

Vadear aguas turbias

***Cables submarinos de
telecomunicaciones y
comportamiento
responsable de los Estados***

CAMINO KAVANAGH

AGRADECIMIENTOS

El apoyo de los patrocinadores principales del UNIDIR proporciona los cimientos de todas las actividades del Instituto. Este informe forma parte de la línea de trabajo en materia cibernética dirigida por el Programa de Seguridad y Tecnología del UNIDIR, financiado por los Gobiernos de Alemania, Chequia, Francia, Italia, Países Bajos, Suiza y Reino Unido, así como por Microsoft. La autora desea expresar su agradecimiento al diverso grupo de expertos de la industria, del gobierno y del mundo académico que han aportado comentarios sustanciales a las distintas iteraciones y secciones de este documento.

SOBRE EL UNIDIR

El Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) es un instituto autónomo de las Naciones Unidas financiado con contribuciones voluntarias. UNIDIR, uno de los pocos institutos de políticas del mundo dedicado al desarme, genera conocimientos y promueve el diálogo y medidas en materia de desarme y seguridad. Tiene su sede en Ginebra, y ayuda a la comunidad internacional a desarrollar las ideas prácticas e innovadoras necesarias para hallar soluciones a problemas críticos para la seguridad.

CITACIÓN

C. Kavanagh: *Vadear aguas turbias: cables submarinos de telecomunicaciones y comportamiento responsable de los Estados*. Ginebra, Suiza: UNIDIR, 2023.

NOTA

Las denominaciones empleadas en esta publicación y la forma en que aparecen presentados los datos que contiene no implican, de parte de la Secretaría de las Naciones Unidas, juicio alguno sobre la condición jurídica de países, territorios, ciudades o zonas, o de sus autoridades, ni respecto de la delimitación de sus fronteras o límites. Las opiniones expresadas en la presente publicación son responsabilidad exclusiva de sus autores. No reflejan necesariamente las opiniones de las Naciones Unidas, de UNIDIR, o de sus funcionarios o patrocinadores.

ÍNDICE

SOBRE EL PROGRAMA DE SEGURIDAD Y TECNOLOGÍA.....	2
ABREVIATURAS Y ACRÓNIMOS	3
Resumen.....	4
Introducción	5
¿Qué contiene un cable de comunicaciones submarino moderno?	8
Amenazas y vulnerabilidades	15
El régimen de gobernanza de los cables submarinos de telecomunicaciones.....	22
¿Cuál es el futuro de la gobernanza de los cables submarinos?	27
Análisis de los esfuerzos seleccionados.....	29
Sentar las bases para una mayor resiliencia de los sistemas de cables submarinos a escala mundial	34
Conclusiones.....	37

SOBRE EL PROGRAMA DE SEGURIDAD Y TECNOLOGÍA

Los avances actuales de la ciencia y la tecnología presentan nuevas oportunidades y desafíos para la seguridad internacional y el desarme. El Programa de Seguridad y Tecnología (SecTec) del UNIDIR tiene por objeto fomentar el conocimiento y concienciar sobre las implicaciones y los riesgos para la seguridad internacional que plantean determinadas innovaciones tecnológicas, así como alentar a las partes interesadas a explorar ideas y desarrollar nuevos pensamientos para darles solución.

SOBRE LA AUTORA

Camino Kavanagh es investigadora superior visitante en el King's College de Londres y experta visitante en la Carnegie Endowment for International Peace. También trabaja como consultora internacional en cuestiones relacionadas con la cibernética, las tecnologías emergentes, la seguridad internacional y los conflictos. Camino actuó como asesora de los presidentes del Grupo de trabajo de composición abierta (GTCA) 2019-2021 y del Grupo de Expertos Gubernamentales (GEG) sobre las TIC y la seguridad internacional. Asimismo, fue relatora/consultora del GEG 2016-2017 en esta misma materia.

ABREVIATURAS Y ACRÓNIMOS

GEG	Grupos de Expertos Gubernamentales
ICPC	Comité Internacional para la Protección de los Cables
TIC	Tecnología de la información y las comunicaciones
GTCA	Grupo de trabajo de composición abierta
CNUDM	Convención de las Naciones Unidas sobre el Derecho del Mar

Resumen

Este informe trata sobre los cables submarinos de telecomunicaciones. Estos cables constituyen un elemento esencial del ecosistema de la tecnología de la información y las comunicaciones (TIC), ya que a través de ellos se transmiten prácticamente todas nuestras telecomunicaciones y datos. Su seguridad y resiliencia son fundamentales para el bienestar y el funcionamiento de las sociedades de todo el mundo, así como para la seguridad y la estabilidad internacionales. Gracias a los avances tecnológicos, es posible transmitir datos a través de cables submarinos de telecomunicaciones a velocidades que difícilmente podrían haberse imaginado hace unos 150 años, cuando se tendieron los primeros cables en el lecho marino. Estos hacen posible la conectividad entre países y regiones históricamente remotos o desatendidos y el resto del mundo, lo que, combinado con otros esfuerzos, es de esperar que desencadena unos dividendos sociales y económicos muy necesarios. Asimismo, posibilitan la investigación científica, incluida la necesaria para comprender los cambios medioambientales que afectan a nuestro planeta. Sin embargo, la red mundial de cables submarinos de telecomunicaciones y los datos que transmiten se encuentran en peligro.

Este informe apunta a la necesidad inaplazable de acelerar los esfuerzos para reforzar la resiliencia de esta infraestructura vital y sus capas física, de red y de datos. Refleja asimismo la naturaleza de las actividades respaldadas por Estados que pueden afectar a los cables en el lecho marino, en tierra o a través del ciberespacio, y el impulso de muchas decisiones políticas que configuran las decisiones de inversión y enrutamiento de los cables submarinos. Reconoce que los Estados individuales y determinadas regiones o subregiones albergan una inquietud legítima con respecto a la seguridad de los sistemas de cables submarinos de telecomunicaciones, especialmente en el marco actual de tensiones geopolíticas exacerbadas y competencia tecnológica. No obstante, cuestiona la dirección de las respuestas actuales, argumentando que, para evitar los errores del pasado, también se requiere un enfoque cooperativo asentado en el fortalecimiento de la resiliencia de los sistemas a nivel mundial. Sus recomendaciones se dirigen principalmente a los Estados, aunque reconoce la importancia del sector privado, el mundo académico y la comunidad técnica para tales esfuerzos. Se inspira en las recomendaciones y compromisos existentes, incluidos los del Comité Internacional para la Protección de los Cables Submarinos y los Estados miembros de las Naciones Unidas que trabajan bajo los auspicios de la Primera Comisión de la Asamblea General sobre Desarme y Seguridad Internacional sobre las TIC y la seguridad internacional. Las recomendaciones se organizan atendiendo a tres áreas temáticas: 1) los cables submarinos de telecomunicaciones como infraestructuras críticas; 2) una cooperación público-privada mejorada; y 3) una agenda política más amplia y basada en principios. Se espera que sirvan de base para avanzar en los debates en curso sobre el comportamiento responsable de los Estados en este ámbito.

Introducción

Hace poco más de una década, cuando el tercer Grupo de Expertos Gubernamentales (GEG) sobre tecnologías de la información y las comunicaciones (TIC) y seguridad internacional concluía sus trabajos, se publicaron varios informes académicos sobre los cables submarinos de telecomunicaciones¹. Estos informes arrojan luz sobre los riesgos emergentes para los sistemas de cables submarinos y también ponen de relieve muchas de las lagunas del régimen jurídico internacional en materia de cables submarinos, así como los retos de gobernanza en general. Por aquel entonces, solo estaban operativos unos doscientos cables submarinos, en su mayoría propiedad de y explotados por empresas de telecomunicaciones. Hoy en día, el número de cables en funcionamiento se ha duplicado y los avances tecnológicos en el campo de la fotónica garantizan velocidades y capacidades antes inimaginables. La naturaleza de la industria ha cambiado drásticamente y plantea nuevos riesgos para los sistemas de cables. Y todo ello mientras sigue aumentando nuestra dependencia de los cables y del ecosistema de TIC en general. Aunque las amenazas relacionadas con los cables submarinos de telecomunicaciones rara vez han recibido mucha atención en los círculos de la ciberpolítica, esta tendencia está cambiando.

En marzo de 2022, en el marco del actual Grupo de trabajo de composición abierta (GTCA) sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso 2021-2025, un representante de un Estado pequeño, pero con una ubicación geoestratégica hizo referencia a los cables submarinos en sus observaciones. Su propósito era llamar la atención sobre los recursos y capacidades necesarios para proteger los cables submarinos que atraviesan las aguas del Estado, así como sobre los retos a los que se enfrenta para garantizar la fiabilidad y disponibilidad de estas conexiones de comunicación de importancia crítica para toda una serie de países del Cuerno de África, el sur de Asia y Europa, especialmente habida cuenta de las crecientes tensiones geopolíticas. Durante la misma reunión, otro representante advirtió de que, a pesar de las normas reconocidas internacionalmente en materia de comportamiento con respecto a las TIC, algunos Estados utilizaban como blanco infraestructuras críticas como los cables submarinos de telecomunicaciones, lo que podría tener efectos disruptivos de importancia².

Estas breves, pero importantes, referencias a los cables submarinos de telecomunicaciones, su vulnerabilidad a los ataques y las cuestiones relacionadas con la resiliencia y la capacidad durante una sesión del GTCA constituyen un pequeño indicio de la creciente preocupación que suscitan en los Estados las amenazas que surgen en torno a estas infraestructuras de información tan crítica³. Sin embargo, en gran medida se les hizo caso omiso. Varios meses más tarde, las explosiones del Nord Stream hicieron que los Estados volviesen los ojos hacia el fondo marino y los sistemas de cables que alberga y nuestra enorme dependencia colectiva de estos cables. La situación revelaba la necesidad de un mayor intercambio de información entre los agentes

¹ Véanse, por ejemplo, Douglas R. Burnett, *et al.* (eds) (2013), *Submarine Cables: The Handbook of Law and Policy*, BRILL; Michael Sechrist (2012), "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems", Harvard Kennedy School; y Michael Sechrist (2010), "Cyberspace in Deep Water: Protecting Undersea Communications Cables by Creating an International Public-Private Partnership", Harvard Kennedy School.

² Véanse las observaciones de los representantes de Djibouti y los Estados Unidos en la segunda sesión sustantiva del Grupo de trabajo de composición abierta, [https://meetings.unoda.org/meeting/57871/statements?ff0\]=segment_statements :Second substantive session&ff1\]=segment_statements :Third substantive session](https://meetings.unoda.org/meeting/57871/statements?ff0]=segment_statements%3ASecond_substantive_session&ff1]=segment_statements%3AThird_substantive_session).

³ El Gobierno de Singapur ya había planteado esta cuestión en el contexto de las Naciones Unidas y sus trabajos sobre las TIC y la seguridad internacional, pero, por diversas razones, no adquirió mucha fuerza en este foro concreto.

industriales y gubernamentales pertinentes, y, tal vez, nuevas medidas para reforzar su resiliencia⁴.

Sin embargo, no está claro si la diplomacia está preparada para entablar una conversación de esta índole. A pesar de la larga y tortuosa historia de los cables submarinos, se ha criticado a las comunidades políticas y de investigación por no comprender bien cómo funciona la red mundial de cables, cómo se regula, quién la controla y cómo se protege de las vulnerabilidades⁵. En clave política, es probable que exista mucha ambigüedad estratégica respecto a lo que quieren revelar o pueden debatir públicamente algunos responsables políticos o las empresas con intereses privados que poseen y explotan la mayoría de los sistemas de cables submarinos de telecomunicaciones. Pero esa falta de concienciación y comprensión en muchos círculos políticos sigue siendo considerable. Desde el punto de vista de la investigación, la bibliografía sobre cables submarinos ha aumentado sustancialmente e incluye diversos enfoques: ciencia y tecnología, ingeniería, seguridad marítima, derecho internacional público, protección del medio ambiente, estudios sobre gobernanza y seguridad o historia y arqueología, por citar algunos⁶. También están surgiendo investigaciones interdisciplinarias muy necesarias⁷. No obstante, los últimos acontecimientos sugieren que ha llegado el momento de abordar un debate más en profundidad sobre los cables submarinos de telecomunicaciones y sobre la idoneidad del actual régimen de gobernanza en esta materia y posibles medidas para reforzarlo. Este diálogo ya se ha iniciado a escala regional y nacional⁸. Este informe es un intento de sentar las bases de una conversación más global e integradora firmemente anclada en los debates multilaterales en curso.

Este informe aborda los cables submarinos de telecomunicaciones desde una perspectiva sistémica, como elementos centrales del ecosistema más amplio de las TIC. Comienza con una visión general de la evolución de la tecnología de cables submarinos y de las infraestructuras conexas de plantas "húmedas" (submarinas) y "secas" (terrestres), así como de los principales agentes implicados en la industria de los cables submarinos⁹. A continuación, ofrece una visión general de las amenazas y vulnerabilidades más comúnmente citadas en relación con los sistemas de cables submarinos y las infraestructuras conexas, seguida de una introducción al régimen de gobernanza existente en esta materia. Inspirándose en parte en las Buenas prácticas gubernamentales del Comité Internacional para la Protección de los Cables¹⁰ y en las

⁴ Véase, por ejemplo, la sección "Future Secure Connectivity Projects" de la Declaración conjunta UE-EE.UU. del Consejo de Comercio y Tecnología de 5 de diciembre de 2022.

⁵ Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", *Contemporary Security Policy* 42:3, p. 392.

⁶ *Ibid.*

⁷ Véase, por ejemplo, Christian Bueger y Tobias Liebetrau (2022), *Security Threats to Undersea Communications Cables and Infrastructure-Consequences for the EU*,

[https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA\(2022\)702557_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf).

⁸ *Ibid.*

⁹ La "planta húmeda" es el segmento del cable que va de una cámara de playa en una masa de tierra a otra. Incluye el cable de fibra óptica, los repetidores, los ecualizadores y las unidades de derivación. La "planta seca" es tradicionalmente el segmento terrestre de un sistema de cable submarino, que va desde la cámara de playa hasta la estación de aterrizaje de cables, situada normalmente a unos cientos de metros de la cámara de playa y conectada mediante un enlace corto de fibra sin repetidor, aunque esta configuración va cambiando con la evolución de las arquitecturas de los sistemas de cables.

¹⁰ En 2022, tras importantes consultas, el Comité Internacional para la Protección de los Cables publicó sus "Buenas prácticas gubernamentales para proteger y promover la resiliencia de los cables submarinos de telecomunicaciones" con el fin de ayudar a los gobiernos a elaborar leyes, políticas y prácticas para fomentar el desarrollo y la protección de los cables submarinos de telecomunicaciones, la infraestructura de Internet; véase <https://www.iscpc.org/publications/icpc-best-practices/>.

recomendaciones existentes negociadas en la Primera Comisión de la Asamblea General¹¹, concluye con algunas recomendaciones preliminares sobre las medidas de cooperación que los gobiernos pueden adoptar para promover un comportamiento responsable de los Estados y reforzar la resiliencia de los sistemas de cables submarinos y las infraestructuras conexas. Estas recomendaciones se organizan en torno a tres áreas temáticas: los cables submarinos de telecomunicaciones como infraestructuras críticas; la colaboración público-privada, y una agenda política más amplia y basada en principios.

¹¹ Desde 1998, los Estados miembros de las Naciones Unidas que trabajan bajo los auspicios de la Primera Comisión de la Asamblea General sobre Desarme y Seguridad Internacional han participado en debates sobre las TIC y la seguridad internacional. A lo largo del tiempo, una serie de Grupos de Expertos Gubernamentales (GEG) y un Grupo de trabajo de composición abierta (GTCA) han recomendado una serie de medidas pertinentes sobre comportamiento responsable de los Estados en su uso de las TIC. Entre ellas figuran tres normas centradas específicamente en las infraestructuras críticas. En 2021, el sexto GEG y el primer GTCA, en los que participaron los 193 Estados miembros, avanzaron en el debate sobre estas normas, señalando que las infraestructuras críticas a las que se refieren las recomendaciones pertinentes pueden incluir aquellas esenciales para la integridad general o la disponibilidad de Internet. Este informe parte de la premisa de que estas últimas incluyen los cables submarinos de telecomunicaciones y las infraestructuras, componentes y sistemas terrestres conexos que facilitan la transmisión de datos.

¿Qué contiene un cable de comunicaciones submarino moderno?

