más del buen funcionamiento de los cables submarinos”, sostiene el informe de la Unión Europea [8].

La fibra óptica transfiere datos cinco veces más rápido que los satélites y lo hace a un costo mucho más bajo. Éstos últimos representan solo el 0,37% de la conectividad para el caso de Estados Unidos [9], aunque, como ha demostrado la experiencia de SpaceX’s Starlink en Ucrania, los satélites de órbita baja están siendo vistos como un complemento necesario para suplir los cables submarinos en situaciones de crisis.

El nivel de dependencia respecto de esta infraestructura contrasta con sus vulnerabilidades. Las redes de cables submarinos no tienen habitualmente ninguna seguridad particular y carecen de un régimen de protección específica dentro del derecho internacional.

Buques especializados en la instalación de cables submarinos
Fuente: Voa News, 29-3-2023.

Marco normativo

La principal norma internacional que sigue rigiendo el tendido de cables submarinos es la Convención para la Protección de Cables Telegráficos Submarinos, que data de 1884, décadas después de que se desplegaron los primeros cables de telégrafo que atravesaban el Atlántico. Este régimen, que sigue vigente, con 36 estados parte, establece que romper o dañar un cable submarino, voluntariamente o por negligencia culposa, constituye un delito (a menos que tal acción sea necesaria para salvar la vida), pero sólo el estado de pabellón puede tomar medidas al respecto.

El tendido de cables submarinos de fibra óptica comenzó cien años después, en 1986, en reemplazo de los cables telefónicos. Esto implica que cuando se inició esta revolución en las comunicaciones globales ya se encontraba aprobada la Convención de las Naciones Unidas sobre Derecho del Mar (CONVEMAR), adoptada en 1982. En esta materia, la CONVEMAR recoge la normativa vigente, estableciendo que todos los estados son libres de tender cables y tuberías en el fondo marino y la plataforma continental hasta el límite de las 12 millas marinas [10]. Para tender un cable que atraviese el mar territorial de otro Estado, se necesita el permiso del estado ribereño. Pero más allá del mar territorial, el poder del estado ribereño para impedir o imponer condiciones sobre el lugar donde se tiende un cable es extremadamente limitado [11].

En línea con la Convención de 1884, la CONVEMAR establece en su artículo 113 que "Todo Estado dictará las leyes y reglamentos necesarios para que constituyan infracciones punibles la ruptura o el deterioro de un cable submarino en la alta mar, causados voluntariamente o por negligencia culpable por un buque que enarbole su pabellón o por una persona sometida a su jurisdicción, que puedan interrumpir u obstruir las comunicaciones telegráficas o telefónicas, así como la ruptura o el deterioro, en las mismas condiciones, de una tubería o de un cable de alta tensión submarinos." Además, la CONVEMAR no prohíbe que los estados traten a los cables como objetivos militares legítimos durante la guerra [12].

En la opinión de los especialistas, este marco normativo resulta insuficiente de cara a la radical transformación de la relevancia de estos tendidos para la seguridad nacional y para la vida cotidiana de las sociedades modernas. "El derecho internacional actual se adapta más al papel periférico que jugaban los cables en los años 70 y 80, en lugar del estatus indispensable que tienen hoy", afirmaba el actual primer ministro británico Rishi Sunak en 2016 [13]. El propietario del cable y el usuario perjudicado no tienen posibilidad de accionar contra los responsables de los cortes, sean éstos accidentales, por

negligencia o deliberados [14].

CORTE DE CABLES SUBMARINOS				
CAUSAS ACCIDENTALES		**CAUSAS INTENCIONALES**		
Catástrofes naturales	Actividades marítimas	Amenazas tradicionales		Amenazas no tradicionales
Terremotos Corrientes marinas Volcanes	Pesca Anclas Dragado	Zona gris/no atribución	Agresión abierta	Sabotaje
Ej: Taiwán 2006 Japón 2011 Tonga 2022	70% casos	Posiblemente Matsu Ártico		Egipto

Fuente: Elaboración propia sobre riesgos y amenazas vinculados al corte de cables submarinos

Riesgos asociados a accidentes y catástrofes

En relación a la seguridad física, la mayoría de los cables -que pueden tener entre 20 y 30 milímetros de ancho-, no tienen ningún blindaje y se apoyan en el fondo, pero en caso de lugares poco profundos o de alto tránsito están protegidos por una armadura de acero o se los entierra. Se registran aproximadamente 150 a 200 fallas de cables cada año en áreas de alto tránsito.

