LA PROTECCIÓN DE LOS CABLES SUBMARINOS DE TELECOMUNICACIONES: SOBERANÍAS DIGITALES Y SEGURIDAD DE LA RED DE CABLE SUBMARINA*

THE PROTECTION OF SUBMARINE TELECOMMUNICATIONS CABLES: DIGITAL SOVEREIGNTY AND SUBMARINE CABLE NETWORK SECURITY

Noelia Arjona Hernández
Centro Universitario San Isidoro adscrito a la Universidad Pablo de Olavide, Sevilla, España
noeliarjonahdez@gmail.com

Recibido: septiembre de 2023
Aceptado: octubre de 2023

Palabras clave: cables submarinos, infraestructura crítica, seguridad nacional, soberanía digital
Keywords: submarine cables. critical infrastructure, national security, digital sovereignity

Resumen: El sabotaje de los gasoductos Nord Stream en octubre de 2022 ha magnificado la vulnerabilidad y la importancia crítica de la infraestructura submarina. También ha puesto de manifiesto la falta de comprensión sobre cómo funcionan las redes submarinas, cómo se regulan, quién las controla y cómo se protegen. El conflicto en Ucrania ha amplificado las tensiones en este contexto en términos de la creciente amenaza de actividad de guerra híbrida/zona gris. Este artículo analizará el contexto y los organismos que intervienen en la gobernanza de los cables submarinos e identificará las lagunas de esta protección, incidiendo en la actuación de actores cable como la Unión Europea y otras iniciativas en el marco de la Ruta de la Seda China.

Abstract: The sabotage of the Nord Stream pipelines in October 2022 has magnified the vulnerability and critical importance of subsea infrastructure. It has also highlighted the lack of understanding of how subsea networks work, how they are regulated, who controls them and how they are protected. The conflict in Ukraine has amplified tensions in this context in terms of the growing threat of hybrid warfare/grey zone activity. This article will analyse the context and bodies involved in the governance of submarine cables and identify gaps in

this protection, with a focus on the actions of cable actors such as the European Union and other initiatives within the framework of China's Silk Road.

1. Introducción

Los cables submarinos comerciales de telecomunicaciones transportan alrededor del 99% de las comunicaciones digitales transoceánicas, incluidas las comunicaciones internacionales de voz, datos e Internet, y las transacciones financieras. Empresas privadas individuales y consorcios de empresas poseen y operan una red de más de 500 cables submarinos comerciales de telecomunicaciones que forman la columna vertebral de la Internet mundial, proporcionando servicios de telecomunicaciones e Internet a consumidores, empresas y organismos gubernamentales, incluidos organismos militares, de seguridad nacional y diplomáticos (Gallagher y Carter, 2023: 1).

Casi 1,4 millones de kilómetros de fibra metálica atraviesan los océanos del mundo, acelerando el tráfico de Internet en todo el planeta. La mayor velocidad y ancho de banda de los datos 5G y la comunicación constante con grandes volúmenes de dispositivos del Internet de las Cosas (IoT) harán que fluyan aún más datos por el cable submarino.

Dada la importancia de los cables submarinos comerciales para transportar 5-6G y tráfico de datos de Internet, la seguridad de los cables submarinos y los datos que transportan, así como el papel de los gobiernos en la protección de estos activos de propiedad privada (Gallagher, 2022: 2), son una cuestión acuciante y más aún, tras los recientes sabotajes contra infraestructuras submarinas, como los gasoductos Nord Stream en el mar Báltico y varios cables submarinos de telecomunicaciones en Europa. Estos acontecimientos han aumentado la concienciación sobre la importancia de las infraestructuras submarinas y han estimulado los llamamientos a una mayor protección de los cables submarinos.

En junio de 2022, el Parlamento Europeo publicó un informe en el que se describían los esfuerzos realizados por varios países de la Unión Europea (UE) para reforzar la protección de los cables, y se pedía una mayor concienciación sobre la importancia de los cables y el intercambio de información, así como una actualización de la estrategia marítima de la UE para proteger los cables y reforzar la resistencia de la red (Bueger, Liebetrau y Franken, 2022: 1-68). Unos meses antes de los ataques a los gasoductos Nord Stream, en enero de 2022, uno de los dos cables de Svalbard[1] perdió señal debido a una interrupción en el suministro eléctrico submarino. En enero de 2023, el Instituto Noruego de Asuntos Internacionales declaró que, aunque se especulaba con la posibilidad de un sabotaje por parte de Rusia, el sabotaje humano no ha sido probado, ni tampoco ninguna conexión entre los ataques a los gasoductos Nord Stream y este cable (Schia, Gjesvik, Rødningen, 2023: 2). El instituto hizo un llamamiento para aumentar las redundancias y la

1 La estación terrestre de satélites de Svalbard (conocida como SvalSat). SvalSat descarga datos de satélites en órbita polar y los transmite por cable submarino a diversos clientes, entre ellos la Administración Nacional de Aeronáutica y del Espacio (NASA) y la Administración Nacional Oceánica y Atmosférica (NOAA).

protección de las redes de comunicación para garantizar la continuidad de las comunicaciones en caso de daños. Según algunos informes, la reparación del cable cortado de Svalbard costará 5,6 millones de euros (unos 6 millones de dólares) y estará plenamente operativo en 2024, lo que equivale a años de datos científicos perdidos (Kirk, 2022).