Los primeros cables submarinos se tendieron en el siglo XIX, primero entre Gran Bretaña y Francia, y después atravesando el Atlántico entre la isla de Valentia (Irlanda) y Heart's Content (Terranova)¹². En estos sistemas, las señales eléctricas se transmitían a través de un cable tendido entre dos estaciones telegráficas. Se utilizaba el código Morse para asignar un conjunto de puntos y rayas a cada letra del alfabeto inglés, lo que permitía la transmisión sencilla de mensajes complejos. La velocidad a la que podían enviarse los mensajes era revolucionaria, y la nueva tecnología se consideró "mucho más útil para la humanidad de lo que jamás ganó un conquistador en el campo de batalla", y capaz de servir como "vínculo de paz y amistad perpetuas entre las naciones"¹³.

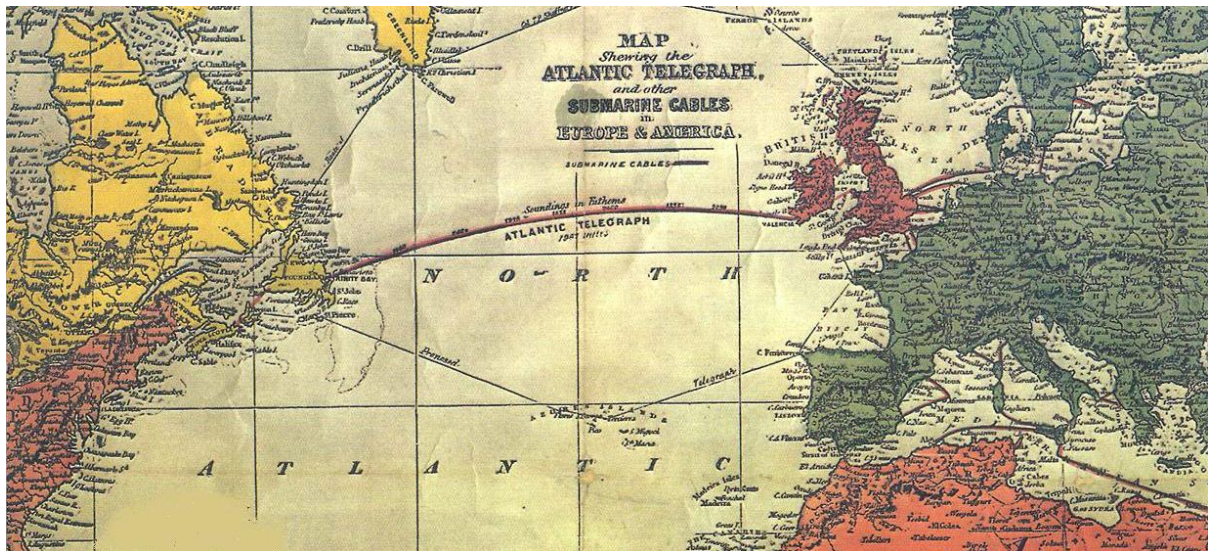


Figura 1. Mapa del cable telegráfico transatlántico de 1858

A pesar de su expansión por los océanos de todo el planeta durante esas primeras décadas, los cables telegráficos dejaron de utilizarse a principios del siglo XX y fueron sustituidos por otras tecnologías emergentes como el teléfono y, más tarde, el fax. Otros avances en la tecnología de las comunicaciones condujeron al tendido del primer sistema de cable telefónico transatlántico en la década de los 50 del siglo pasado, seguido tres décadas más tarde por el primer sistema de cable de fibra óptica transatlántico. Desde entonces han pasado 35 años y, en la actualidad, hay unos 530 sistemas de cables activos o en construcción¹⁴. Los cables submarinos de fibra óptica son ahora el eje vertebrador de nuestra infraestructura de comunicaciones: más del 95 %

¹² Para conmemorar este importante momento de la historia de las comunicaciones mundiales, Irlanda y Canadá solicitan conjuntamente que las estaciones telegráficas transatlánticas de Valentia y Heart's Content sean declaradas Patrimonio de la Humanidad por la UNESCO; véase <https://www.irishtimes.com/ireland/2022/07/22/valentia-islands-transatlantic-cable-to-be-put-forward-for-unesco-world-heritage-status/>.

¹³ Palabras del Presidente estadounidense James Buchanan en su mensaje de felicitación a la Reina Victoria, los primeros intercambiados a través del telégrafo transatlántico en 1858. El primer mensaje transatlántico tardó 17 horas en enviarse, a 2 minutos y 5 segundos por letra.

¹⁴ TeleGeography, <https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions>.

del tráfico mundial de Internet, voz y datos pasa por esta vasta red sumergida. Literalmente, todas nuestras comunicaciones privadas, empresariales y militares dependen de ella, al igual que las transacciones financieras mundiales y muchos sistemas de defensa. El valor estratégico de las infraestructuras sigue aumentando a la par que nuestra dependencia digital, la llegada del 5G y las necesidades de los centros económicos de conectividad de alta calidad y baja latencia, unidas al valor comercial y estratégico inherente al acceso a nuevos mercados y a los datos que albergan o a los que se puede acceder en ellos¹⁵.

Los cables submarinos actuales utilizan tecnología de fibra óptica para transmitir datos. Algunos sistemas de cable individuales pueden alcanzar los 45.000 kilómetros de longitud¹⁶. En conjunto, representan aproximadamente 1,3 millones de kilómetros de cable en servicio tendidos por todo el mundo. Los cables están formados por varios pares de fibras ópticas, del diámetro aproximado de un cabello humano, que se cubren con gel de silicona y se enfundan en varias capas de plástico, cables de acero y cobre. A veces se aplican capas adicionales de alambre de acero al exterior del cable para blindarlo contra daños externos. El grosor de la armadura de acero suele venir determinado por la profundidad del mar y la proximidad de la actividad marina comercial. En aguas poco profundas (por lo general, menos de 1.000 metros), el cable también puede enterrarse bajo el lecho marino para protegerlo, por ejemplo, de las anclas de los barcos y las operaciones pesqueras.

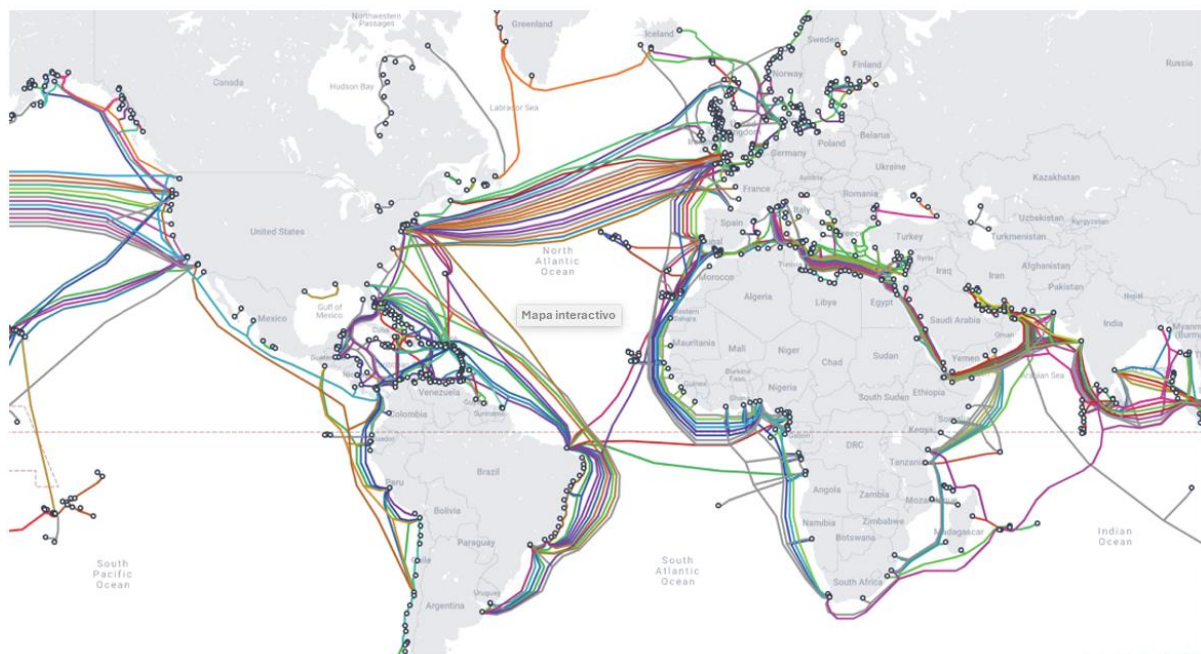


Figura 2. Mapa de cables submarinos de 2022¹⁷

¹⁵ Hilary McGeachy (2022), "The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns", *Australian Journal of International Affairs* 76:2.

¹⁶ DataCenterDynamics (2022), 'World's Longest Subsea Cable Lands in Djibouti, East Africa', <https://www.datacenterdynamics.com/en/news/worlds-longest-subsea-cable-lands-in-djibouti-east-africa/>; Reuters (2022), "MTN Lands Subsea Cable in South Africa to Boost Africa's Connectivity", <https://www.reuters.com/world/africa/mtn-lands-subsea-cable-south-africa-boost-africas-connectivity-2022-12-13/>.

¹⁷ TeleGeography's 2022 Submarine Cable Map depicting 486 cable systems and 1,306 landings currently active of under construction; see <https://submarine-cable-map-2022.telegeography.com/>.

Hasta hace poco más de una década, la modulación de intensidad y detección directa era la tecnología de transmisión óptica más utilizada en los cables submarinos. Este método transmite información a través de fibras ópticas submarinas y terrestres utilizando impulsos láser para codificar datos digitales. Desde entonces, los avances en la transmisión óptica coherente han permitido multiplicar por más de cien la velocidad de transmisión de datos a través de un solo canal¹⁸. Además, la multiplexación por división de longitud de onda ha aumentado el número de canales transportados por fibra¹⁹. La capacidad de los cables varía según el sistema, pero avances como la multiplexación por división espacial permitirán a los nuevos sistemas transportar hasta 500 terabytes por segundo²⁰. En los sistemas de más de varios cientos de kilómetros, los amplificadores ópticos (alojados en contenedores estancos conocidos como repetidores) amplifican las señales a lo largo del cable aproximadamente cada 100 km.

Las construcciones de cable tradicionales llegan a tierra en una de las 1.306 estaciones de aterrizaje de cables actualmente en funcionamiento en todo el mundo, desde donde los datos se enrutan y conectan a los sistemas terrestres²¹. En un sistema tradicional de estación a estación, las estaciones albergan la infraestructura de 'planta seca', que incluye el equipo terminal de la línea submarina que controla sus operaciones y el equipo de alimentación del cable. Esta arquitectura tradicional ha cambiado en los últimos años, impulsando una mayor convergencia entre las redes de fibra submarinas y terrestres y los centros de datos. Por ejemplo, en un sistema que conecte centros de datos, el equipo de alimentación puede alojarse en una estación de aterrizaje modular más pequeña cerca de la costa, y el equipo terminal tierra adentro en un centro de datos "o en un centro de colocación e interconexión con alta conectividad perteneciente a un operador neutral"²². Estos sistemas, denominados 'de cable abierto', separan el equipo terminal de la 'planta húmeda' y permiten actualizar el sistema y diversificar los equipos, incluso en sistemas heredados. El tipo de sistema dependerá en última instancia de los intereses de los usuarios finales en lo que respecta a la capacidad que adquieren (acceso a los principales mercados, puntos finales, redes IP de primer nivel, puntos de intercambio de Internet, opciones de redundancia, conexión a servicios de agregación en la nube, etc.), aunque la decisión final dependerá de una serie de factores, como si se trata de una construcción conjunta (es decir, encargada por dos o más compradores), así como de la apertura del mercado, el coste, la distancia, las condiciones geográficas, el entorno normativo y la regulación nacional de la inversión extranjera, etc.²³ Es probable que sigan surgiendo nuevos ecosistemas en un futuro próximo.

Ejecutar un proyecto de cableado nuevo puede llevar entre 2,5 y 5 años, desde la planificación inicial hasta la puesta en marcha del sistema. Como cualquier proyecto de infraestructura,

¹⁸ Véase Ciena, "What Are Coherent Optics", <https://www.ciena.com/insights/what-is/What-Is-Coherent-Optics.html>; y Google (2022), "Google's Subsea Fiber Optics, Explained", <https://cloud.google.com/blog/topics/developers-practitioners/google-subsea-fiber-optics-explained>.

¹⁹ Ibid.

²⁰ Se puede conseguir una mayor capacidad mediante la multiplexación por división espacial, en la que más pares de fibras transportan canales con menor potencia y relación señal/ruido; véase <https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions>.

²¹ Ibid.

²² Vinay Nagpal (2019), "Convergence of Data Centers, Subsea and Terrestrial Fiber", Pacific Telecommunications Council.

²³ Ibid.

implica una serie de pasos y largas negociaciones²⁴. Una vez alcanzado un acuerdo, comienza la construcción. Esto implica instalar la infraestructura de la ‘planta húmeda’ (sumergida) y la ‘planta seca’ (terrestre), así como la infraestructura de gestión y supervisión de la red necesaria para que el sistema de cable submarino funcione de forma fiable²⁵. El ciclo de vida de diseño de un sistema de cable es de unos 25 años, aunque muchos pueden seguir utilizándose más tiempo si los ingresos siguen superando los costes²⁶. Actualmente, un número considerable de cables está llegando al final de su vida útil.

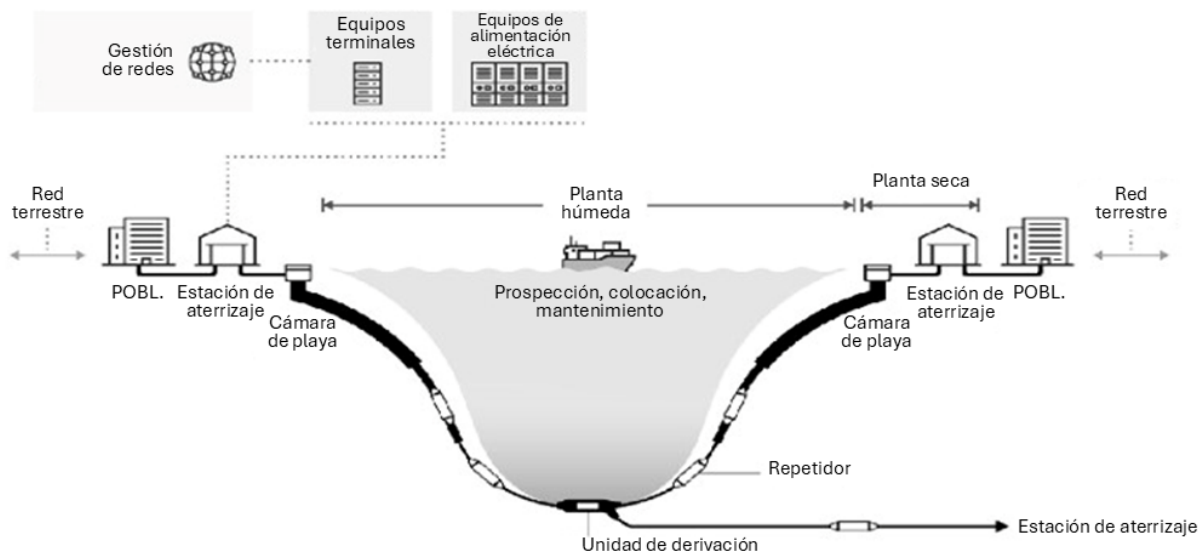


Figura 3. Sistemas de cables submarinos - Infraestructura y componentes de la planta húmeda y seca²⁷

En principio, la gestión y mitigación de riesgos se integra en el diseño del sistema de cable y el proceso de gestión de la red para contrarrestar posibles riesgos de inactividad del sistema y los costes de reparación resultantes, así como para garantizar el máximo grado de resiliencia²⁸. Por un lado, la arquitectura de los sistemas de cable garantiza un nivel intencionado de capacidad redundante. De este modo se evita, por lo general, que los daños en un cable tengan efectos de segundo o tercer orden en los servicios o las infraestructuras. Se espera que la resiliencia siga aumentando a medida que se añade nueva capacidad a los sistemas actuales. En el pasado, se

²⁴ Por ejemplo, solo el contrato de suministro suele constar de seis partes principales: las condiciones del contrato, las especificaciones técnicas del proyecto, un calendario de precios, un plan de trabajo, un calendario de facturación y la descripción del sistema del proveedor. Estos acuerdos contractuales se negocian normalmente con diversos agentes, ya que los proyectos de cable se suelen ejecutar a través de consorcios o como construcciones conjuntas.