Algunos riesgos como los enredos de ballenas y las mordeduras de peces y tiburones se han resuelto técnicamente, pero los cortes por parte de artes de pesca, como redes de arrastre, palangres y dispositivos de concentración de peces, así como anclas y dragas, representan el 70% de los daños causados accidentalmente. Ya se han mencionado, por

Instalación de cables submarinos
Fuente: Reuters, 2023.

otro lado, los cortes vinculados a fenómenos naturales, como fuertes mareas, terremotos, tsunamis o volcanes.

Estados y empresas han buscado mejorar la resiliencia mundial de los cables submarinos a través de sistemas de detección automatizados, una mayor redundancia de rutas y la consolidación de una red de barcos de reparación [15]. Además, se buscan trayectorias que eviten las áreas geológicamente activas del lecho marino, como grietas activas, zonas de fallas y áreas que son propensas a deslizamientos de tierra submarinos. En general, se prefieren las aguas más profundas, ya que las aguas poco profundas son propensas

a que los cables se enganchen con la realización de actividades marítimas.

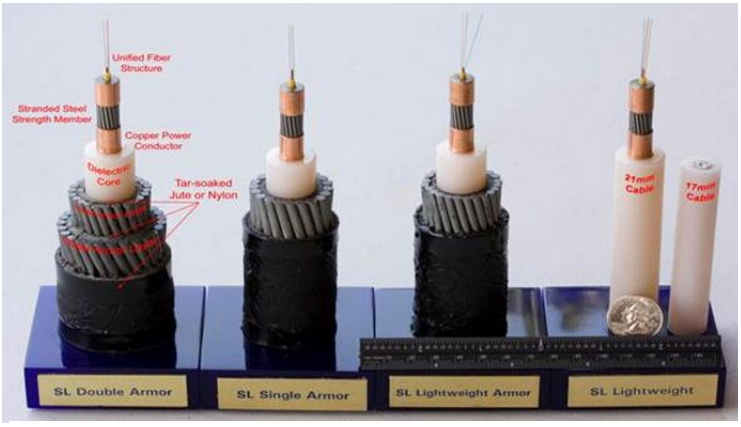
El Comité Internacional de Protección de Cables, una organización privada compuesta por 180 miembros estatales y comerciales que representan el 97 % de los cables de telecomunicaciones submarinos del mundo, publicó una guía voluntaria de mejores prácticas en 2021 que aborda algunos de estos problemas [16]. Para hacer frente a un accidente o sabotaje, existen organizaciones de nivel regional que coordinan entre los privados.

Se dispone de unos 59 buques especializados en el tendido de cables alrededor del mundo. Las banderas de los mismos pertenecen a Reino Unido, Francia, Islas Marshall, Singapur, Japón, China, Corea, Emiratos Árabes Unidos e Indonesia. Su contratación puede rondar los 100.000 dólares por día. Las reparaciones de cables dañados son más complejas que el tendido y generalmente se realizan con pequeños sumergibles especializados que reparan los cortes usando brazos robóticos o, en aguas menos profundas, con equipos de buceo [17].

Amenazas emergentes: sabotajes, espionaje y ciberataques

Al margen de estas interrupciones involuntarias, ha surgido como preocupación especial la posibilidad de que se produzcan daños deliberados a las redes de cables submarinos que, como hemos visto, resultan fáciles de cortar y pueden generar efectos gravísimos. Su ubicación precisa es posibilitada por la publicación de las trayectorias para evitar accidentes, las mejoras en los equipos de reconocimiento del fondo y los vehículos submarinos no tripulados. Además los puntos de terminación en tierra son particularmente vulnerables y más fáciles de encontrar que un cable sumergido.