En abril de 2023, la pregunta de una eurodiputada para respuesta escrita por el Parlamento Europeo en virtud del artículo 138 del Reglamento interno del Parlamento Europeo, concentraba con claridad varias problemáticas. Por una parte, y según los informes, la eurodiputada resaltó la cuestión de que los cables de telecomunicaciones submarinos transatlánticos, capaces de velocidades de transferencia de 4,7 petabits por segundo, no serán suficientes para satisfacer la demanda de ancho de banda de 2030 de 13,1 petabits por segundo. Se necesitarían 17 nuevos cables, lo que supondría una inversión de 4 250 millones de euros. Los gigantes estadounidenses de Internet, que poseen el 80% de la capacidad de los cables submarinos transatlánticos, podrían asegurar estas inversiones futuras. En este sentido, la interpelación es rotunda: ¿Cómo planea la Comisión promover la soberanía digital europea? En segundo lugar, recordó que la infraestructura de cable es parte del proyecto Digital Silk Road de China y que el Departamento de Justicia de EE.UU. ya expresó su preocupación de que Pekijo podría usar su nueva ley de seguridad nacional para acceder a los datos por cable en el lado de Hong Kong. En el contexto de su estrategia de seguridad marítima (11205/14 de 24 de junio de 2014), plantea la eurodiputada cómo garantizará la Comisión la seguridad de la red de cable submarino, en particular con respecto a ciertos territorios de ultramar o bases militares (Bilde, 2023).

En junio de 2023, la Organización del Tratado del Atlántico Norte (OTAN) acordó crear el Centro Marítimo para la Seguridad de las Infraestructuras Submarinas Críticas para, entre otras cosas, compartir las mejores prácticas para la protección de los cables y facilitar el intercambio de información entre las naciones de la OTAN (OTAN, 2023).

En julio de 2023, la European Union Agency for Cybersecurity (ENISA) elaboró un informe titulado Subsea cables-What is at stake? validado por las autoridades nacionales responsables de la seguridad de las telecomunicaciones en la UE (ENISA, 2023: 1-34).

La reciente cumbre entre la UE y América Latina y el Caribe es un momento importante, pero como ha destacado el Alto representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, Borrell, no es el principio ni el final. En muchos frentes, la pelota ya está en movimiento. Ya se ha cooperado en la ampliación del cable BELLA, el Centro de Ciberseguridad de Latinoamérica y el Caribe en Santo Domingo y la creación de dos centros regionales Copernicus para la reducción del riesgo de catástrofes, el cambio climático y la vigilancia terrestre y marina (Borrell, 2023).

En la Cumbre del G20 de 2023 celebrada en Nueva Delhi (India), el Presidente Biden y el Primer Ministro Modi copresidieron un grupo de líderes del G20 para acelerar las inversiones destinadas a ampliar los proyectos de infraestructuras de alta calidad y el desarrollo de corredores económicos a través de la Asociación para la Infraestructura y la Inversión Mundiales (PGI) (The White House, 2023).

Este artículo esbozará la práctica estatal para reforzar la protección de los cables submarinos que aterrizan en los estados, fortificar la red de telecomunicaciones y apoyar la continuidad de las comunicaciones, con el fin de salvaguardar la economía y la seguridad nacional. A nivel nacional, ¿Qué autoridad debe tener competencias para supervisar los cables submarinos y recibir informes de incidentes relacionados con ellos? ¿Qué aportan las estrategias nacionales de ciberseguridad? ¿Cómo ha cambiado la situación de la protección de la infraestructura marítima en esta nueva era de seguridad asociada con una agenda de seguridad marítima, la geopolítica y la autonomía de las estrategias, la guerra híbrida y las tácticas de la llamada zona gris? (Bueger, 2023) ¿A qué estados pertenecen las empresas que han dominado el suministro y la instalación de estos cables?

La metodología utilizada para la elaboración de este artículo ha sido fundamentalmente el apoyo en la práctica estatal e internacional, aunando investigación documental, en la que se hizo balance de la bibliografía pertinente sobre el tema, entrevistas específicas con las partes interesadas del sector del cable y consolidación y análisis de la información recogida.