²⁵ Véase la nota a pie de página 9.

²⁶ Para compensar el efecto negativo en los beneficios de unos precios de capacidad más bajos, es preciso aumentar constantemente la capacidad de los cables; véase Alan Maudlin (2018), "The Next Mass Extinction: Ageing Submarine Cables", <https://www2.telegeography.com/submarine-networks-world-2018>.

²⁷ Jill C. Gallagher (2022), "Undersea Telecommunication Cables: Technology Overview and Issues for Congress", US Congressional Research Service, p. 5, <https://crsreports.congress.gov/product/pdf/R/R47237>.

²⁸ Según Subcom, la reparación de un cable submarino puede costar más de un millón de dólares y normalmente tarda dos o más semanas en volver a estar operativo, dependiendo de los requisitos de permisos y las condiciones climáticas, entre otros factores. En cuanto a las amenazas a la ciberseguridad, los proveedores de conectividad deben ser capaces de proteger el tráfico que proporcionan integrando funciones de seguridad. Pueden incluir un cortafuegos de nueva generación (NGFW), acceso remoto seguro y servicios de gestión unificada de amenazas (UTM). Además, la conectividad que ofrece cifrado de extremo a extremo, seguridad de red y filtrado a nivel de aplicación mejora la calidad de servicio y contribuye a prevenir las amenazas a la ciberseguridad; véase Brendan Press (2021), "The Role of Subsea Cables in a World Going Local", <https://datacentremagazine.com/automation/role-subsea-cables-world-going-local>.

prestaba más atención a los riesgos asociados a la infraestructura y los componentes físicos de los sistemas de cables, asociados fundamentalmente a fallos y daños causados por la actividad marítima comercial. Hoy en día, ese enfoque se ha ampliado y también se contemplan los riesgos que puedan surgir en las capas de datos y de red de los sistemas. Entre estos últimos figuran los riesgos que afectan a la fibra y a la ciberseguridad y que pueden surgir durante el proceso de fabricación o en puntos vulnerables como componentes de *hardware* sumergidos, las cámaras de playa, las estaciones de aterrizaje de cables, los 'puntos de presencia' o instalaciones de interconexión, los puntos de intercambio de Internet y los centros de datos, así como en los sistemas de gestión de redes de cables, que funcionan mediante un *software* y suelen manejarse a distancia²⁹. Los enfoques de gestión de riesgos relacionados incluyen el refuerzo de la seguridad física de las edificaciones pertinentes, entre otras medidas mediante el refuerzo de la seguridad periférica, innovaciones en la construcción de estaciones modulares de aterrizaje de cables y arquitecturas de geomalla de ciberseguridad, un cifrado de datos robusto y otros controles y tecnologías de seguridad de confianza cero en todos los elementos troncales³⁰. Los avances en las arquitecturas de los sistemas de cable también pueden aportar mayor resiliencia, ya que, presuntamente, los nuevos sistemas compartidos limitan el acceso a los elementos físicos y virtuales de un cable en el equipo terminal³¹. Asimismo, existen normas y técnicas que pueden ayudar tanto a prevenir y detectar vulnerabilidades en el *hardware* óptico como posibles interferencias o ataques a las redes ópticas. Así, cada vez son más frecuentes las técnicas de detección como la interferometría óptica y la detección acústica distribuida (DAS) en los cables para vigilar segmentos de estos cercanos a la costa a fin de identificar actividad cercana o irregularidades y fallos en la transmisión³². Los avances más recientes en técnicas de detección en otras partes del sistema pueden resultar muy beneficiosos para la integridad de la red y la vigilancia ambiental³³.

Los cables submarinos de telecomunicaciones de fibra óptica son en su mayoría propiedad de empresas privadas que se encargan de su explotación. Tradicionalmente, los principales propietarios y operadores eran empresas de telecomunicaciones que utilizaban el modelo de consorcio para trabajar con las partes interesadas en utilizar los cables para, de este modo,

²⁹ Michael Sechrist (2012), "New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems", Harvard Kennedy School; see also Nadia Schadlow and Brayden Helwig (2020), "Protecting Undersea Cables Must be Made a National Security Priority", *Defense One*, <https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/>; and Olga Khazan (2013), "The Creepy, Long-Standing Practice of Undersea Cable Tapping", *The Atlantic*, <https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>.

³⁰ Los elementos troncales a los que se hace referencia son la identidad, los puntos finales, los datos, las aplicaciones, la infraestructura y las redes; véase Microsoft (2022), "Guiding Principles of Zero Trust", <https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview>.

³¹ Comunicación con un representante de la industria, diciembre de 2022.

³² A diferencia de las anteriores funciones de supervisión a distancia, que se realizaban a través de *hardware* instalado en cada extremo del cable, en los nuevos sistemas de cable la propia fibra es el sensor. Para más información sobre DAS, véase SAGE, "Distributed Acoustic Sensing (DAS) Research Coordination Network (RCN)", https://www.iris.edu/hq/initiatives/das_rcn.

³³ Las nuevas investigaciones también han demostrado "el primer transceptor coherente en tiempo real con detección de fase y polarización incorporadas en tiempo real mientras se transmite información simultáneamente". Los investigadores "afirman haber transmitido con éxito a lo largo de 12.800 km mientras realizaban una detección ambiental continua"; véase M. Mazur *et al.* (2022), "Transoceanic Phase and Polarization Fiber Sensing using Real-Time Coherent Transceiver", *Optical Fiber Communications Conference (OFC) 2022*, págs. 1 a 3, <https://opg.optica.org/abstract.cfm?uri=OFC-2022-M2F.2>. En cuanto a desarrollos relacionados en sistemas terrestres, véase Optica (2023), "Scientists Perform Real-Time Environmental Sensing over 524 Kilometers of Live Aerial Fiber", <https://phys.org/news/2023-01-scientists-real-time-environmental-kilometers-aerial.html>.

compensar los costes. En la década de auge y caída de los noventa, varias empresas privadas invirtieron en cables submarinos y obtuvieron beneficios vendiendo capacidad a empresas de telecomunicaciones y otros agentes privados³⁴. Hoy en día conviven ambos modelos de financiación, pero se han producido importantes cambios en lo que respecta a la extensión geográfica y el tipo de entidades privadas participantes. Por ejemplo, en la última década, las empresas chinas han ocupado un papel cada vez más destacado en las inversiones en proyectos de cables submarinos por todo el mundo, generalmente en el marco de consorcios y, a nivel regional, en el mantenimiento y la reparación de cables³⁵. Estas inversiones van acompañadas de inversiones domésticas en investigación, desarrollo y fabricación de tecnologías de transmisión óptica de alta velocidad y capacidad y tecnologías conexas de cables submarinos y redes³⁶. El sector también ha sido testigo de la llegada de grandes proveedores de servicios de *streaming* e hiperescaladores como Meta, Alphabet, Microsoft y Amazon. En su afán por conectar nuevos centros de datos a gran escala y redes en la nube, estos colosos mundiales han añadido capacidad a una tasa anual compuesta de al menos el 70 % entre 2015 y 2019 en seis de las siete regiones del mundo³⁷, cambiando las estructuras tradicionales de inversión y propiedad del cable en muchas de estas mismas regiones y “superando a los proveedores de redes troncales de Internet para convertirse en los principales propietarios de capacidad de cable submarino”.³⁸ También ha aumentado el número de promotores independientes de infraestructuras de cable submarino que poseen y explotan sistemas de cable. Aprendiendo de las dificultades que plantean otras estructuras de propiedad, presuntamente, han creado una diferenciación inesperada en el mercado³⁹. Estos son los agentes más visibles del sector. Entre bastidores, una gran cantidad de empresas privadas especializadas y organismos técnicos prestan servicios que abarcan todo el ciclo de vida de los sistemas de cable.

Los ministerios y organismos gubernamentales también desempeñan un papel importante en la gobernanza y protección de los cables submarinos, y sus funciones reguladoras y políticas abarcan

³⁴ Se denominan años de “caída” debido a que muchas de estas empresas quebraron posteriormente cuando la industria de Internet implosionó y dejó de ser necesaria.

³⁵ Por ejemplo, la empresa china HMN Technologies (antes Huawei Marine) participó en 13 proyectos de cable diferentes entre 2012 y 2019, la mayoría de ellos fuera de su región de origen; Lane Burdette (2021), “Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy”, *Journal of Public and International Affairs*, <https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>. Véase también Hilary McGeachy (2022), “The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns”, *Australian Journal of International Affairs* 76:2; Jonathan E. Hillman (2021), “Securing the Subsea Network: A Primer for Policymakers”, Centro para Estudios Estratégicos e Internacionales (CSIS); y Christian Bueger y Tobias Liebetrau (2021), “Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network”, *Contemporary Security Policy* 42:3. La participación de empresas chinas en la construcción de cables ha disminuido desde entonces por diversas razones, en algunos casos, debido a la preocupación por la seguridad nacional de otros Estados. La empresa china de mantenimiento y reparación SBSS opera principalmente en Asia y presta servicios tanto en el sector de los cables de fibra óptica como en el de los cables eléctricos.

³⁶ Notice of the State Council on the Publication of *Made in China 2025* (2015) No. 28, PRC State Council, p. 19, ‘New Generation IT Industry’. Translation made available by Center for Security and Emerging Technology, 10 March 2022, <https://cset.georgetown.edu/publication/notice-of-the-state-council-on-the-publication-of-made-in-china-2025/>

³⁷ Matthew P. Goodman and Matthew Wayland (2022), “Securing Asia’s Subsea Network: U.S. Interests and Strategic Options”, *CSIS Briefs*, p. 3.

³⁸ *Ibid.* Véase también Alan Mauldin (2017), “A Complete List of Content Providers’ Submarine Cable Holdings”, <https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list>.

³⁹ Suvesh Chattopadhyaya (2018), “A New Coming for Submarine Cable Systems—the Independent Infrastructure Developers”, <https://www.submarinenetworks.com/en/insights/a-new-coming-for-submarine-cable-systems-the-independent-infrastructure-developers>; Olivier Pinaud (2023), “Big Tech Colonizes Seabed to Assert Control of the Internet”, *Le Monde*, https://www.lemonde.fr/en/international/article/2023/01/02/big-tech-colonizes-seabed-to-assert-control-of-the-internet_6010073_4.html.

todo el ciclo de vida de los sistemas de cable y sus infraestructuras submarina y terrestre. Tradicionalmente, tal labor ha correspondido a ministerios, departamentos y agencias competentes en materia de telecomunicaciones, asuntos marítimos y navieros, pesca, medio ambiente, aduanas, fuerzas de seguridad y defensa. Hoy en día, también se incluyen en esta lista ministerios y agencias responsables de la ciberseguridad y la protección de infraestructuras críticas, transformación digital, política exterior, innovación, comercio, inversión y desarrollo⁴⁰. Organizaciones regionales como el Foro de Cooperación Económica de Asia y el Pacífico (APEC), la Asociación de Naciones de Asia Sudoriental (ASEAN) y varios organismos de la Unión Europea elaboran políticas, investigaciones y orientaciones relacionadas con los cables submarinos de telecomunicaciones⁴¹. También intervienen organismos internacionales especializados, como la Unión Internacional de Telecomunicaciones (en lo referente a normas técnicas), la Organización Hidrográfica Internacional (en cuestiones de cartografía y separación espacial), la Oficina de las Naciones Unidas contra la Droga y el Delito (en cuestiones de asistencia técnica y capacitación relacionadas con la seguridad marítima, incluida la protección de los cables submarinos), y la Conferencia Intergubernamental sobre Biodiversidad Marina de Áreas fuera de la Jurisdicción Nacional (en lo relativo a la resolución 72/249 sobre el uso sostenible de la diversidad biológica marina de las zonas situadas fuera de la jurisdicción nacional), que acaba de aprobar un nuevo instrumento internacional jurídicamente vinculante⁴². También desempeñan un papel importante varias organizaciones no gubernamentales, organismos técnicos e institutos de investigación⁴³.

⁴⁰ ICPC (2022), "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables", <https://www.iscpc.org/documents/?id=3733>.

⁴¹ Véanse, por ejemplo, las publicaciones de la APEC, incluidas las derivadas de su Plan de Acción del Marco de Conectividad de la Cadena de Suministro; el Plan Maestro Digital 2025 de la ASEAN, y sus directrices de 2019 para reforzar la resistencia y la reparación de los cables submarinos ("Guidelines for Strengthening Resilience and Repair of Submarine Cables"); la Directiva (UE) 2022/2555 de 14 de diciembre de 2022, <https://eur-lex.europa.eu/eli/dir/2022/2555>; véase también Christian Bueger y Tobias Liebetrau (2022), "Security Threats to Undersea Communications Cables and Infrastructure—Consequences for the EU", [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA\(2022\)702557_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf).

⁴² Declaración del Secretario General de las Naciones Unidas en la Conferencia Intergubernamental del instrumento internacional jurídicamente vinculante en el marco de la Convención de las Naciones Unidas sobre el Derecho del Mar (CNUDM) relativa a la conservación y el uso sostenible de la diversidad biológica marina de las zonas situadas fuera de la jurisdicción nacional, 5 de marzo de 2023, <https://www.un.org/ebnj/sites/www.un.org.ebnj/files/sgstatementbbnj5resumed.pdf>. Véase también <https://www.un.org/ebnj/>.

⁴³ La lista es larga, pero algunas organizaciones clave son Safe Seas, para cuestiones marítimas, y el Instituto de Ingenieros Eléctricos y Electrónicos y la Internet Society, en lo relacionado con tecnologías, redes y ciberseguridad.

Amenazas y vulnerabilidades

En comparación con los cables de cobre del siglo XIX, los cables de fibra óptica utilizados actualmente ofrecen una alta fiabilidad y se han diseñado según la 'norma de los 5 nueves': están disponibles el 99,999 % del tiempo y "sufren pocas interrupciones importantes en proporción con su gran dispersión por todo el mundo"⁴⁴. No obstante, se producen fallos; se estima que unos 200 al año⁴⁵. Como se explica más adelante, las averías e interrupciones pueden tener importantes consecuencias, sobre todo cuando no es posible el reenrutamiento automático a la capacidad no utilizada y disponible en otros cables submarinos y redes terrestres o por satélite.

Las amenazas a los sistemas de telecomunicaciones por cable submarino afectan a varios dominios y abarcan los ámbitos marítimo, terrestre y ciberespacial. Pueden deberse a fenómenos naturales o a la actividad humana (involuntaria o intencionada), y afectar a los propios cables y a la transmisión de datos o a otras partes de la infraestructura, como los amplificadores, las estaciones de aterrizaje, los buques de mantenimiento y reparación, los sistemas de gestión de redes y las cadenas de suministro de cables⁴⁶. Asimismo, los cables suelen presentar una elevada concentración geográfica en el mar y en tierra —los denominados 'puntos de estrangulamiento'—, lo que dificulta su tendido y reparación en circunstancias normales y facilita su bloqueo en situaciones de tensión o crisis⁴⁷.

Los propios cables son vulnerables a los fenómenos naturales relacionados con la meteorología (marejadas, tifones, huracanes), la geología (terremotos, fallas geológicas, deslizamientos de tierra submarinos, erupciones volcánicas) y el medio marino (densidad de corriente, oleaje). Las perturbaciones causadas por fenómenos naturales suelen producirse cerca de tierra y afectan a varios cables al mismo tiempo, haciendo que se pierda redundancia. Estos sucesos son aún más problemáticos cuando un país se abastece de un solo cable. Por ejemplo, la erupción volcánica submarina que se produjo cerca de Tonga y el consiguiente tsunami del 15 de enero de 2022 cortaron el único cable submarino que conectaba Tonga con el resto del mundo a través de Fiji. Aunque fue posible garantizar la conectividad de bajo nivel mediante conexiones vía satélite una semana después del suceso, se tardó más de cinco semanas en reparar el cable y restablecer la conectividad total con la isla principal de Tongatapu, y varios meses en reparar el cable nacional que conecta la isla principal con las islas periféricas más afectadas por el tsunami⁴⁸.

⁴⁴ Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", *Contemporary Security Policy* 42:3, p. 396.

⁴⁵ Según los debates del pleno del Comité Internacional de Protección de los Cables (ICPC) de 2019, la tasa de averías por cada 1.000 km se mantuvo estática o disminuyó ligeramente en la última década, a pesar del crecimiento de la longitud total de los cables en servicio.