Se identifican al menos dos formas de atacar los cables submarinos. Una es utilizando diferentes tipos de embarcaciones civiles (pesqueras, de investigación, de trasporte, de recreo) para desplegar dispositivos de corte improvisados, como anclas y herramientas de dragado. La segunda es a través de explosivos. Estos pueden llevarse a cabo mediante el uso de minas navales de grado militar o dispositivos explosivos improvisados marítimos, que pueden activarse de forma remota y son relativamente fáciles de fabricar [18].



Tipos de protección de los cables submarinos
Fuente: Burnett, 25-3- 2016.

Como sostiene Esteban Crespo Kennedy en una anterior edición del Boletín de este Observatorio, “atacar los cables de comunicación ha sido la norma de varios países durante conflictos militares, incluso en casos donde los propietarios de los cables no eran parte de estos. Ejemplos recientes muestran cómo un corte limitado de un par de cables

puede dañar la conectividad de millones de personas en varios continentes, afectar la provisión de servicios de internet como Google, Microsoft, Amazon o directamente dejar a países sin Internet, produciendo la caída de todos los servicios como correo, mensajería, bancos, comercio electrónico y demás" [19].

Es por ello que no puede descartarse un ataque abierto, múltiple y sincronizado a los cables submarinos, en el contexto de hostilidades, tal como ha ocurrido reiteradamente a lo largo de la historia [20]. Como señala Bryan Clark, "en una crisis, un agresor podría usar múltiples ataques coordinados en cables para obligar a un oponente a retroceder, o emplearlos como parte de una ofensiva inicial para aislar a las fuerzas militares del defensor de los comandantes nacionales, de los datos de inteligencia y de la información de sensores". Se especula, por ejemplo, que China podría cortar los cables que conectan a Taiwán con el mundo como una acción ofensiva inicial. Fuentes occidentales señalan que el buque de investigación ruso *Admiral Vladimirsky*, que navega las aguas cercanas a Dinamarca con el transponder apagado hace semanas, se encontraría mapeando posibles blancos para ataques o sabotajes en caso de escalada [21].

Asimismo, el corte de cables puede formar parte de ataques provenientes de actores no estatales. Aunque no se conocen todos los detalles del incidente, en 2013 tres buzos con herramientas manuales cortaron el cable principal que conectaba a Egipto con Europa, reduciendo el ancho de banda de Internet del país en un 60 %. Este caso permitió exponer la magnitud de las consecuencias para el funcionamiento del estado y la sociedad derivados de los problemas de conectividad.

A pesar de que la interrupción física de los cables parece ser el uso militar más lineal, existen fuertes temores sobre la posibilidad de interceptar datos que fluyen por los cables, ya que las comunicaciones militares también utilizan estas redes, aunque con mayores medidas de seguridad [22]. Justin Sherman, miembro de *Cyber Statecraft Initiative* del *Atlantic Council*, afirmó: "Cuando hablamos de competencia tecnológica entre Estados Unidos y China, cuando hablamos de espionaje y captura de datos, los cables submarinos están involucrados en todos los aspectos de esas crecientes tensiones geopolíticas" [23]. Los cables submarinos son "una mina de oro de vigilancia" para las agencias de inteligencia del mundo, agregó [24]. Existen antecedentes que justifican la preocupación, como un incidente sospechoso de 2019 durante el cual el tráfico de algunas de las redes móviles más grandes de Europa se enrutó a través de China Telecom durante poco más de dos horas [25]. Aun así, se considera que con los niveles actuales de encriptación esa tarea sería muy dificultosa y poco eficiente, y las promesas de la criptografía cuántica ofrecerían aún más seguridad a los datos.

Los cables también pueden ser objetivos de ataques cibernéticos, como el efectuado a un cable de telecomunicaciones que conecta Hawái y la región del Pacífico en 2022 [26]. El hackeo de los cables puede permitir robar información personal o financiera, pedir rescate para liberar los sistemas o causar una interrupción generalizada en las comunicaciones.
Estas preocupaciones de seguridad llevaron a los gobiernos a involucrarse directamente en una actividad que estuvo siempre gestionada entre privados, lo que devino en múltiples condicionalidades y prohibiciones que están llevando hacia un verdadero desacople digital o balcanización de las redes [27].