2. Infraestructura Marítima Crítica

El derecho digital no es un tema científico nuevo. Son múltiples las publicaciones que ya se ocupan de determinados sectores económicos: blockchain y plataformas, o de cuestiones más generales: soberanía digital, ciberseguridad, digitalización del Estado, emergencia de un derecho internacional de Internet, etc. Sin embargo, los enfoques existentes, que ya son numerosos y ricos, revelan dos lagunas relativas (Maurel, 2023: 1).

Por una parte, la cuestión de las infraestructuras digitales sigue planteándose más fácilmente desde el ángulo de la geopolítica que del derecho. Los grandes manuales y obras de referencia sobre derecho digital suelen eludir el tema. Sin embargo, se trata de una cuestión de gran envergadura económica, políticamente sensible y ecológicamente ineludible; como lo demuestran los intentos de los Estados por atraer inversores susceptibles de establecer cables submarinos o centros de datos competitivos en materia de energía en su territorio y las inversiones de los propios Estados en este sentido, o los litigios en torno a Starlink, que probablemente se multiplicarán a la vista de los numerosos proyectos de la empresa (Maurel, 2023: 2).

Por lo general, los estudios jurídicos se han centrado, y siguen centrándose, en el derecho de las actividades digitales, descuidando a veces los problemas jurídicos planteados por sus infraestructuras físicas. Las cuestiones infraestructurales son, además, eminentemente públicas, en la medida en que están en juego los regímenes administrativos nacionales de autorización de establecimiento y mantenimiento de estructuras digitales como los cables submarinos, regímenes que varían de un Estado a otro, dependiendo, por ejemplo, de si una operación económica relacionada con el sector digital se clasifica como inversión estratégica (Maurel, 2023: 3).

Definir la "Infraestructura Marítima Crítica" es una tarea difícil. Diferentes actores entienden la infraestructura marítima

crítica de diferentes maneras, desde un enfoque amplio que engloba la protección de toda la infraestructura con un elemento marítimo (como los puertos), hasta una definición técnicamente más estrecha que se centra en un pequeño número de infraestructuras críticas seleccionadas (como cables de datos submarinos) donde cualquier nivel de interrupción crearía fallas en todo el sistema (McCabe, Flynn, 2023: 2-3).

La ley portuguesa de infraestructuras críticas adoptada en 2022 proporciona el marco legal para identificar, designar, proteger y aumentar la resiliencia de las infraestructuras críticas, consolidando en la legislación nacional la transposición de la Directiva 2008/114/CE del Consejo.

El Tratado de Alta Mar adoptado por consenso el pasado 19 de junio durante la reunión de las Naciones Unidas en Nueva York, también conocido como "BBNJ" (biodiversidad más allá de las jurisdicciones nacionales), utiliza el concepto de tecnología marina, señalando su artículo 1(10) que la tecnología Marina incluye, entre otras cosas, información y datos, facilitados en un formato fácil de usar, sobre ciencias marinas y operaciones y servicios marinos relacionados; manuales, directrices, criterios, normas y materiales de referencia; equipos de muestreo y metodología; instalaciones y equipos de observación para observaciones in situ y de laboratorio, análisis y experimentación; ordenadores y programas informáticos, incluidos modelos y técnicas de modelización; biotecnología relacionada; y experiencia, conocimientos, competencias, conocimientos técnicos, científicos y jurídicos y métodos analíticos relacionados con la conservación y el uso sostenible de la diversidad biológica marina.

El Proceso abierto de consultas oficiosas de las Naciones Unidas sobre los océanos y el derecho del mar en su vigesimotercera reunión (5 - 9 de junio de 2023) dedicó uno de sus paneles a las Nuevas tecnologías marítimas (United Nations Open-ended Informal Consultative Process (ICP) on Oceans and the Law of the Sea, 2023: 1-20). Dentro de estas "Nuevas tecnologías marítimas" se puso el acento sobre los cables SMART. En este sentido, se espera que la integración de sensores medioambientales en los cables submarinos de telecomunicaciones, conocidos como cables SMART, impulse la vigilancia de los océanos y la alerta temprana de tsunamis y terremotos para reducir el riesgo de catástrofes. Del mismo modo, se espera que un sistema piloto de cable SMART esté operativo frente a las costas de Portugal en 2025 (ICP, 2023: 3). Se recomendó la educación del Comité Internacional de Protección de Cables (ICPC) a través del Proceso Consultivo Informal de las Naciones Unidas (ICPC, 2023). La Convención Marco de las Naciones Unidas sobre el Cambio Climático ha señalado la necesidad de seguir reforzando las observaciones sistemáticas sostenidas del océano y de colmar las lagunas con nuevas técnicas de observación oceánica que se están desarrollando o empleando para vigilar el océano y comprender mejor los impactos del cambio climático (ICP 2023: 3,5). Dado que la zona más afectada por las catástrofes naturales de origen oceánico es Asia-Pacífico, que también alberga el mayor número de cables submarinos de telecomunicaciones que atraviesan el planeta, es esencial que el testigo del cambio político lo encabecen las naciones de Asia, es decir, China, Japón, ASEAN e India. Es discutible si eso llegará a ver la luz del día. Sin embargo, en el presen-

te inmediato, necesitamos desarrollar la tecnología necesaria para generar fe y resultados para que estas naciones creen la necesidad de modificar las normas de uso de dichos cables de doble uso.