⁴⁶ Por ejemplo, según *Quintillion*, la creciente demanda y fenómenos como la COVID-19 han provocado escasez de cables de fibra e infraestructuras de red de distribución óptica (ODN) y de componentes electrónicos como memorias flash, condensadores y semiconductores. *Quintillion*, "Connecting the World to Fiber: The Subsea Cable Industry's 5 Biggest Challenges", 26 de noviembre de 2021, <https://www.quintillionglobal.com/connecting-the-world-to-fiber-the-subsea-cable-industrys-5-biggest-challenges/>

⁴⁷ Véase, por ejemplo, Matt Burgess (2022), "The Most Vulnerable Place on the Internet", <https://www.wired.com/story/submarine-internet-cables-egypt/>, donde se analiza la vulnerabilidad de la ruta del Mar Rojo como uno de los mayores puntos de estrangulamiento de Internet del mundo.

⁴⁸ Simon Scarr et al. (2022), "The Race to Reconnect Tonga", *Reuters*, <https://www.reuters.com/graphics/TONGA-VOLCANO/znpnejbovl/>.

Las averías o interrupciones de los cables también pueden deberse a actividades marinas comerciales, como la pesca y el fondeo. Según las estadísticas del ICPC, la pesca y anclaje suelen ser las causas más comunes de alteraciones, y representan aproximadamente el 70 % de las averías de los cables⁴⁹. Otros tipos de actividad comercial que pueden causar alteraciones en los cables son el transporte marítimo, el dragado y la minería de aguas profundas, que se está intensificando en algunas regiones marítimas.

A veces, la dinámica del mercado también puede ser la causante de los fallos de los cables. Esto ocurre cuando los propietarios intentan reducir el coste de las infraestructuras de cable utilizando equipos y componentes de menor calidad en la construcción del sistema de cables⁵⁰. Los esfuerzos por aumentar la eficiencia también pueden ocasionar problemas. Por ejemplo, la transición a sistemas remotos de gestión de redes resultó llamativa debido a la vulnerabilidad a la explotación del *software* de los sistemas, aunque estos sistemas remotos se han reforzado considerablemente en consonancia con la mayor atención prestada a los riesgos de ciberseguridad en la última década⁵¹. También suscita cierta preocupación que el ecosistema digital, cada vez más complejo y con dependencias estratificadas y escalonadas a nivel mundial, desencadene una serie de fallos escalonados que actualmente no están contemplados en los marcos actuales de gestión y mitigación de riesgos⁵².

Más allá de las averías de los cables en sí, los problemas de la cadena de suministro, como la dependencia de componentes básicos o su escasez, pueden plantear riesgos importantes, especialmente cuando se necesita llevar a cabo reparaciones con urgencia⁵³. También puede resultar problemática la inversión insuficiente en capacidades de buques de mantenimiento y reparación y para dar solución a la escasez de mano de obra cualificada; dos de las principales preocupaciones del sector en la actualidad⁵⁴.

Aunque se hace escasa referencia a ello, las deficiencias de la política gubernamental y los marcos normativos “también pueden agravar los riesgos de daños y reducir la resiliencia” de los sistemas de cables, además de retrasar las actividades de reparación⁵⁵, como también es el caso con la falta de claridad con respecto a las funciones y responsabilidades de las autoridades nacionales. Para muchos integrantes del sector, las decisiones sobre el trazado de los cables y las inversiones orientadas a la seguridad nacional también pueden repercutir negativamente en la competitividad de los agentes del sector y obstaculizar la innovación. También pueden generar nuevos riesgos para la seguridad.

⁴⁹ ICPC (2022), “Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables” Section 2, “Fishing and anchoring risks”, <https://www.iscpc.org/publications/icpc-best-practices/>

⁵⁰ Comunicación con un representante de la industria del cable, 2 de diciembre de 2022.

⁵¹ Michael Sechrist (2012), “New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems”, Harvard Kennedy School.

⁵² Comunicación con el director de un centro nacional de ciberseguridad, 24 de enero de 2022.

⁵³ Sobre los problemas de la cadena de suministro, en particular el suministro de componentes (incluidos los semiconductores), véanse Jim Fagan, “Managing tight supply chains in global subsea connectivity”, *Mission Critical*, 25 de octubre de 2022, <https://www.missioncriticalmagazine.com/articles/94311-managing-tight-supply-chains-in-global-subsea-connectivity>; Sebastian Moss, “Global shortage of fibre optic cables leads to delays, price increases”, *DataCenterDynamics*, 25 de julio de 2022, <https://www.datacenterdynamics.com/en/news/global-shortage-of-fiber-optic-cables-leads-to-delays-price-increases/>. Véase también la nota 47.

⁵⁴ Comunicación con expertos del sector, noviembre de 2022. Véase también la nota 47.

⁵⁵ ICPC (2022), “Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables”, <https://www.iscpc.org/documents/?id=3733>; Andy Palmer-Felgate et al. (2013), “Marine Maintenance in the Zones—A Global Comparison of Repair Commencement Times”, <https://minz.org.nz/i/2018-challenges/Marine-maintenance-in-the-zones.pdf>.

Hasta hace poco, la forma más común de daño intencionado a los cables era el robo de los materiales que los componen, en particular, el cobre⁵⁶. Podría decirse que las redes terrestres se enfrentan a problemas similares, ya que son frecuentes los robos de tramos de cable bajo la asunción errónea de que contienen cobre, aunque esta es la única similitud, ya que reparar los daños en los cables submarinos es mucho más costoso y requiere más tiempo. También ha suscitado preocupación la posibilidad de que grupos terroristas alteren las infraestructuras críticas, incluidas las de comunicaciones, como los cables submarinos. Tal inquietud llegó incluso a plasmarse en una resolución del Consejo de Seguridad, pero nunca se ha producido tal acontecimiento, al menos que se sepa públicamente⁵⁷.

Sin embargo, recientemente han adquirido más notoriedad las amenazas, existentes y potenciales, que plantean los Estados a los cables de comunicación submarinos. Estas amenazas tienen una larga historia. Por ejemplo, antes de la negociación de la Convención para la Protección de los Cables de Telégrafos Submarinos de 1884, la intervención de los Estados en los proyectos de cables aumentó considerablemente, a la par que el expansionismo territorial propio de la época. La competencia por el acceso a los recursos críticos para el funcionamiento de los cables se intensificó. La interceptación de transmisiones y el sabotaje de cables se convirtieron en prácticas habituales de los conflictos —primero disturbios civiles y después conflictos internacionales—, y las grandes potencias las incorporaron a sus tácticas de guerra⁵⁸. Los efectos cuando estalló una gran guerra fueron considerables, incluso entonces, cuando el mundo no dependía tanto de las tecnologías de la información. Hoy en día, aunque la mayoría de los proyectos de cable se asientan en una sólida gestión de riesgos y prevén altos niveles de redundancia para garantizar la disponibilidad o una recuperación relativamente rápida en caso de fallo, la situación no está exenta de dificultades. La velocidad de recuperación disminuye en los países más alejados y con puntos únicos de fallo. Es probable que la recuperación también se ralentice si se producen intentos de interrumpir puntos críticos de estrangulamiento, bloquear el acceso a buques de reparación y depósitos de piezas de repuesto o alterar las cadenas de suministro.

Muchos de los comportamientos por parte de Estados a los que se ha hecho referencia son evidentes hoy en día, lo que pone de manifiesto las fuertes y preocupantes corrientes geopolíticas de nuestro tiempo. En tierra, existe constancia de operaciones cibernéticas dirigidas contra

⁵⁶ Véase, por ejemplo, Robert Martinage (2015), "Under the Sea: The Vulnerability of the Commons", *Foreign Policy* 94:1 Mick P. Green y Douglas R. Burnett, "Security of International Submarine Cable Infrastructure: Time to Rethink?", Comité Internacional para la Protección de los Cables, pág. 5, <https://www.iscpc.org/documents/?id=2974>.

⁵⁷ Consejo de Seguridad, documento de la ONU S/RES/2341 (2017); véase también el mensaje de 2017 del Secretario General de las Naciones Unidas para el debate abierto del Consejo de Seguridad de las Naciones Unidas sobre la "protección de la infraestructura vital contra atentados terroristas", <https://www.un.org/sg/en/content/sg/statement/2017-02-13/secretary-generals-message-security-council-open-debate-protection>.

⁵⁸ Camino Kavanagh (próxima publicación), "The ties that bind... And the geopolitics that can unwind", Conferencia SubOptic Telecoms, marzo de 2023.

instalaciones terrestres de cable y puntos de intercambio de Internet⁵⁹; de competencia por el control o la destrucción de instalaciones terrestres de sistemas de cables en conflictos activos,⁶⁰ y de empresas y particulares que proporcionan apoyo material e información de inteligencia a agencias de espionaje⁶¹. En el mar, se ha informado de incidentes relacionados con actividades sospechosas en las aguas territoriales o la zona económica exclusiva de varios Estados⁶².

También existen informes de sabotaje intencionado de cables por parte de Estados (afortunadamente, aún son pocos los casos), y son motivo de preocupación los posibles efectos de dicha actividad en las operaciones militares⁶³. En general, se supone que cuanto más alejado de tierra se produzca el ataque, mayores son las probabilidades de que esté detrás una gran potencia, ya que se requieren importantes capacidades y recursos tecnológicos y marítimos para llegar a los cables y acceder a ellos. Este sería el caso de la interceptación de comunicaciones transmitidas por cables en alta mar, aunque los avances en las técnicas de detección óptica y encriptación de datos están, al parecer, dificultando la detección y prevención de tales actividades⁶⁴.

⁵⁹ Véanse, por ejemplo, *CyberScoop* (2022), "DHS Investigators Say They Foiled Cyberattack on Undersea Internet Cable in Hawaii", <https://www.cyberscoop.com/undersea-cable-operator-hacked-hawaii/>; Colin Wall y Pierre Morcos (2021), "Invisible and Vital: Undersea Cables and Transatlantic Security", CSIS, <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>; Devirupa Mitra (2022), "Snooping Storm Brews in Mauritius Over Indian Team Accessing Internet Landing Station", *The Wire*, <https://thewire.in/diplomacy/mauritius-snooping-storm-india-internet>; Reuters (2021), "U.S. Spied on Merkel and Other Europeans through Danish Cables-broadcaster DR", <https://www.euronews.com/2021/05/30/us-denmark-defence>; Olga Khazan (2013), "The Creepy, Long-Standing Practice of Undersea Cable Tapping", *The Atlantic*, <https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>; y Yuval Shavitt y Chris C. Demchak (2022), "Unlearned Lessons from the First Cybered Conflict Decade-BGP Hijacks Continue", *Cyber Defense Review* 7:1, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/20_Shavitt_Demchak_CDR_V7N1_WINTER_2022.pdf.

⁶⁰ Véase Celine Alkhalidi y Mostafa Salem (2022), "Airstrikes Kill 70 People and Knock out Internet in Yemen", *CNN*, <https://edition.cnn.com/2022/01/21/middleeast/yemen-detention-strike-internet-outage-intl/index.html>; *Recorded Future* (2018), "Underlying Dimensions of Yemen's Civil War: Control de Internet", <https://go.recordedfuture.com/hubfs/reports/cta-2018-1128.pdf>.

⁶¹ En 2018, el Departamento del Tesoro de los Estados Unidos sancionó a cinco empresas rusas y a tres ciudadanos rusos que presuntamente habían prestado apoyo al Servicio Federal de Seguridad ruso en el rastreo de cables submarinos de fibra óptica; Morgan Chalfant y Olivia Beavers (2018), "Spotlight Falls on Russian Threat to Undersea Cables", *The Hill*, <https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables/>.

⁶² CSIS (2022), "What Lies Beneath: Chinese Surveys in the Maritime Sea", <https://amti.csis.org/what-lies-beneath-chinese-surveys-in-the-south-china-sea/>; Huong Le Thu and Bart Hogeveen (2022), "UK, Australia and ASEAN Cooperation for Safer Seas", ASPI, <https://www.aspi.org.au/report/uk-australia-and-asean-cooperation-safer-seas>; Naomi O'Leary (2022), "Ireland's Crucial Submarine Cables are Vulnerable to Attack", *The Irish Times*, <https://www.irishtimes.com/world/europe/2022/09/28/irelands-submarine-cables-are-vulnerable-to-attack/>; Office of the Director of National Intelligence (2022), "Annual Threat Assessment of the US Intelligence Community", <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf>.

⁶³ Atle Staalesen (2022), "Human Activity' behind Svalbard Cable Disruption", *The Barents Observer*, <https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption>; Rishi Sunak (2017), "Undersea Cables: Indispensable, inseguro", Policy Exchange, <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>; en cuanto a las operaciones militares en el extranjero, véase Michael Sechrist (2010), "Cyberspace in Deep Water: Protecting Undersea Communications Cables by Creating an International Public-Private Partnership", Harvard Kennedy School. Sechrist explica cómo, a finales de 2008, se cortaron tres cables entre Italia y Egipto, lo que supuestamente provocó una reducción significativa de las operaciones de vehículos aéreos no tripulados estadounidenses en el Iraq.

⁶⁴ La interceptación de transmisiones por cable era una práctica de todas las grandes potencias navales en la era anterior a la fibra óptica. En comparación con los cables de cobre y coaxiales de antaño, hoy es más difícil intervenir físicamente los cables de fibra óptica y los repetidores. Se necesitarían equipos especiales que, al parecer, solo están al alcance de unos pocos Estados. Se trata de submarinos especialmente equipados o sumergibles que operan desde barcos y se requiere capacidad para exfiltrar y descifrar los datos de los cables sin ser advertido. Por el contrario, la infraestructura terrestre y los sistemas de gestión de red de un sistema de cable son mucho más vulnerables a las actividades de espionaje. Aunque se están destinando importantes esfuerzos a reforzar su seguridad física y cibernética, la protección total, incluso frente a amenazas y decisiones políticas internas, siempre será difícil de alcanzar.

A su vez, estas amenazas físicas y cibernéticas, que se producen en un contexto de creciente competencia tecnológica entre Estados, se incluyen explícita o implícitamente y cada vez con más frecuencia en las políticas y estrategias nacionales y regionales⁶⁵, así como en los acuerdos bilaterales de cooperación entre Estados⁶⁶. Se está aumentando el gasto en investigación y desarrollo de capacidades navales y tecnologías estratégicas para permitir, vigilar y disuadir de actividades que puedan afectar a los sistemas de cables submarinos, o bien conferir una ventaja sobre otros Estados en este ámbito⁶⁷. Estas amenazas impulsan decisiones legislativas destinadas a aumentar las inversiones en capacidad de reparación de cables⁶⁸ e investigación y desarrollo de tecnologías y redes de cables fiables para comunicaciones militares/de defensa. También son la razón por la que se están creando nuevos grupos de trabajo y estructuras de coordinación en determinadas regiones⁶⁹. Además, muchos Estados han empezado a intervenir más activamente en proyectos de cable para influir en las decisiones sobre su trazado, tecnologías y financiación por motivos de seguridad nacional⁷⁰, lo que dilata los procesos de concesión de licencias y permisos. En algunos casos, los Estados bloquean proyectos específicos en los que participan determinadas empresas, o cuando los cables llegan a tierra o conectan con determinadas jurisdicciones (véase el cuadro 1).

Tales decisiones van en la línea de otras similares de ámbito nacional o regional en materia de seguridad cuyo propósito es incluir otras tecnologías relacionadas con los cables submarinos

⁶⁵ Véase, por ejemplo, el Decreto 13873 (2019) de los Estados Unidos sobre protección de la cadena de suministro de servicios y tecnología de la información y las comunicaciones; Ministerio de las Fuerzas Armadas de Francia (2022), Estrategia ministerial para la guerra en los fondos marinos, https://archives.defense.gouv.fr/content/download/636000/10511901/file/20220214_FRENCH_SEABDED_STRATEGY_key_points.pdf; Directiva (UE) 2022/2555 de 14 de diciembre de 2022, <https://eur-lex.europa.eu/eli/dir/2022/2555>; OTAN (2023), "NATO Stands up Undersea Infrastructure Coordination Cell", https://www.nato.int/cps/en/natohq/news_211919.htm. Esta iniciativa se produce tras el anuncio de la creación de un grupo de trabajo conjunto UE-OTAN: OTAN (2023), "NATO and the EU Set up Taskforce on Resilience and Critical Infrastructure", https://www.nato.int/cps/en/natohq/news_210611.htm.