TIPO DE ATAQUE A LOS CABLES SUBMARINOS	Corte físico de los cables	Espionaje datos	Ciberataque
RESPUESTAS	Redundancia Estrategias de protección infraestructura crítica submarina (seabed warfare) Reparación eficiente	Desacople de redes Encriptación	

Fuente: Elaboración propia en torno a las respuestas posibles frente a diferentes tipos de ataques

Hacia el desacople digital

A pesar de ofrecer servicios esenciales, el mercado de los cables submarinos está manejado por privados, que cumplen diferentes roles. Por un lado se encuentran los consorcios de empresas e inversores que construyen los cables submarinos y venden la capacidad a los operadores. Algunos de los proveedores más grandes incluyen Alcatel Submarine Networks y Nexans (Francia), Prysmian Group (Italia), NKT A/S (Dinamarca), SubCom (Estados Unidos), NEC (Japón) y Huawei Marine Networks (China) [28].

Por otro lado, se encuentran las empresas de telecomunicaciones (p. ej., AT&T, Verizon, Deutsche Telekom, China Mobile) y los proveedores de contenido, como Google, Meta, Microsoft y Amazon, que construyen sus propios cables submarinos para garantizar la interconexión de sus centros de datos. Según TeleGeography, estas últimas, consideradas "hiperescaladores", agregaron capacidad a una tasa anual del 70 % entre 2015 y 2019, en seis de las siete regiones del mundo, convirtiéndose en los principales propietarios de la capacidad de cableado submarino [29].

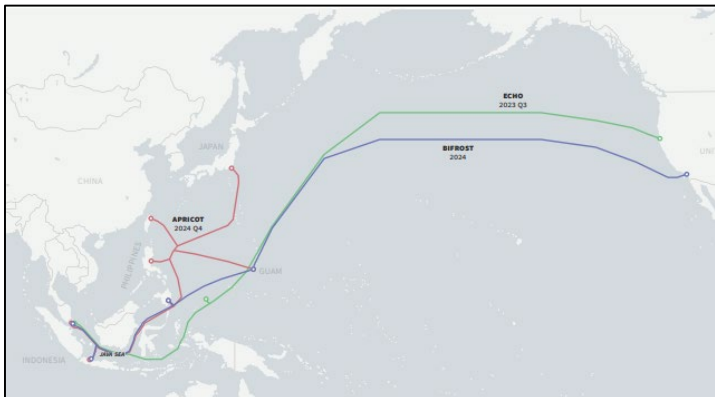
El manejo privado de estas redes de comunicación no constituía una preocupación de seguridad nacional hasta que, en 2008, Huawei irrumpió en el mercado a través de su subsidiaria HMN Technologies Co Ltd [30]. HMN Tech se convirtió en poco tiempo en la empresa con mayor expansión dentro del negocio, desplazando a la estadounidense SubCom, la japonesa NEC Corporation y la francesa Alcatel Submarine Networks, Inc. [31]. Como parte de la iniciativa Digital Silk Road, China subvenciona sus proyectos de 5G en todo el mundo, buscando un liderazgo en el mercado y una participación en el establecimiento de estándares globales. Estas subvenciones permiten a la empresa china realizar ofertas hasta 30% inferiores al precio de sus competidoras, por lo que está en condiciones de ganar todas las licitaciones, incluso se impuso en Estados Unidos en un primer momento.

En 2020 el gobierno de Estados Unidos denunció que Huawei tenía puertas traseras en su red que iban más allá de las que a veces solicitan los gobiernos anfitriones como parte de interceptaciones legales, [32] por lo cual la empresa fue incorporada dentro de una lista de restricciones para el acceso a la tecnología (Bureau of Industry and Security Entity List). Para evitar limitaciones, Huawei Marine fue vendida en 2020 a Hengtong Group, otra empresa china, y renombrada como HMN Technologies Co, pero al año siguiente ésta fue también incorporada en la lista negra.

Este veto forma parte de una política sistemática de desacople por parte de Estados Unidos, liderada por el llamado Team Telecom [33], un equipo interagencial que asesora a la Federal Communications Commission (FCC) [34], encargada de aprobar las licencias vinculadas a proyectos de comunicaciones. La FCC ha logrado la cancelación de numerosos cables impulsados por Google, Meta y Amazon, que vincularían Estados Unidos con Hong Kong, especialmente luego de que la ciudad perdiera los niveles de autonomía de los que gozaba hasta 2020 [35]. Ello demandó a las empresas replantear el tendido de sus cables, que ahora no llegan a Hong Kong sino que finalizan en terminales aliadas como Filipinas, Taiwán, Indonesia o Japón.

Un primer indicio del desacople había tenido lugar en 2018, cuando Australia resolvió financiar el cable Coral Sea para proveer conectividad a las Islas Salomon y Papúa Nueva Guinea y así evitar que Huawei realizara el tendido entre las Islas Salomon y Sidney.

Entre los proyectos cancelados o rediseñados por Estados Unidos a partir de 2020 se encuentran los cables Hong Kong - Guam (HK-G) y Hong Kong - ESTADOS UNIDOS (HK-A); el Pacific Light Cable Network, de Google y Meta, que solo llegará a Filipinas y Taiwán; el Bay to Bay Express (BtoBE), desarrollado por Amazon, Meta y China Mobile, que estaba previsto unir Singapur, Hong Kong y California y ahora solo unirá California y Filipinas



Tendido de nuevos cables submarinos por fuera de la Primera Cadena de Islas
Fuente: Telegeography, en CSIS, 2023.

(CAP-1), excluyendo a la compañía china [36].

Una dinámica similar se reiteró en 2021, cuando Australia, Japón y Estados Unidos anunciaron planes para financiar un nuevo cable que unirá Guam, Micronesia y las Islas Marshall (HANTRU-1), bloqueando la participación de China [37].

En 2022 la atención se centró en el cable de fibra óptica SeaMeWe-6, que unirá Asia y Europa a través de África y Medio Oriente, sin tocar territorio chino ni estadounidense. Este negocio estaba prácticamente cerrado en 2020 en beneficio de la china HMN Technologies, que ofrecería el servicio a un precio un tercio inferior al de sus competidoras. Los cables prestarían servicio a un consorcio de 12 compañías, entre las que se encontraban las tres grandes empresas de telecomunicaciones chinas (China Telecom, China Mobile, China Unicom). Para revertir este hecho prácticamente consumado, altos diplomáticos estadounidenses se reunieron con los ejecutivos de empresas de telecomunicaciones involucradas, advirtiéndoles que las empresas tecnológicas estadounidenses no podrían usar el cable debido a las sanciones sobre HMN Tech. Como resultado de estas presiones y un paquete de incentivos, Estados Unidos logró que este cable quede en manos de la compañía estadounidense SubCom LLC.

En una maniobra que espeja esta desconfianza, China obstaculiza el denominado cable 2 Sudeste Asiático Japón, que partiría desde Singapur y tocaría Hong Kong y China continental antes de continuar a Corea del Sur y Japón. China ha retrasado la concesión de la licencia para que el cable pase por el Mar de China Meridional, preocupada de que el fabricante del cable, NEC de Japón, inserte equipos de espionaje en la línea. Es oportuno observar, en este sentido, que China entiende que los tendidos de cable por el Mar del Sur de China deben ser autorizados, aun cuando, además de ser un área en litigio, la CONVEMAR establece que solo se requiere permiso del estado ribereño para tender cables en el mar territorial, dentro de las 12 millas marinas. Según declaraciones de Bryan Clark, ex oficial de submarinos de EE. UU., al *Finantial Times*, "China está tratando de ejercer más control sobre las actividades submarinas en su región, en parte para evitar que se instalen sistemas de vigilancia de Estados Unidos dentro del despliegue de cables submarinos" [38]. Estados Unidos ha utilizado frecuentemente los cables para inteligencia, en especial en la Guerra Fría pero también en tiempos recientes, a través de las capacidades de la Agencia Nacional de Seguridad.