⁶⁶ Véanse, por ejemplo, el Acuerdo de Economía Digital Australia-Singapur 2020, párr. 22, <https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf>; y el Acuerdo sobre Economía Digital entre el Reino Unido y Singapur de 2022, apartado 7, Disposiciones adicionales, "Submarine Cable Landing Systems", <https://www.gov.uk/government/publications/uk-singapore-digital-economy-agreement-explainer/uk-singapore-digital-economy-agreement-final-agreement-explainer>. El Consejo UE-EE. UU. de Comercio y Tecnología también tiene previsto tratar la cuestión de los cables submarinos de telecomunicaciones en el marco de su Grupo de Trabajo sobre Seguridad y competitividad de las TIC. Entre los temas que se debatirán figuran la conectividad y la seguridad de los cables submarinos transatlánticos y posibles rutas alternativas, como la transatlántica, para conectar Europa, Norteamérica y Asia; los esfuerzos de diversificación de proveedores en las cadenas de suministro de TIC, y las tendencias del mercado hacia enfoques abiertos e interoperables y arquitecturas establecidas y de confianza; véase la Declaración Conjunta EE.UU.-UE de 2022 del Consejo de Comercio y Tecnología, titulada "Future Secure Connectivity Projects", <https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/>.

⁶⁷ Charlotte le Breton and Hugo Decis (2022), "France's Deep Dive into Seabed Warfare", IISS Military Balance Blog, <https://www.iiss.org/blogs/military-balance/2022/02/frances-deep-dive-into-seabed-warfare>; Martina Bet (2022), "Ben Wallace: Specialist Ships Will Protect Underwater Cables from Russia", *Evening Standard*, <https://www.standard.co.uk/news/politics/ben-wallace-moscow-russia-keir-starmmer-government-b1029675.html>; Jonathan Beale (2021), "New Royal Navy Ship to Protect 'Critical' Undersea Cables", *BBC News*, <https://www.bbc.com/news/uk-56472655>; Alexandra Brzozowski (2020), "NATO Seeks Ways of Protecting Undersea Cables from Russian Attacks", *Euractiv*, <https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/>; and Dimitrios Eleftherakis and Raul Vicen-Bueno (2020), "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors", *Sensors* 20:3, <https://www.mdpi.com/1424-8220/20/3/737>.

⁶⁸ En 2019, en virtud de su Ley de Autorización de la Defensa Nacional para el año fiscal 2020, Estados Unidos dispuso la creación de una "Flota de Seguridad de Cables"; en relación a los retos que afectan a la operatividad de la flota, véase Douglass R. Burnett (2022), "Repairing Submarine Cables Is a Wartime Necessity", *US Naval Institute, Proceedings* 148:10, <https://www.usni.org/magazines/proceedings/2022/october/repairing-submarine-cables-wartime-necessity>.

⁶⁹ Véase la nota a pie de página 67.

⁷⁰ Hilary McGeachy (2022), "The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns", *Australian Journal of International Affairs* 76:2.

de telecomunicaciones en listas de tecnologías críticas y emergentes y listas de control de exportaciones⁷¹, o invertir en proyectos de cable submarino y otras infraestructuras digitales en regiones marítimas de importancia estratégica, como el océano Atlántico, el mar Báltico, el Mediterráneo, el Indo-Pacífico, el paso del Noroeste, el mar de China Meridional, o regiones comercialmente importantes ricas en datos como África y Asia Sudoriental⁷².

En resumen, los cables submarinos de telecomunicaciones se están convirtiendo en un importante elemento de disputa geopolítica, lo que repercute notablemente en la seguridad y resiliencia de los cables y el ecosistema de las TIC en general, del que dependen cada vez más el funcionamiento y el bienestar de nuestras sociedades. Este hecho nos lleva a cuestionarnos si el actual régimen de gobernanza de los cables submarinos es el adecuado.

⁷¹ Véase, por ejemplo, Consejo Nacional de Ciencia y Tecnología de los Estados Unidos (2022), "Critical and Emerging Technologies List Update", pág. 4, <https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf>.

⁷² véase en las notas 68, 72 y 138 una visión más amplia de las inversiones en infraestructuras de cables submarinos.

Cuadro 1: Una década de decisiones reactivas de enrutamiento

- Esfuerzos de los Estados BRICS para construir un cable submarino que los conecte entre sí, a fin de evitar los elevados costes de enrutamiento a través de Europa y Estados Unidos, así como la posible interceptación de información crítica de índole financiera y de seguridad por parte de entidades ajenas a dicho grupo de Estados. A pesar de los positivos estudios de mercado, de tráfico y de viabilidad, el proyecto de cable no salió adelante. <https://www.offshore-energy.biz/brics-unveils-new-submarine-cable-system/>
- Esfuerzos de Brasil por buscar rutas alternativas, incluso con la Unión Europea, para evitar el tráfico a través de Estados Unidos (2014). <https://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224>
- Decisión de Australia de costear un cable submarino de 4.000 km que conecte Australia, las Islas Salomón y Papúa Nueva Guinea (2018). <https://www.bbc.co.uk/news/world-australia-44463553>
- Decisión de Chile de tender un cable a Australia, en lugar de a Asia (2020). <https://www.datacenterdynamics.com/en/news/chiles-transoceanic-cable-connect-new-zealand-and-australia/>
- Recomendación [del Team Telecom de Estados Unidos] a la Comisión Federal de Comunicaciones de Estados Unidos para que deniegue la conexión por cable submarino de Hong Kong a Estados Unidos de la Pacific Light Cable Network (2020). <https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea>
- Decisión de varias empresas de volver a presentar o retirar las solicitudes de licencia de aterrizaje para proyectos de cable transpacífico conectados con Hong Kong (2020-2021). <https://blog.telegeography.com/trans-pacific-cables-asian-hubs-plcn-status>
- Decisión de la Federación Rusa sobre el proyecto de cable Polar Express, destinado a conectar las comunidades árticas a lo largo de la costa noroeste (2021). <https://www.capacitymedia.com/article/29otdtk3j2ycxulos7b40/news/russia-begins-889m-polar-express-arctic-cable>
- Decisión de desarrollar la Ruta Far North Fibre Express, un proyecto de cable multicontinental a través del paso del Noroeste, en lugar del proyecto Arctic Connect previsto anteriormente, que habría discurrido por el paso del Noreste (2022). <https://www.thearcticinstitute.org/geopolitics-subsea-cables-arctic/>
- Recomendación [de Team Telecom de Estados Unidos] a la Comisión Federal de Comunicaciones de Estados Unidos, en relación con una propuesta de modificación del sistema de cable ARCOS-1 para incluir un punto de aterrizaje autorizado en Cuba, recomendando que se deniegue la conexión (2022). <https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through>
- Anuncio por parte del operador estatal de telecomunicaciones cubano ETESCA de que ha comenzado a trabajar con el operador francés de telecomunicaciones Orange para dotar al país de una conexión adicional, a través del territorio francés de ultramar Martinica (2022). <https://www.reuters.com/business/media-telecom/cuba-french-telecoms-operator-orange-begin-work-subsea-cable-martinique-2022-12-08/>
- Decisión de las empresas chinas de telecomunicaciones China Telecom y China Mobile de retirar su inversión en el proyecto de cable Sea-Me-We 6 tras la decisión de adjudicar la construcción a una empresa estadounidense en lugar de a una china (2022) <https://www.ft.com/content/8f35bf1e-fe32-4998-9e13-a13bac23506d>

El régimen de gobernanza de los cables submarinos de telecomunicaciones

El actual régimen de gobernanza de los cables se compone de un mosaico de tratados internacionales, marcos reguladores, organizaciones internacionales y regionales, asociaciones industriales, protocolos, normas y buenas prácticas⁷³. El Comité Internacional de Protección de los Cables (ICPC), uno de los principales organismos competentes en materia de cables submarinos, es un foro que permite a propietarios, operadores y proveedores de cables submarinos eléctricos o de telecomunicaciones y representantes de los gobiernos compartir información técnica, jurídica y medioambiental. La organización cuenta con más de 190 miembros de más de 69 países y representa a más del 98 % de los cables submarinos de telecomunicaciones del mundo. Busca concienciar sobre el hecho de que los cables submarinos son infraestructuras críticas, publicar buenas prácticas para la protección y resiliencia de los cables, ofrecer orientaciones sobre cuestiones técnicas y normativas y realizar recomendaciones para la instalación, la protección y el mantenimiento de los cables⁷⁴. La participación de los gobiernos en el ICPC es bienvenida y ha aumentado en los últimos años, aunque sigue siendo muy escasa. A nivel regional existen asociaciones de menor tamaño, como la Asociación Europea de Cables Submarinos (ESCA), la Asociación Norteamericana de Cables (NASCA) y la Asociación de Cables Submarinos de Oceanía (OSCA)⁷⁵.

Desde el punto de vista de la política gubernamental, la protección de los cables submarinos abarca una serie de ámbitos políticos como la seguridad marítima, los asuntos internos, la seguridad nacional, la defensa, la ciberseguridad, el espacio digital, las comunicaciones, el comercio, las inversiones y la industria. Aunque no existe un acuerdo internacional para la gobernanza de los cables submarinos, como se ha señalado, algunas organizaciones regionales como la Asociación de Naciones de Asia Sudoriental o la Unión Europea abarcan diversos aspectos de la gobernanza⁷⁶.

El eje vertebrador de la participación (y las responsabilidades) de los gobiernos en la protección de los cables submarinos puede hallarse en la legislación internacional vigente. De hecho, la cuestión de los cables submarinos se ha abordado en varios convenios, el primero de los cuales se remonta a finales del siglo XIX. Entre ellos, destacan los siguientes:

- Convención para la Protección de los Cables de Telégrafos Submarinos de 1884⁷⁷.
- La Convención de 1907 sobre las Leyes y Costumbres de la Guerra Terrestre y su anexo: Reglamento relativo a las Leyes y Costumbres de la Guerra Terrestre⁷⁸.

⁷³ Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", *Contemporary Security Policy* 42:3.

⁷⁴ Véase <https://www.iscpc.org>.

⁷⁵ Véanse más detalles sobre sus respectivos mandatos y miembros en ESCA, <https://escaeu.org>; NASCA, <https://www.n-a-s-c-a.org>; y OSCA, <http://www.oscagroup.com>. El Comité Danés de Protección de Cables es otro comité de este tipo que reúne a los agentes de la industria submarina, incluido el sector de las telecomunicaciones, que trabajan en aguas marítimas danesas.

⁷⁶ Véanse las notas 8 y 42.

⁷⁷ Para consultar el texto completo, véase <https://www.iscpc.org/documents/?id=13>.

⁷⁸ Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land (1907), regulations: art. 54, <https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907>.

- La Convención sobre la Alta Mar de 1958⁷⁹ y la Convención sobre la Plataforma Continental de 1958⁸⁰.
- La Convención de las Naciones Unidas sobre el Derecho del Mar de 1982 (CNUDM)⁸¹, que sustituye a las dos últimas y establece tres zonas de jurisdicción marítima en lo que respecta a los cables: los mares territoriales, la zona económica exclusiva y la alta mar⁸².

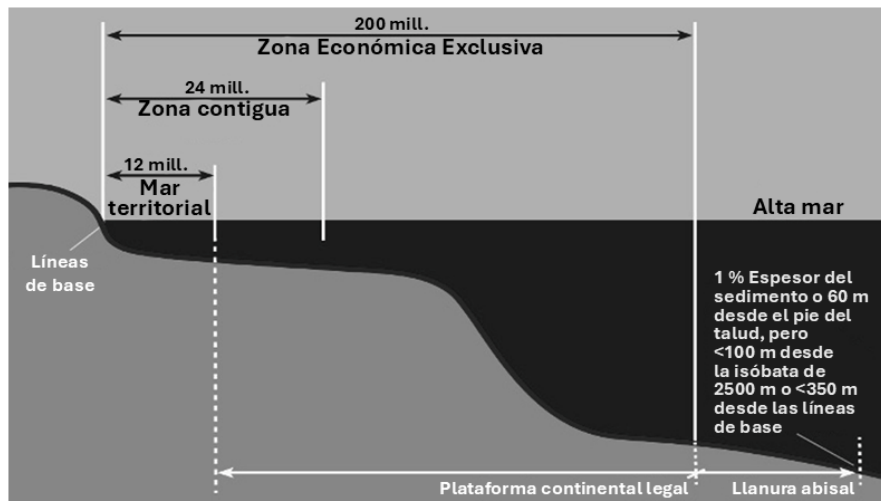


Figura X. Zonas marítimas CNUDM⁸³

En la actualidad, la CNUDM sigue siendo el principal punto de referencia en materia de cables submarinos (véanse las disposiciones pertinentes en el anexo 1). La CNUDM permite a los Estados tender cables en alta mar, en la zona económica exclusiva y en la plataforma continental, así como repararlos (art. 79). Incluye disposiciones sobre rotura y daños a cables submarinos (arts. 113, 114) y sobre indemnización por pérdidas (art. 115). Al igual que en la Convención sobre la Alta Mar, el art. 113 insta a los Estados Parte a adoptar una legislación nacional que penalice los daños causados a los cables en alta mar por buques que enarboles su pabellón o por personas sometidas a su jurisdicción. También amplía el ámbito de un delito punible para incluir "conductas que tengan por objeto causar tales rupturas o deterioros [en un cable submarino] o que puedan tener ese efecto", una disposición que se ha interpretado en el sentido de que permite a los Estados actuar para *evitar* que se produzcan roturas de cables⁸⁴.

Sin embargo, no son pocas las dificultades en lo que respecta a la cobertura legal y la adhesión. Para empezar, no todos los Estados son parte de la CNUDM. Además, esta Convención no otorga una jurisdicción adecuada sobre los infractores ni la capacidad de abordar los buques

⁷⁹ Artículos 1, 26-30; véase el texto completo en <https://www.iscpc.org/documents/?id=14>.

⁸⁰ Artículo 4; para consultar el texto completo, véase <https://www.iscpc.org/documents/?id=16>.

⁸¹ Artículos 3, 21, 33, 57-58, 79, 86-87, 112-115, 297; para el texto completo, véase https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm.

⁸² Lane Burdette (2021), "Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy", *Journal of Public and International Affairs*, <https://jpiia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>.

⁸³ United Nations (2013), "UNCLOS at 30", p. 4, https://www.un.org/depts/los/convention_agreements/pamphlet_unclos_at_30.pdf.

⁸⁴ Eric Wagner (1995), "Submarine Cables and Protections Provided by the Law of the Sea", *Marine Policy* 19:2, p. 136.

sospechosos, ya que la jurisdicción civil y penal en caso de daños a un cable se limita al Estado de origen del individuo responsable o al Estado del pabellón del buque responsable⁸⁵. La Convención para la Protección de los Cables de Telégrafos Submarinos de 1884 incluía una disposición que autorizaba a cualquier buque de guerra que sospechara que un buque extranjero había dañado un cable a “exigir del Capitán o patrón la exhibición de las piezas oficiales que justifiquen la nacionalidad de dicho barco”⁸⁶. Sin embargo, ni en las Convenciones de 1958 ni en la CNUDM se incluyó una norma a tales efectos⁸⁷. Asimismo, aunque la CNUDM exige a todos los Estados que adopten leyes que penalicen los daños causados intencionadamente o por negligencia culpable a un cable submarino, son pocos los Estados que lo han hecho de forma significativa⁸⁸. En los casos en que sí lo han hecho, se han calificado de “lamentablemente inadecuadas y no proporcionales a los daños resultantes de una interferencia intencionada”⁸⁹. Y, lo que es más importante, muchos Estados no cumplen la disposición de la UNCLOS relativa al mantenimiento y la reparación, imponiendo largos procesos de concesión de permisos de reparación cuyos efectos algunos han descrito como comparables al sabotaje⁹⁰.