Así, las exigencias de China se suman a la política de desacople de Washington para redibujar el trazado de todos los nuevos cables de la región, que ahora se despliegan casi enteramente por fuera de la primera cadena de islas, al este de Indonesia (Cables Apricot, Echo y Bifrost).

Según señala Geoff Huston, "Hay una realineación en el Pacífico occidental con nuevos sistemas de comunicaciones submarinos que se desplazan hacia el Este del Mar de China Meridional y el Estrecho de Luzón" [39]. Según el autor, los nodos seguirían siendo Singapur y Japón, pero Hong Kong sería gradualmente reemplazado por Guam, que gana protagonismo a partir de este rediseño. Un desacople que puede afectar el papel de Estados Unidos en el almacenamiento y procesamiento de datos a nivel global, ya que las empresas chinas buscarán instalar sus estaciones en otros países e impulsarán nuevos centros de datos.

Finalmente, un caso menos comentado dentro de este desacople pero que nos concierne en forma cercana es el de Chile, que también ha cambiado de recorrido y proveedor de su cable transpacífico en el marco de estas presiones. Chile proyectaba en 2017 participar del primer cable que uniría Asia y Sudamérica en forma directa, impulsado por Huawei y que incluiría un nodo en Shanghai. La propuesta debió ser dejada de lado por presiones de Estados Unidos, y finalmente el cable submarino Humboldt unirá Valparaíso y Sydney, con potencial de alcanzar otros países, como Brasil y Argentina [40].

Conclusiones

Los cables submarinos forman una parte esencial de la dimensión física que sostiene la era digital. Ello nos exime de señalar la relevancia que éstos tienen para la seguridad nacional de los estados. Aunque la dependencia de los cables de fibra óptica lleva décadas de expansión, el fenómeno que irrumpe con intensidad desde el año pasado es, claramente, la entrada de los cables submarinos en los cálculos ofensivos de la competencia estratégica. Hasta el momento, dentro de la ambigüedad y no atribución de la estrategia de zona gris, pero con enorme potencial para convertirse en blancos muy redituables en un conflicto caliente, como lo han sido las infraestructuras de comunicaciones en el pasado. Se trata de una red muy vulnerable y al mismo tiempo vital, que está caracterizada por la redundancia y la encriptación como principales medidas de resiliencia.

Dos aspectos complejizan la cuestión de los cables submarinos desde el punto de vista de su protección y manejo: por un lado, un marco normativo del siglo XIX, que impide accionar contra afectaciones supuestamente accidentales, entre otras limitaciones. La preocupación compartida por los diferentes actores sobre las vulnerabilidades de los cables para su seguridad podría ser un punto de arranque para compromisos normativos. Por otro lado, la naturaleza privada de la red, que obliga a los estados a recurrir a mecanismos complejos para atender las necesidades de seguridad nacional, especialmente en aquellos países que tienen sistemas abiertos.

Los desafíos relacionados con la protección física han tenido como respuesta el despliegue de estrategias de vigilancia de la infraestructura crítica submarina, un esfuerzo que demanda capacidades particulares y que recién está tomando forma. Los puntos de entrada a tierra y los cuellos de botella (choke points) en el tendido de cables son espacios que se convierten naturalmente en focos especiales de atención. En relación a la protección de los datos que fluyen por los cables, que pueden ser violados por medio de ciberataques o interceptaciones, la estrategia ha devenido en medidas más radicales, llevando a un creciente desacople de consecuencias aún no mensurables.

Estados Unidos despliega una política tardía pero consistente, con centro en el Indo Pacífico, para evitar que China se apodere del control de las redes y lidere el establecimiento de estándares a través de prácticas de subsidios. Algunos especialistas advierten, sin embargo, que Estados Unidos puede poner en riesgo su ventaja estratégica a través del desacople, favoreciendo la reubicación de cables y *hubs* en países no amigos y padeciendo cierta latencia, que le haría perder competitividad en aplicaciones en tiempo real.

No es el propósito de esta breve investigación profundizar aspectos técnicos de las telecomunicaciones, que demandan una mirada especializada, sino poner de manifiesto cómo, a partir de este tema particular que tiene un fuerte efecto multiplicador, se van anticipando tendencias de fragmentación que conviven incómodamente con la interdependencia, y generan presiones múltiples sobre todos los países.