Existen otras lagunas, sobre todo en lo que respecta a la protección de los cables durante los conflictos. En la Convención de 1884 se incluyó una disposición específica sobre la actividad beligerante, pero esta, más que restringir, permite libertad de acción a los beligerantes⁹¹. La CNUDM no contempla este asunto. El único otro instrumento que se refiere a los cables submarinos en situaciones de conflicto es la Convención de 1907⁹². Su artículo 54 establece protecciones especiales para los cables submarinos (incluidos los componentes terrestres) que conectan territorios ocupados con territorios neutrales, señalando que no pueden ser confiscados ni destruidos salvo en caso de absoluta necesidad y que debe pagarse inmediatamente una indemnización⁹³. El *Manual de San Remo sobre el derecho internacional aplicable a los conflictos armados en el mar* se hizo eco de esta postura, afirmando que “los beligerantes deberán evitar causar daños a los cables y tuberías tendidos en los fondos marinos que no sirvan exclusivamente a los beligerantes”⁹⁴. Sin embargo, hoy en día los cables submarinos transmiten datos de valor para todos los Estados, aunque no aterricen directamente en su territorio, lo que invita a cuestionar la pertinencia continua de esta

⁸⁵ Véase el comentario a colocación de esta cuestión en Yoram Dinstein y Arne Willy Dahl (eds.) (2020), *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*, regla 67, pág. 61 y siguientes; véase también Rishi Sunak (2017), “Undersea Cables: Indispensable, Insecure”, Policy Exchange, pág. 6, <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>.

⁸⁶ Convención para la Protección de los Cables de Telégrafos Submarinos de 1884, art. X.

⁸⁷ Communication with Prof. Dr. Wolff Heintschel von Heinegg, Chair of Public Law, in particular Public International Law, European Law and Foreign Constitutional Law, Europa-Universität Viadrina, 19 January 2023.

⁸⁸ Michael N. Schmitt (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, rule 54, para. 19, p. 258.

⁸⁹ Tara Davenport (2015), “Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis”, *Catholic University Journal of Law and Technology* 24(1).

⁹⁰ Lane Burdette (2021), “Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy”, *Journal of Public and International Affairs*, p. 4, <https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>; Hai Dang Vu (2020), “ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables”, *The International Journal of Marine and Coastal Law* 36:1.

⁹¹ “Queda bien entendido que las estipulaciones del presente Convenio no atacan de ningún modo la libertad de acción de los beligerantes”, art. XV, Convención para la Protección de los Cables de Telégrafos Submarinos de 1884.

⁹² Convención (IV) sobre las Leyes y Costumbres de la Guerra Terrestre y su anexo: Reglamento relativo a las Leyes y Costumbres de la Guerra Terrestre (1907), <https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907>.

⁹³ *Ibid.*, reglamento: art. 54.

⁹⁴ *Manual de San Remo sobre el derecho internacional aplicable a los conflictos armados en el mar* (1994), párr. 37. Obsérvese que el *Manual de San Remo* “tiene por finalidad exponer el actual derecho internacional aplicable a los conflictos armados en el mar” y fue elaborado por un grupo de expertos jurídicos y navales a título personal entre 1988 y 1994; véase <https://international-review.icrc.org/sites/default/files/S0250569X0002481Xa.pdf>.

disposición para los cables de comunicaciones submarinos⁹⁵. Los expertos también se preguntan si atentar contra un cable submarino fuera de la jurisdicción de un Estado podría considerarse un ataque armado a efectos del artículo 51 de la Carta de las Naciones Unidas, que permite el uso de la fuerza por un Estado en legítima defensa.

Varias iniciativas han abordado estas lagunas, y también han considerado nuevos desarrollos, como las operaciones cibernéticas que afectan a los cables submarinos. Algunos de estos trabajos han servido de base a publicaciones como el *Manual de Tallin*, sobre el derecho internacional aplicable a las operaciones cibernéticas, y el *Manual de Oslo*, que aborda una selección de temas sobre derecho de los conflictos armados. Por ejemplo, el *Manual de Tallin 2.0* señala que la CNUDM es aplicable a las operaciones cibernéticas llevadas a cabo desde o a través de infraestructuras cibernéticas situadas en los mares, e indica que “operaciones cibernéticas pueden desplegarse desde buques y navíos en el mar, aeronaves sobre el mar, instalaciones en alta mar o a través de cables submarinos de telecomunicaciones, tanto en tiempos de paz como de conflicto”⁹⁶. Concluye que “el derecho internacional vigente aplicable a los cables submarinos, incluidos los de telecomunicaciones, y a su explotación, refleja en general el derecho internacional consuetudinario”⁹⁷, al considerar los cables submarinos de telecomunicaciones como cualquier “cable propiedad de un Estado, explotado o tendido por este, o de propiedad privada, autorizado por dicho Estado para el tráfico de telecomunicaciones y datos”⁹⁸. En cuanto al artículo 113 de la CNUDM, el *Manual de Oslo* concluye que los “Estados que hayan tendido cables submarinos [...], o cuyos nacionales hayan tendido y exploten tales cables [...] tienen derecho a adoptar medidas de protección a fin de prevenir o poner fin a cualquier interferencia perjudicial”⁹⁹. Por su parte, el *Manual de Tallin 2.0* concluye que una operación cibernética que dañe un cable submarino está prohibida por el derecho internacional consuetudinario, aunque implica que los cables submarinos pueden ser blanco de ataques en el contexto de un conflicto armado, con sujeción a los principios de distinción y proporcionalidad¹⁰⁰. También sugiere que un ciberataque realizado a través de un cable submarino de telecomunicaciones en el contexto de un conflicto armado convertiría al cable en un objetivo lícito. Ambos manuales establecen que los cables de telecomunicaciones modernos plantean dudas sobre el artículo 54 de la Convención de 1907, y el *Manual de Oslo* señala específicamente que “solo en circunstancias excepcionales será posible determinar que sirven exclusivamente a uno o más beligerantes”, de ahí la importancia de “distinguir entre cables submarinos de telecomunicaciones y otros cables submarinos”¹⁰¹.

⁹⁵ El *Manual de Tallin 2.0* presta especial atención a esta disposición, señalando que dado que los cables submarinos facilitan las comunicaciones cibernéticas, este punto tiene especial relevancia en el contexto cibernético; Michael N. Schmitt (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, regla 150, párr. 10, pág. 549. Véase también Lane Burdette (2021), “Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy”, *Journal of Public and International Affairs*, pág. 3, <https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy> quien destaca el precedente estadounidense, confirmado posteriormente en un tribunal de arbitraje entre Estados Unidos y el Reino Unido en 1923, que permite cortar cables entre Estados objetivo y neutrales dentro de una ZEE objetivo, lo que no se refleja en la evaluación de los expertos del *Manual de Tallin*.

⁹⁶ Michael N. Schmitt (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, regla 54, párr. 1, págs. 252 y 253.

⁹⁷ *Ibid.*, pp. 252–258.

⁹⁸ *Ibid.*

⁹⁹ Yoram Dinstein and Arne Willy Dahl (eds) (2020), *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*, rule 67, p. 61.

¹⁰⁰ Michael N. Schmitt (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, rule 54, para. 15, p. 256.

¹⁰¹ Yoram Dinstein and Arne Willy Dahl (eds) (2020), *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*, rule 69, p. 63.

Varios estudiosos han abogado por una cobertura jurídica internacional adicional para la actividad que afecta a los cables submarinos, incluida la negociación de un nuevo instrumento¹⁰². Para ello, algunos han sugerido “utilizar la estructura de las convenciones antiterroristas [de Naciones Unidas]” como guía¹⁰³. Otros han adoptado un enfoque más limitado, sugiriendo nuevas disposiciones de la CNUDM que aclaren las responsabilidades, obligaciones y medidas de cumplimiento, y refuercen la cooperación mutua en materia de aplicación de la ley contra las actividades delictivas¹⁰⁴. Otros planteamientos más limitados proponen establecer zonas de protección de cables en áreas costeras con corredores de comunicaciones de alto valor, aunque esto podría hacer que los cables fueran más vulnerables de lo que ya son¹⁰⁵.

Algunos estudiosos también han sugerido la creación de un organismo internacional bajo el amparo del sistema de las Naciones Unidas con responsabilidad jurídica y política sobre los cables submarinos¹⁰⁶. Otros han propuesto utilizar el sistema vinculante de resolución de controversias del Tribunal Internacional del Derecho del Mar “para crear un régimen internacional de protección contra los daños causados a los cables submarinos” y “contra las violaciones del derecho a la privacidad”¹⁰⁷. Por su parte, las propuestas académicas más centradas en el derecho internacional aplicable a los cables submarinos durante los conflictos armados incluyen sugerencias para modificar la disposición de la Convención de 1884 sobre la actividad beligerante a fin de prohibir los daños intencionados por medios físicos o cibernéticos. También se propone establecer otra convención más, que coloque los cables submarinos de telecomunicaciones bajo una protección especial durante los conflictos, similar a la protección de los bienes culturales durante los conflictos armados¹⁰⁸. Otros han sugerido modificar la aplicación de la norma ordinaria de proporcionalidad en la selección de objetivos¹⁰⁹.

¹⁰² Robert Beckman, “Protecting Submarine Cables from Intentional Damage: the Security Gap”, in Douglas R. Burnett, et al. (eds) (2013), *Submarine Cables: The Handbook of Law and Policy*, BRILL; Tara Davenport (2015), “Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis”, *Catholic University Journal of Law and Technology* 24(1); Zoe Scanlon (2017), “Addressing the Pitfalls of Exclusive Flag State Jurisdiction: Improving the Legal Regime for the Protection of Submarine Cables”, *Journal of Maritime Law and Commerce* 48:3; Rishi Sunak (2017), “Undersea Cables: Indispensable, Insecure”, Policy Exchange, pp. 35–36. <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>.

¹⁰³ Christian Bueger and Tobias Liebetrau (2021), “Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network”, *Contemporary Security Policy* 42:3, p. 398.

¹⁰⁴ Tara Davenport (2015), “Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis”, *Catholic University Journal of Law and Technology* 24(1).

¹⁰⁵ Rishi Sunak (2017), “Undersea Cables: Indispensable, Insecure”, Policy Exchange, <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>. En sus Buenas prácticas gubernamentales, el CIPC recomienda no establecer zonas y corredores de protección de cables dentro de áreas geográficas fijas o, como mínimo, sugiere entablar consultas con los operadores de cable cuando se adopte un enfoque de este tipo. Estos últimos suelen estar en contra de tales zonas y corredores de protección, ya que “1) proporcionan una separación espacial insuficiente de otros cables submarinos para su instalación y mantenimiento, y 2) fomentan la agrupación geográfica de las rutas y los puntos de aterrizaje de los cables submarinos, lo que aumenta el riesgo de que un único suceso natural o provocado por la acción del hombre pueda dañar varios cables”; ICPC (2022), “Buenas prácticas gubernamentales para proteger y promover la resiliencia de los cables submarinos de telecomunicaciones”, pág. 3, <https://www.iscpc.org/documents/?id=3733>.

¹⁰⁶ Christian Bueger and Tobias Liebetrau (2021), “Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network”, *Contemporary Security Policy* 42:3, p. 399.

¹⁰⁷ Jason Petty (2021), “How Hackers of Submarine Cables May Be Held Liable Under the Law of the Sea”, *Chicago Journal of International Law* 22:1.

¹⁰⁸ Por ejemplo, la Convención para la Protección de los Bienes Culturales en caso de Conflicto Armado de 1954 (a su vez guiada por los principios relativos a la protección de los bienes culturales durante los conflictos armados, las Convenciones de La Haya de 1899 y 1907 y el Pacto de Washington de 1935); véase Dennis E. Harbin III (2021), “Targeting Submarine Cables: New Approaches to the Law of Armed Conflict in Modern Warfare”, *Military Law Review* 229, <https://tjagcls.army.mil/documents/35956/304883/3+Harbin+Final.pdf>.

¹⁰⁹ Véase Rob McLaughlin, Tamsin Phillipa Paige y Douglas Guilfoyle (2022), “Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization”, *Journal of Conflict and Security Law* 27:3.

¿Cuál es el futuro de la gobernanza de los cables submarinos?

Existe una sólida base para afirmar que el actual régimen de gobernanza de los cables submarinos es insuficiente para afrontar los retos que depara este siglo. También son muchos los argumentos a favor de la necesidad de un nuevo instrumento mundial, particularmente si se tiene en cuenta nuestra dependencia de los cables submarinos para la conectividad y el hecho irrefutable de que los instrumentos existentes no reflejan la naturaleza de las tecnologías actuales. Sin embargo, muchos expertos insistirían en que el derecho internacional vigente es suficiente y que los Estados deben cumplir las obligaciones y compromisos ya contraídos antes de plantearse siquiera desarrollar un nuevo instrumento. Incluso si los Estados acordasen que es necesario un nuevo tratado centrado específicamente en la protección de los cables submarinos, probablemente la negociación se alargaría décadas y sería difícil acordar su ámbito de aplicación, dado que los sistemas de cables submarinos son solo un elemento, aunque crítico, del ecosistema más amplio de las TIC. Como se ha señalado, se han sugerido enfoques menos ambiciosos centrados en reforzar los instrumentos existentes. Cada uno de ellos tiene su valor y debería estudiarse más a fondo.

Existen otras formas complementarias de reforzar el régimen de gobernanza y resiliencia de los sistemas de cables submarinos. Por ejemplo, existe la opción de aumentar la participación de las fuerzas militares en la protección y seguridad de los cables, incluso con medidas como la creación de estructuras de coordinación específicas, la detección y vigilancia submarinas y el destacamento de patrullas marítimas de superficie en aguas de importancia estratégica, así como la vigilancia por satélite de dichas aguas¹¹⁰. Existe asimismo la opción de establecer una regulación más estricta, en particular para garantizar el uso de tecnologías de confianza, asegurar capacidades soberanas de mantenimiento y reparación¹¹¹ y aumentar el intercambio de información con los propietarios y operadores de los cables¹¹². Por importantes que sean, estos distintos enfoques responden a las preocupaciones con respecto a la resiliencia y la seguridad de determinados países o regiones. Deben ir acompañadas de esfuerzos para reforzar la resiliencia de los cables submarinos de telecomunicaciones a escala mundial.

Tal vez un punto de partida para ese diálogo global podría ser reconocer la naturaleza sistémica de los retos que nos ocupan y profundizar en la comprensión de los esfuerzos de mitigación de riesgos que la industria y las comunidades técnicas ya están llevando a cabo (como una mayor diversificación de las rutas y la capacidad de los cables, la adopción de principios y tecnologías de confianza cero, el refuerzo de la seguridad de las infraestructuras y los componentes terrestres, o el avance de las técnicas de detección óptica para la supervisión de los sistemas). Los Estados pueden complementar estos esfuerzos fomentando la aplicación y la adhesión a las recomendaciones existentes y los nuevos requisitos relativos a las infraestructuras críticas de TIC. Entre ellos, destacan los siguientes:

¹¹⁰ Por ejemplo, la nueva célula de coordinación de la OTAN anunciada el 15 de febrero de 2022; véase también Rishi Sunak (2017), "Undersea Cables: Indispensable, Insecure", Policy Exchange, págs. 35 y 36, <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>; Andreas Rinke y Matthias Williams (2022), "Germany and Norway Want NATO to Protect Subsea Infrastructure after Nord Stream Attacks", *Reuters*, <https://www.reuters.com/business/energy/germany-norway-ask-nato-protect-subsea-infrastructure-after-nord-stream-attacks-2022-11-30/>.

¹¹¹ Ian Douglas (2021), "Future Proofing the UK's Critical Subsea Cable Infrastructure", Global Marine Group, <https://nationalpreparednesscommission.uk/2021/09/future-proofing-the-uks-critical-subsea-cable-infrastructure/>.

¹¹² Véase, por ejemplo, la Directiva (UE) 2022/2555 de 14 de diciembre de 2022, <https://eur-lex.europa.eu/eli/dir/2022/2555>.

- las buenas prácticas del ICPC para proteger y promover la resiliencia de los cables submarinos de telecomunicaciones, cuya esencia se deriva de la CNUDM, y su próxima recomendación sobre la seguridad de las cámaras de playa, las redes *fronthaul* y las estaciones de aterrizaje de cables;
- los elementos pertinentes del marco para el comportamiento responsable de los Estados negociado en las Naciones Unidas en relación con las TIC y la seguridad internacional¹¹³; y
- los nuevos requisitos que surgen a escala nacional y regional, incluida la Directiva de la Unión Europea sobre redes y sistemas de información¹¹⁴.

Este planteamiento no resolverá algunas de las cuestiones geopolíticas más espinosas que aquí se debaten, como el señalamiento de algunos Estados que podrían poner en peligro infraestructuras críticas, como los sistemas de cables submarinos, en su propio beneficio. No obstante, puede suponer un avance en los esfuerzos para proteger y asegurar los sistemas y las redes terrestres y por satélite a las que se conectan, mejorando así su resistencia y su capacidad para generar los dividendos económicos y sociales que tanto se necesitan.

¹¹³ Véase, por ejemplo, <https://www.unep.org/civil-society-engagement/why-civil-society-matters/major-groups-stakeholders>

¹¹⁴ Por ejemplo, la Directiva (UE) 2022/2555 de 14 de diciembre de 2022, <https://eur-lex.europa.eu/eli/dir/2022/2555>.

Análisis de los esfuerzos seleccionados

Las buenas prácticas gubernamentales del ICPC son recomendaciones elaboradas a partir de la legislación y la política internacionales existentes, los protocolos y normas del sector, la práctica de los Estados y el sentido común básico¹¹⁵. Abarcan una amplia variedad de temas. Por ejemplo, los principios generales (apartado 1) sugieren que en sus planes nacionales de resiliencia, los Estados se centren en:

- riesgos estadísticamente significativos en los que la acción gubernamental podría ser fundamental para la reducción del riesgo;
- puntos de aterrizaje múltiples y diversos de cables submarinos en la jurisdicción de los Estados;
- respeto y aplicación de las obligaciones contraídas y el derecho internacional consuetudinario que define la jurisdicción de los Estados sobre los cables submarinos y su protección;
- fomento de regímenes reguladores transparentes que agilicen la instalación y la reparación de los cables siguiendo unos plazos bien establecidos;
- estrechas consultas con el sector para comprender la tecnología y los parámetros de funcionamiento del mismo y compartir datos sobre los riesgos;
- complementar las buenas prácticas existentes en el sector;
- reconocer que las propias leyes y políticas gubernamentales pueden a veces aumentar los riesgos de daños y reducir la capacidad de recuperación; y
- comprometerse con otros Estados a nivel mundial y regional, ya que las acciones de otros Estados pueden afectar en gran medida a la propia conectividad de un Estado.

Buenas prácticas gubernamentales para proteger y promover la resiliencia de los cables submarinos de telecomunicaciones

1. Principios generales
2. Riesgos de la pesca y el fondeo (70 % de los fallos)
3. Separación espacial
4. Cartas náuticas
5. Leyes de protección del cableado nacional y sanciones por daños
6. Planificación del espacio marino y coordinación interindustrial
7. Punto de contacto único
8. Optimización de las rutas y de los puntos de aterrizaje; diversidad geográfica
9. Permisos de instalación y reparación
10. Restricciones al cabotaje y a la tripulación
11. Requisitos de entrada al puerto
12. Aranceles de aduana, impuestos y tasas
13. Reclamaciones y disputas sobre límites marítimos
14. Designación de infraestructuras críticas
15. Intercambio de datos sobre riesgos e incidentes
16. Impacto de otras actividades reguladoras en alta mar.

Cuadro 1. Buenas prácticas gubernamentales del ICPC

¹¹⁵ ICPC (2022), "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables", <https://www.iscpc.org/documents/?id=3733>.

Las buenas prácticas del ICPC ofrecen orientaciones más detalladas sobre diversas áreas temáticas, todas ellas pertinentes para reforzar la resiliencia. Por ejemplo, las recomendaciones de que los Estados designen los cables submarinos como infraestructuras críticas¹¹⁶, recopilen y evalúen datos sobre vulnerabilidades y amenazas y desarrollen y apliquen políticas para reducirlas, probablemente sean adecuadas para todos los Estados. También convendría priorizar la atención y los recursos y diferenciar entre los riesgos involuntarios y los que afectan a la seguridad nacional e internacional. Asimismo, supondría un gran avance establecer un único punto de contacto para coordinar mejor la actuación de los gobiernos a lo largo del ciclo de vida de los cables, parámetros básicos para la concesión de permisos de instalación y reparación y mecanismos para que operadores y gobiernos intercambien datos sobre incidentes e información sobre amenazas.

También podrían obtenerse resultados aplicando la recomendación sobre las leyes nacionales de protección de cables de forma coherente con la CNUDM. Ello contribuiría a asegurar que se aplican sanciones importantes por daños. Las guardias costeras y otras fuerzas de seguridad pertinentes estarían “suficientemente familiarizados con las leyes de protección de los cables para hacerlas cumplir y [cooperar] con los operadores de cable y [ayudarles] a investigar las reclamaciones por daños”¹¹⁷. Del mismo modo, un conocimiento más profundo por parte de los gobiernos en materia de separación espacial, enrutamiento y aterrizaje puede ayudar a proteger contra las malas decisiones políticas y aceleraría la adopción de los marcos reguladores y la asignación de recursos tan necesarios en este ámbito¹¹⁸. Además, una mayor claridad sobre la aplicación por parte de los Estados de estas prácticas recomendadas, así como de las dificultades a las que se enfrentan, contribuiría notablemente al diálogo en curso. También resultaría de utilidad aprender de los esfuerzos de la Oficina de las Naciones Unidas contra la Droga y el Delito, entre otras organizaciones, para apoyar a los Estados miembros en la aplicación de estas buenas prácticas¹¹⁹.

Además de estas buenas prácticas, el Grupo de Trabajo sobre Seguridad de los Cables del ICPC también trabaja en la elaboración de una recomendación para la protección de elementos singulares de la infraestructura de cables submarinos, como las cámaras de playa, las redes *fronthaul* y las estaciones de aterrizaje de cables. La recomendación no aborda cuestiones relacionadas con la ciberseguridad o la seguridad de la información, y reconoce que la seguridad de las comunicaciones en sí no es una cuestión exclusiva de los cables submarinos y se aborda en la ciberseguridad de las redes de comunicaciones electrónicas, como la norma ISO 27001 y los marcos de ciberseguridad normativos a nivel nacional¹²⁰.

¹¹⁶ *Ibid.*, apartado 4, punto 5, señala que la resolución 4/1967 de la Organización Hidrográfica Internacional exige que las autoridades cartográficas incluyan un cuadro de texto en todas las cartas náuticas en el que se establezcan las distancias mínimas para operar cerca de los cables e insta a “considerar a los cables submarinos una infraestructura crítica” cuyo daño “podría provocar una catástrofe nacional”, [énfasis añadido]; véase también el debate sobre la separación espacial en *ibid.*, apartado 3, que también aborda la aplicación de la resolución.

¹¹⁷ *Ibid.*, apartado 5.

¹¹⁸ *Ibid.*, p. ej., apartados 3, 6 y 8.

¹¹⁹ Véase, por ejemplo, Kaithlin Meredith (2021), “Protecting Submarine Cables in the Indian Ocean”, UNODC, <https://www.unodc.org/easternafrika/en/Stories/protection-of-submarine-cables-in-indian-ocean.html>.

¹²⁰ Communication with ICPC representative, 17 January 2022.

Promover esta recomendación una vez se publique, así como los intercambios pertinentes sobre los avances en su aplicación, será también una contribución importante.

En lo que respecta a la ciberseguridad, también cabe abordar una serie de desarrollos internacionales. Por ejemplo, las negociaciones de la Primera Comisión de la Asamblea General sobre las TIC y la seguridad internacional han dado lugar a un marco en ciernes sobre comportamiento responsable de los Estados, cuyos elementos se refieren concretamente a la protección de infraestructuras críticas¹²¹. De hecho, la primera de las tres normas relacionadas con las infraestructuras críticas recomendadas por el GEG en 2015 se refiere a la responsabilidad de los Estados de “no realizar ni apoyar a sabiendas actividades de las TIC contrarias a las obligaciones que les incumben en virtud del derecho internacional que perjudiquen intencionadamente las infraestructuras críticas o dificulten de otro modo la utilización y funcionamiento de esas infraestructuras para prestar servicios al público”¹²². En su explicación de los tipos de infraestructuras críticas que pueden desprenderse de esta norma, dos informes posteriores aclaran que puede referirse a aquellas infraestructuras que prestan servicios a través de varios Estados, como “la infraestructura técnica esencial para la integridad y disponibilidad general de Internet”, que, según una lógica más amplia del ecosistema de las TIC, incluiría los cables submarinos de telecomunicaciones¹²³.

También son aplicables las otras dos normas relacionadas con las infraestructuras críticas recomendadas en el mismo informe, en particular que “los Estados deben tomar medidas apropiadas para proteger sus infraestructuras críticas frente a amenazas relacionadas con las TIC, teniendo en cuenta la resolución 58/199 de la Asamblea General”¹²⁴; y que “los Estados deben atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras críticas sean objeto de actos malintencionados relacionados con las TIC. Los Estados también deben atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada con las TIC originada en su territorio que se dirija contra infraestructuras críticas de otro Estado, teniendo debidamente en cuenta la soberanía”¹²⁵. En un informe de 2021 de

¹²¹ Véanse los informes pertinentes en Asamblea General, documento de la ONU A/70/174 (2015), https://digitallibrary.un.org/record/799853/files/A_70_174-ES.pdf; Asamblea General, documento de la ONU A/76/135 (2021), <https://documents.un.org/doc/undoc/gen/n21/075/89/pdf/n2107589.pdf>; y Asamblea General, documento de la ONU A/AC.290/2021/CRP.2 (2021), <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>.

¹²² Asamblea General, documento de la ONU A/76/135 (2021), norma 13 f), párrs. 42 a 46, <https://documents.un.org/doc/undoc/gen/n21/075/89/pdf/n2107589.pdf>.

¹²³ *Ibid.* La redacción “la infraestructura técnica esencial para la integridad o disponibilidad general de Internet” se deriva de las propuestas de los Países Bajos relativas al núcleo público de Internet, que a su vez se inspira en el trabajo del académico holandés Dennis Broeders sobre el tema, retomado posteriormente por la Comisión Global sobre la Estabilidad del Ciberespacio en su propuesta de norma para proteger el núcleo público de Internet. Véanse los informes pertinentes de las Naciones Unidas en la nota 122. Véase la publicación de Broeders en Dennis Broeders (2016), *The Public Core of the Internet: An International Agenda for Internet Governance*, Netherlands Scientific Council for Government Policy, <https://library.oapen.org/bitstream/handle/20.500.12657/32439/610631.pdf>. En relación al informe de la Comisión Global sobre la Estabilidad del Ciberespacio y su defensa de una norma de no interferencia con el “núcleo público de Internet”, definido como aquel que incluye elementos críticos de la infraestructura de Internet, como el enrutamiento y reenvío de paquetes, los sistemas de nombres y numeración, los mecanismos criptográficos de seguridad e identidad, los medios de transmisión [incluidos los cables terrestres y submarinos y las estaciones de aterrizaje, los centros de datos y otras instalaciones físicas que les dan servicio], el *software* y los centros de datos (págs. 30 y 31), véase Comisión Global sobre la Estabilidad del Ciberespacio (2019), “Advancing Cyberstability: Informe final”, <https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf>.

¹²⁴ General Assembly, UN document A/76/135 (2021), norm 13(g), paras. 47–50, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

¹²⁵ *Ibid.*, norma 13 h), párrs. 51 a 55.

otro GEG se ofrecieron orientaciones específicas sobre cómo interpretar estas normas, que fueron abordadas por un GTCA con un enfoque más amplio¹²⁶.

Normas recomendadas por la ONU en materia de infraestructuras críticas

13 f) Los Estados no deben realizar o apoyar a sabiendas actividades de TIC contrarias a sus obligaciones en virtud del derecho internacional que dañen intencionadamente infraestructuras críticas o perjudiquen de otro modo el uso y funcionamiento de infraestructuras críticas para prestar servicios al público.

13 g) Los Estados deberían tomar las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las TIC, teniendo en cuenta la resolución 58/199 de la Asamblea General.

13 h) Los Estados deberían atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras fundamentales fueran objeto de actos malintencionados relacionados con las TIC. Los Estados también deberían atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada con las TIC originada en su territorio contra infraestructuras fundamentales de otro Estado, teniendo debidamente en cuenta la soberanía.

Cuadro 2. Normas recomendadas en materia de infraestructuras críticas, GEG 2015

Muchas más recomendaciones y conclusiones de los informes elaborados por estos grupos de negociación pueden y deben entenderse como aplicables también a los cables submarinos y las infraestructuras conexas. En ellas se determina que el derecho internacional vigente, incluida la Carta de las Naciones Unidas, se aplica al uso de las TIC por parte de los Estados, otras recomendaciones sobre normas¹²⁷ y las recomendaciones sobre medidas de fomento de la confianza pertinentes para la protección de infraestructuras críticas, incluidas las relativas a puntos de contacto e intercambios entre Estados y con el sector privado de información sobre amenazas, vulnerabilidades y respuesta a incidentes¹²⁸. Nuevamente, un conocimiento claro de la adhesión de los Estados a dichos compromisos en lo que respecta a los cables submarinos y la infraestructura conexas contribuiría notablemente a los debates en curso.

A escala regional, la Unión Europea ha seguido esta línea de pensamiento en su versión actualizada de la directiva sobre redes y sistemas de información, al señalar la importancia de las comunicaciones submarinas para “la digitalización competitiva de la Unión y su economía”¹²⁹. Basándose en marcos existentes, como el marco europeo de telecomunicaciones, la Ley de Ciberseguridad de la UE y la Directiva 2013/40/UE que prohíbe los ataques contra los sistemas de información, lleva más allá algunas de las recomendaciones sobre intercambio de información y notificación de incidentes, imponiendo a las empresas una nueva obligación de notificación de incidentes que afecten a dichos sistemas y ampliando el alcance de la cobertura

¹²⁶ Véase la nota a pie de página 122.

¹²⁷ Véase, por ejemplo, la norma 13 c), conocida como la norma de “diligencia debida” que insta a los Estados a no permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando TIC; la norma 13 e), relativa a la protección de los derechos humanos; y la norma 13 i), que establece que se debe garantizar la integridad de la cadena de suministro; Asamblea General, documento de la ONU A/76/135 (2021), norma 13 g), párrs. 47 a 50, <https://documents.un.org/doc/undoc/gen/n21/075/89/pdf/n2107589.pdf>

¹²⁸ Ibid.

¹²⁹ Directive (EU) 2022/2555 of 14 December 2022, para. 97, <https://eur-lex.europa.eu/eli/dir/2022/2555>.

para incluir a las entidades de telecomunicaciones¹³⁰. La directiva sobre redes y sistemas de información también insta a los gobiernos a contemplar los aspectos de ciberseguridad de los sistemas de cables submarinos en sus estrategias nacionales de ciberseguridad, cuando proceda, y a elaborar un mapa de posibles riesgos de ciberseguridad y medidas de mitigación “para garantizar el máximo nivel de protección”¹³¹. Más concretamente, hace un llamamiento para que los Estados miembros adopten políticas “relacionadas con el mantenimiento de la disponibilidad general, la integridad y la confidencialidad del núcleo público de la internet abierta, incluida, cuando proceda, la ciberseguridad de los cables submarinos de comunicaciones”¹³². Se está trabajando para conciliar estas y otras medidas de la Directiva de las medidas propuestas en otros instrumentos recientes. También sería muy positivo para el diálogo en curso garantizar intercambios regulares y bidireccionales entre los Estados pertinentes y los agentes de la industria sobre la aplicación de estas medidas.

¹³⁰ Proposal COM/2020/823 of 16 December 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0823>; Directive 2002/21/EC of 7 March 2002, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021>; Directive (EU) 2018/1972 of 11 December 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2018.321.01.0036.01.ENG>; and Directive 2013/40/EU of 12 August 2013, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040>.

¹³¹ Directive (EU) 2022/2555 of 14 December 2022, para. 97, <https://eur-lex.europa.eu/eli/dir/2022/2555>.

¹³² *Ibid.*, art. 7, párr. 2, letra d).

Sentar las bases para una mayor resiliencia de los sistemas de cables submarinos a escala mundial

¿Qué se puede hacer para alcanzar una mayor resiliencia de los cables submarinos a escala mundial y lograr que evolucione el marco existente de comportamiento responsable de los Estados en relación con las TIC? Teniendo en cuenta el apartado anterior, podría plantearse una agenda preliminar centrada en lo siguiente.