Los escenarios que pueden derivarse de esta balcanización son variados, pero ninguno es muy auspicioso. No parece estar claro aún cómo va a evolucionar una economía global con redes fragmentadas. Por otro lado, nadie puede evaluar con precisión qué sucedería si los cables que conectan países y continentes lograran ser cortados simultáneamente por el enemigo, por más redundantes que sean.

NOTAS

[1] Elisabeth Braw (February 21, 2023) China Is Practicing How to Sever Taiwan's Internet. Foreign Policy; Huizhong Wu y Johnson Lai (5 marzo 2023). Taiwan suspects Chinese ships cut islands' internet cables. AP'sNews. https://apnews.com/article/matsu-taiwan internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70; Wen Lii (April 15, 2023) After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience. The Diplomat. https://thediplomat.com/2023/04/after-chinese vessels-cut-matsu-internet-cables-taiwan-shows-itscommunications-resilience/.

[2] Para características de la estrategia de zona gris y guerra híbrida ver: Silvana Elizondo (Abril 2021) La escalada en la zona gris y el escenario marítimo: el caso de los Mares de China. Observatorio Estratégico de los Mares de China. Escuela Superior de Guerra Conjunta de las Fuerzas Armada. https://www.esgcffaa.edu.ar/maresdechina/boletin/boletin2-04-

2021.pdf

[3] Thomas Newdick (Jan 10, 2022). Undersea Cable Connecting Norway With Arctic Satellite Station Has Been Mysteriously Severed. The Wire. https://www.thedrive.com/the-war zone/43828/undersea-cable-connecting-norway-with-arctic satellite-station-has-been-mysteriously-severed

[4] Morten Soendergaard Larsen (2 de mayo de 2023). Russian 'Ghost Ships' Are Turning the Seabed Into a Future Battlefield. Foreign Policy. https://foreignpolicy.com/2023/05/02/russia europe-denmark-spy-surveillance-ships-seabed-cables/? tpcc=recirc_latest062921

[5]Rachael Bunyan (28 April 2023). Russian navy vessel carrying a mini-submarine was seen near Nord Stream pipelines four days before they were blown up. Daily Mail.https://www.dailymail.co.uk/news/article-12024925/Russian navy-vessel-seen-near-Nord-Stream-pipelines-four-days-blown up.html

[6] Una de las primeras estrategias integrales es la de Francia, que en 2022 publicó su Seabed Warfare Strategy.

[7] TeleGeography. https://www2.telegeography.com/, en: Xiaoshan Xue y Adrianna Zhang (March 29, 2023). Tensions With China Emerge Over Undersea Cables Carrying Internet Traffic. VOA Mandarin. China News. https://www.voanews.com/a/tensions-with china-emerge-over-undersea-cables-carrying-internet traffic/7027809.html

[8] Christian Bueger, Tobias Liebetrau, Jonas Franken (June 2022) Security threats to undersea communications cables and infrastructure –consequences for the EU. European Parliament.

[9] Xiaoshan Xue y Adrianna Zhang, op. cit.

[10] Douglas R. Burnett (25 March 2016). Submarine Cables and the UNCLOS. Squire Patton Boggs. squirepattonboggs.com. Se refieren además a los cables submarinos la Convención sobre la Plataforma Continental, la Convención de Alta Mar, ambas de 1958, y el Reglamento de abordajes de 1972.

[11] Los artículos 21, 58, 79, 87 y 112 a 115 de la CONVEMAR establecen los criterios para el tendido de cables y tuberías. Para el caso del tendido de tuberías (no los cables) en la plataforma continental, si bien el estado ribereño no puede rechazarla, debe brindar el consentimiento sobre su trazado.

[12] Rishi Sunak (2017). "Undersea Cables Indispensable, insecure". Policy Exchange UK.

[13] Rishi Sunak, ibid.