Los cables submarinos de telecomunicaciones como infraestructuras críticas

Los cables submarinos de telecomunicaciones son un elemento esencial del ecosistema de las TIC. Todos dependemos de ellos, directa o indirectamente, por lo que redundaría en nuestro interés colectivo garantizar que sean considerados como tal. En este sentido, todos los Estados, incluidos aquellos sin litoral, deberían declarar los cables submarinos de telecomunicaciones como infraestructuras críticas. Los Estados pueden además tomar las siguientes medidas:

- Reafirmar públicamente su compromiso hacia las tres normas relacionadas con las infraestructuras críticas y otras disposiciones conexas recomendadas por las Naciones Unidas en su trabajo sobre la seguridad internacional y las TIC. Los Estados pueden anunciar públicamente su compromiso con estas directrices, también en lo que se refiere a los cables submarinos y las infraestructuras conexas, y promover la adhesión a las mismas en foros y acuerdos bilaterales, plurilaterales o multilaterales. A la luz de la creciente preocupación por la actividad intencionada de los Estados que daña deliberadamente los sistemas de cables submarinos o menoscaba de otro modo el uso y el funcionamiento de dichas infraestructuras para prestar servicios al público, los Estados también pueden avanzar en el debate, por difícil que sea, sobre las consecuencias de dicha actividad.
- Reforzar la legislación, los marcos normativos y las políticas nacionales pertinentes para la protección y la resiliencia de los cables submarinos y las infraestructuras conexas, en consonancia con las obligaciones y prácticas existentes, así como aclarar las funciones y responsabilidades de las autoridades nacionales.
- Reforzar los planteamientos nacionales de gestión y mitigación de riesgos de los sistemas de cables, la preparación ante emergencias que compete a la respuesta a incidentes y la reparación, y los enfoques de clasificación y notificación de incidentes que afecten a los cables submarinos y a las infraestructuras y componentes conexas.
- Intercambiar experiencias sobre la aplicación de las recomendaciones y mejores prácticas del ICPC para la protección y resiliencia de los cables submarinos, así como su futura recomendación sobre la seguridad de las infraestructuras terrestres.
- Intercambiar experiencias de cooperación mutua en la reparación de cables en territorios en disputa o durante catástrofes naturales y sobre la facilitación del acceso a los buques de reparación de cables, con vistas a establecer mecanismos para situaciones de crisis.
- Intercambiar experiencias de cooperación entre guardacostas y fuerzas de seguridad para investigar las alteraciones de cables y otras actividades ilícitas.

- Publicar e intercambiar puntos de vista nacionales sobre la aplicación de la legislación internacional vigente a la alteración o el sabotaje de cables en situaciones de crisis y conflicto, incluidas las operaciones militares destinadas a dañar deliberadamente componentes e infraestructuras de cables submarinos o las operaciones de espionaje que provocan daños involuntarios, actividades estas que afectan a la disponibilidad de la red, al tránsito de las telecomunicaciones y el tráfico de datos.
- Proporcionar mayores fuentes de apoyo internacional y desarrollo de capacidades para los países vulnerables a fin de garantizar la seguridad física y cibernética de las infraestructuras de cables submarinos y otras instalaciones y sistemas similares, así como en los ámbitos del desarrollo y la aplicación de la legislación y la reglamentación nacionales¹³³.

Reforzar la cooperación entre los sectores público y privado

Las empresas privadas poseen y explotan la mayoría de los sistemas de cables submarinos y disponen de información esencial sobre las amenazas y vulnerabilidades que afectan a dichos sistemas, así como de una vasta experiencia en la gestión y mitigación de riesgos. Los nuevos requisitos de información estimulan una mayor cooperación entre los agentes públicos y privados. No obstante, como en otros ámbitos, estas relaciones conllevan numerosas ventajas y contrapartidas. Se requiere tiempo para cultivarlas y es posible que no se parta de una confianza plena. Para garantizar que los nuevos requisitos de información que surjan a nivel nacional y regional cumplan su objetivo de resiliencia, los Estados deben colaborar con la industria y otros actores pertinentes a fin de mejorar la comprensión mutua de:

- el lugar que ocupan los sistemas de cables submarinos en el ecosistema de las TIC;
- las estructuras de incentivos y rendición de cuentas que pueden ayudar a superar los actuales déficits de confianza y otros obstáculos al intercambio de datos, y los posibles modelos de intercambio de información seguro y fiable inspirados en las mejores prácticas existentes en otros entornos sensibles;
- los cambios en las arquitecturas de los sistemas de cables submarinos de telecomunicaciones y equipos vinculados;
- las vulnerabilidades de la cadena de suministros;
- las tendencias de los fallos y alteraciones de los sistemas de cables submarinos, para poder identificar posibles incidentes de alto riesgo y baja probabilidad que tengan repercusiones en la seguridad nacional o internacional y en la estabilidad del sistema financiero mundial, y con el fin de aclarar las funciones y responsabilidades en tales casos; y finalmente
- los enfoques de la industria en lo que respecta a la gestión y mitigación de los riesgos de los sistemas de cables submarinos y los avances tecnológicos y de otro tipo que contribuyen a proteger y reforzar la resiliencia de estos sistemas.

¹³³ Christian Bueger and Tobias Liebetrau (2021), "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network", *Contemporary Security Policy* 42:3, p. 402.

Una agenda política amplia y basada en principios

La seguridad y resiliencia de los sistemas de cables submarinos suscitan preocupaciones legítimas. Sin embargo, sobredimensionar el debate político sobre los cables submarinos puede resultar problemático. Por un lado, la actual trayectoria política podría fracturar aún más la Internet global y obstaculizar la innovación y la competencia, cuyas consecuencias a largo plazo pueden superar con creces los beneficios de un sistema más resiliente e interconectado. Además, se corre el riesgo de desvincular el diseño y la ejecución de proyectos de infraestructuras digitales muy necesarios en los países en vías de desarrollo de principios clave como la transparencia, la sostenibilidad y la rendición de cuentas. Con añadidura, existe el riesgo de desvincularlos de objetivos fundamentales centrados en el ser humano, como garantizar que las poblaciones desatendidas históricamente puedan beneficiarse de los dividendos sociales y económicos de una mayor conectividad, según el espíritu del Objetivo de Desarrollo Sostenible 9¹³⁴. En este sentido, al tiempo que mantienen una postura fuertemente orientada a la seguridad y la resiliencia, los Estados también deben garantizar:

- un equilibrio adecuado en la forma de abordar la cuestión de los cables submarinos en las agendas políticas nacionales, regionales e internacionales;
- un debate más integrador sobre las contrapartidas sociales, económicas y medioambientales que pueden derivarse de las decisiones de trazado, financiación e inversión de los cables motivadas por la seguridad nacional;
- una intensificación de las consultas a los agentes pertinentes en lo que respecta al diseño y la ejecución de proyectos de infraestructuras de cables submarinos, como los que se prevén actualmente en el marco de diferentes iniciativas de desarrollo e infraestructuras¹³⁵; y
- una mayor transparencia con respecto a la aplicación de principios ampliamente aceptados como la sostenibilidad y la responsabilidad en tales iniciativas.

¹³⁴ C. Kavanagh (forthcoming), "The Ties that Bind...", paper prepared for the annual SubCom conference in Bangkok.

¹³⁵ US Blue Dot Network, <https://www.dfc.gov/our-work/blue-dot-network>; China's Belt and Road Initiative (see <https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative>) and related Digital Silk Road and Global Development Initiatives (see https://csis-website-prod.s3.amazonaws.com/s3fs-public/event/220912_Global_Development_Initiative.pdf); EU Global Gateway Strategy, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en; G7 Partnership for Global Infrastructure Development, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment/>; U.S.--E.U. Joint Statement of the Trade and Technology Council', 05 December 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/>.

Conclusiones

Cada vez hay una mayor conciencia de que los cables submarinos de telecomunicaciones son un elemento crítico del ecosistema mundial de las TIC, dado que transmiten la práctica totalidad de nuestras telecomunicaciones y datos. Su seguridad y resiliencia son fundamentales para el bienestar y el funcionamiento de las sociedades de todo el mundo. También se reconoce que los Estados de todas las regiones albergan preocupaciones legítimas con respecto a la seguridad de estos cables, especialmente en el entorno actual de escalada de las tensiones geopolíticas. En consecuencia, la situación actual exige un enfoque más global y cooperativo para reforzar la resiliencia de los sistemas. Este informe pone en relieve algunas de las lagunas del actual régimen de gobernanza de los cables, al tiempo que arroja luz sobre otras prácticas y medidas recomendadas que pueden contribuir a su protección y resiliencia. Las recomendaciones recogidas en este documento se dirigen principalmente a los Estados, aunque reconoce la importancia y constante contribución de la industria y otros agentes a tales esfuerzos. Estas sugerencias apuntan a que todos los Estados consideren los cables submarinos de telecomunicaciones como infraestructuras críticas y colaboren con los agentes de la industria para comprender los esfuerzos que ya se están realizando para mejorar la resiliencia y establecer medios fiables y seguros para compartir información. Asimismo, destacan la necesidad de adoptar un enfoque más amplio y basado en principios para contemplar los cables submarinos en las políticas a fin de evitar el riesgo de introducir en la agenda un excesivo hincapié en la seguridad. El objetivo no es evitar ni criticar los enfoques actuales para proteger y asegurar los sistemas de cables submarinos a nivel nacional o regional, sino garantizar que todos los Estados y regiones contribuyan de forma responsable a garantizar un ecosistema de TIC más seguro y resiliente.

Anexo 1

Disposiciones de la CNUDM relativas a los cables submarinos

Artículo 3. Anchura del mar territorial.	Todo Estado tiene derecho a establecer la anchura de su mar territorial hasta un límite que no exceda de 12 millas marinas medidas a partir de líneas de base determinadas de conformidad con esta Convención.
Artículo 21. Leyes y reglamentos del Estado ribereño relativos al paso inocente	1. El Estado ribereño podrá dictar, de conformidad con las disposiciones de esta Convención y otras normas de derecho internacional, leyes y reglamentos relativos al paso inocente por el mar territorial, sobre todas o algunas de las siguientes materias: ... c) La protección de cables y tuberías;
Artículo 33. Zona contigua.	1. En una zona contigua a su mar territorial, designada con el nombre de zona contigua, el Estado ribereño podrá tomar las medidas de fiscalización necesarias para: a) prevenir las infracciones de sus leyes y reglamentos aduaneros, fiscales, de inmigración o sanitarios que se cometan en su territorio o en su mar territorial; b) Sancionar las infracciones de esas leyes y reglamentos cometidas en su territorio o en su mar territorial. 2. La zona contigua no podrá extenderse más allá de 24 millas marinas contadas desde las líneas de base a partir de las cuales se mide la anchura del mar territorial.
Artículo 57. Anchura de la zona económica exclusiva.	La zona económica exclusiva no se extenderá más allá de 200 millas marinas contadas desde las líneas de base a partir de las cuales se mide la anchura del mar territorial.
Artículo 58. Derechos y deberes de otros Estados en la zona económica exclusiva.	1. En la zona económica exclusiva, todos los Estados, sean ribereños o sin litoral, gozan, con sujeción a las disposiciones pertinentes de esta Convención, de las libertades de navegación y sobrevuelo y de tendido de cables y tuberías submarinos a que se refiere el artículo 87, y de otros usos del mar internacionalmente legítimos relacionados con dichas libertades, tales como los vinculados a la operación de buques, aeronaves y cables y tuberías submarinos, y que sean compatibles con las demás disposiciones de esta Convención. 2. Los artículos 88 a 115 y otras normas pertinentes de derecho internacional se aplicarán a la zona económica exclusiva en la medida en que no sean incompatibles con esta Parte. 3. En el ejercicio de sus derechos y en el cumplimiento de sus deberes en la zona económica exclusiva en virtud de esta Convención, los Estados tendrán debidamente en cuenta los derechos y deberes del Estado ribereño y cumplirán las leyes y reglamentos dictados por el Estado ribereño de conformidad con las disposiciones de esta Convención y otras normas de derecho internacional en la medida en que no sean incompatibles con esta Parte.
Artículo 79. Cables y tuberías submarinos en la plataforma continental.	1. Todos los Estados tienen derecho a tender en la plataforma continental cables y tuberías submarinos, de conformidad con las disposiciones de este artículo. 2. El Estado ribereño, a reserva de su derecho a tomar medidas razonables para la exploración de la plataforma continental, la explotación de sus recursos naturales y la prevención, reducción y control de la contaminación causada por tuberías, no podrá impedir el tendido o la conservación de tales cables o tuberías. 3. El trazado de la línea para el tendido de tales tuberías en la plataforma continental estará sujeto al consentimiento del Estado ribereño. 4. Ninguna de las disposiciones de esta Parte afectará al derecho del Estado ribereño a establecer condiciones para la entrada de cables o tuberías en su territorio o en su mar territorial, ni a su jurisdicción sobre los cables y tuberías construidos o utilizados en relación con la exploración de su plataforma continental, la explotación de los recursos de ésta o las operaciones de islas artificiales, instalaciones y estructuras bajo su jurisdicción. 5. Cuando tiendan cables o tuberías submarinos, los Estados tendrán debidamente en cuenta los cables o tuberías ya instalados. En particular, no se entorpecerá la posibilidad de reparar los cables o tuberías existentes.
Artículo 86. Aplicación de las disposiciones de esta Parte.	Las disposiciones de esta Parte se aplican a todas las partes del mar no incluidas en la zona económica exclusiva, en el mar territorial o en las aguas interiores de un Estado, ni en las aguas archipelágicas de un Estado archipelágico. Este artículo no implica limitación alguna de las libertades de que gozan todos los Estados en la zona económica exclusiva de conformidad con el artículo 58.
Artículo 87. Libertad de la alta mar.	1. La alta mar está abierta a todos los Estados, sean ribereños o sin litoral. La libertad de la alta mar se ejercerá en las condiciones fijadas por esta Convención y por las otras normas de derecho internacional. Comprenderá, entre otras, para los Estados ribereños y los Estados sin litoral: a) La libertad de navegación; b) La libertad de sobrevuelo;

- c) La libertad de tender cables y tuberías submarinos, con sujeción a las disposiciones de la Parte VI;
 - d) Libertad de construir islas artificiales y otras instalaciones permitidas por el derecho internacional, con sujeción a las disposiciones de la Parte VI;
 - e) La libertad de pesca, con sujeción a las condiciones establecidas en la sección 2;
 - f) La libertad de investigación científica, con sujeción a las disposiciones de las Partes VI y XIII;
2. Estas libertades serán ejercidas por todos los Estados teniendo debidamente en cuenta los intereses de otros Estados en su ejercicio de la libertad de la alta mar, así como los derechos previstos en esta Convención con respecto a las actividades en la Zona.

**Artículo 112.
Derecho a tender cables y tuberías submarinos.**

1. Todos los Estados tienen derecho a tender cables y tuberías submarinos en el lecho de la alta mar más allá de la plataforma continental.
2. El párrafo 5 del artículo 79 se aplicará a tales cables y tuberías.

**Artículo 113.
Ruptura o deterioro de cables o tuberías submarinos.**

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. Esta disposición se aplicará también en el caso de actos que tengan por objeto causar tales rupturas o deterioros o que puedan tener ese efecto. Sin embargo, esta disposición no se aplicará a las rupturas ni a los deterioros cuyos autores sólo hayan tenido el propósito legítimo de proteger sus vidas o la seguridad de sus buques, después de haber tomado todas las precauciones necesarias para evitar la ruptura o el deterioro.

**Artículo 114.
Ruptura o deterioro de cables o tuberías submarinos causados por los propietarios de otros cables o tuberías submarinos.**

Todo Estado dictará las leyes y reglamentos necesarios para que las personas sometidas a su jurisdicción que sean propietarias de cables o tuberías en la alta mar y que, al tender o reparar los cables o tuberías, causen la ruptura o el deterioro de otro cable o de otra tubería respondan del costo de su reparación.

**Artículo 115.
Indemnización por pérdidas causadas al tratar de prevenir daños a cables o tuberías submarinos.**

Todo Estado dictará las leyes y reglamentos necesarios para que los propietarios de buques que puedan probar que han sacrificado un ancla, una red o cualquier otro aparejo de pesca para no causar daños a un cable o a una tubería submarinos sean indemnizados por el propietario del cable o de la tubería, a condición de que hayan tomado previamente todas las medidas de precaución razonables.

**Artículo 297.
Limitaciones a la aplicabilidad de la sección 2.**

1. Las controversias relativas a la interpretación o la aplicación de esta Convención con respecto al ejercicio por parte de un Estado ribereño de sus derechos soberanos o su jurisdicción previstos en esta Convención se someterán a los procedimientos establecidos en la sección 2 en los casos siguientes:
 - a) Cuando se alegue que un Estado ribereño ha actuado en contravención de lo dispuesto en esta Convención respecto de las libertades y los derechos de navegación, sobrevuelo o tendido de cables y tuberías submarinos o respecto de cualesquiera otros usos del mar internacionalmente legítimos especificados en el artículo 58[.]