[14] Karen Scott (January 21, 2022) Laws governing undersea cables have hardly changed since 1884 – Tonga is a reminder they need modernising. The Conversation. https://www.canterbury.ac.nz/news/2022/laws-governing undersea-cables-have-hardly-changed-since-1884-tonga-is-a reminder-they-need-modernising.html

[15] Bueger et al., op, cit.

[16] Scott, op cit.

[17] Sunak, op. Cit.

[18] Bueger et al., op, cit.

[19] Esteban Crespo Kennedy (Agosto 2022). Daños colaterales: las posibles implicancias para Argentina de un conflicto convencional entre China y Estados Unidos. Boletín nro. 13 - Observatorio Estratégico de los mares de China. ESGFFAA.

[20] Rush Doshi y Kevin Mcguiness (Marzo 2021) Huawei meets history. Great powers and telecommunications risk, 1840-2021. Brookings Institution. https://www.brookings.edu/research/huawei-meets-history-great powers-and-telecommunications-risk-1840-2021/

[21] Gordon Corera (19 April 2023). Ukraine war: The Russian ships accused of North Sea sabotaje. BBC.

[22] De hecho, algunos de estos cables que conectan Europa a los Estados Unidos fueron los que intervino la Agencia de Seguridad Nacional de EE. UU. para escuchar a la entonces canciller alemana, Angela Merkel. En: Morten Soendergaard Larsen, op. Cit.

[23] Xiaoshan Xue y Adrianna Zhang , op. Cit

[24] Joe Brock (March 24, 2023). U.S. and China wage war beneath the waves – over internet cables. Reuters Special Report. https://www.reuters.com/article/us-china-tech-cables idUSL1N35U2ZZ. Xiaoshan Xue y Adrianna Zhang, op. Cit.

[25] Matthew P. Goodman and Matthew Wayland (abril 2022). Securing Asia's Subsea Network U.S. Interests and Strategic Options. CSIS BRIEFS | WWW.CSIS.ORG.

[26] Jamie Tarabay (20 de abril de 2022). An Underwater Hack and the Digital Ripple Effects. Bloomberg. https://www.bloomberg.com/news/newsletters/2022-04-20/an underwater-hack-and-the-digital-ripple-effects.

[27] Matthew P. Goodman and Matthew Wayland op. cit.

[28] Además, hay que tener en cuenta las compañías de fabricación de cables de fibra óptica, como Corning, y las que proveen los equipamientos de las terminales y componentes de transmisión (como las norteamericanas Infinera, Ciena, and Cisco). (CSIS)

[29] Matthew P. Goodman and Matthew Wayland, op. Cit.

[30] Jill C. Gallagher (September 13, 2022). Undersea Telecommunication Cables: Technology Overview and Issues for Congress Congressional Research Service https://crsreports.congress.gov

[31] Geoff Huston (June 05, 2022). The Politics of Submarine Cable in the Pacific. Circle id. https://circleid.com/posts/20220605-the politics-of-submarine-cable-in-the-pacific

[32] Rush Doshi y Kevin Mcguiness. op. cit.

[33] Formalmente se trata del Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, a cargo del Departamento de Justicia.

[34] Farhad Jalinous, Ryan Brady y Michael Crowley (25 April 2022) Team Telecom Two-Year Anniversary.
https://www.whitecase.com/insight-alert/team-telecom-two-year anniversaryTeam Telecom Two-Year Anniversary

[35] Geoff Huston, op. Cit.. Gallagher, op. Cit.

[36] Joe Brock, op. cit.; Jill C. Gallagher; op. cit.

[37] Geoff Huston. op. cit.

[38] Anna Gross et al. (Marzo 13 2023). China exerts control over internet cable projects in South China Sea Beijing imposes strict permit requirements for access to underwater data infrastructure over spying fears Finantial Tmes, https://www.ft.com/content/89bc954d-64ed-4d80-bb8f 9f1852ec4eb1.

[39] Geoff Huston. op. cit.

[40] Digital Economy Partnership Agreement (Singapore, New Zealand, y Chile, 2020).Carlos Solar 31 (January 2023). For Latin American Countries, Geopolitical Competition Begins at Sea. RUSI. https://rusi.org/explore-our research/publications/commentary/latin-american-countries geopolitical-competition-begins-sea