El pasado 9 de septiembre, Úrsula von der Leyen hizo un balance de los dos años del lanzamiento del Partnership for Global Infrastructure and Investment (PGII) en el marco de la Cumbre del G20. El PGII representa una visión conjunta de las principales economías del mundo para invertir en la infraestructura que necesitan los países de ingresos bajos y medios. Dos años después, más proyectos a gran escala están viendo la luz. En este sentido, la presidenta de la Comisión se refiere al corredor económico India-Oriente Medio-Europa, haciendo hincapié en los cables submarinos de datos como infraestructura global. Este corredor será la conexión más directa hasta la fecha entre la India, el Golfo Arábigo y Europa: con un cable de datos de alta velocidad para vincular algunos de los ecosistemas digitales más innovadores del mundo y crear oportunidades de negocio a lo largo del camino. Este corredor es mucho más que un ferrocarril o un cable, es un puente verde y digital a través de continentes y civilizaciones (von der Leyen, 2023).

2.1. Tecnologías de cable submarino y red mundial

TeleGeography calcula que hay 552 sistemas comerciales de cables submarinos de telecomunicaciones planificados y activos en todo el mundo (nacionales e internacionales) (TeleGeography, 2023), que conectan todos los continentes excepto la Antártida (International Trade Administration, 2022). Los cables submarinos de telecomunicaciones nacionales van de punto a punto dentro de un país. Pueden mejorar la conectividad entre regiones dentro de un país, proporcionar conectividad a la Internet mundial y conectar el continente con islas cercanas; algunos cables nacionales cruzan aguas internacionales cuando conectan dos puntos nacionales. Los cables submarinos de telecomunicaciones internacionales conectan dos o más países y permiten la conexión entre los países y, a veces, con otros países a lo largo de la ruta (Gallagher y Carter, 2023: 3).

Señala el reciente informe elaborado por la ENISA que los cables submarinos son fundamentales para la UE y protegerlos de ataques físicos y cibernéticos tiene una importancia estratégica (ENISA, 2023: 4).

El artículo 7 de la Directiva sobre seguridad de las redes y sistemas de información (Directiva NIS2) pide a los EM que adopten políticas, como parte de sus estrategias nacionales de ciberseguridad relacionadas con el mantenimiento de la disponibilidad general, la integridad y la confidencialidad del núcleo público de la Internet abierta, incluida, en su caso, la ciberseguridad de los cables de comunicaciones submarinos. El Código Europeo de Comunicaciones Electrónicas (Code EECC) como la Directiva NIS2 adoptan un enfoque que abarca todos los riesgos, lo que significa que incluyen los ciberataques, pero también los ataques físicos a los sistemas de red y de información, incluidos, por ejemplo, los daños no intencionados a los cables por el transporte marítimo, o los ataques de sabotaje. Los ataques físicos a infraestructuras críticas en general están cubiertos por la Directiva sobre Entidades Críticas.

La reunión informal del Consejo de Ministros de Telecomunicaciones, celebrada en Nevers el 9 de marzo de 2022, dio lugar a un llamamiento conjunto para reforzar las capacidades de ciberseguridad de la UE. En su punto 4 se reconoció que las infraestructuras críticas, como las redes de telecomunicaciones y los servicios digitales, son de suma importancia para muchas funciones críticas de nuestras sociedades y, por lo tanto, constituyen un objetivo primordial de los ciberataques. Los cables submarinos entran el ámbito de aplicación del citado punto 4 (ENISA, 2023: 7).

La ley portuguesa sobre infraestructuras críticas adoptada en 2022 establece el marco jurídico para identificar, designar, proteger y aumentar la resiliencia de las infraestructuras críticas, consolidando en la legislación nacional la transposición de la Directiva 2008/114/CE del Consejo. El sector de las telecomunicaciones entra en el ámbito de aplicación de esta legislación y, aunque la clasificación de las infraestructuras críticas nacionales está actualmente en curso, los cables submarinos podrían entrar en el ámbito de aplicación de esta clasificación (ENISA, 2023: 8).

El Comité Internacional para la Protección de los Cables pretende concienciar a los gobiernos y a otros usuarios de los fondos marinos de que los cables submarinos son infraestructuras críticas.

2.1.1. Propiedad

Los cables submarinos comerciales pueden ser propiedad de una sola empresa o de un consorcio de empresas. Los propietarios de los cables son proveedores de telecomunicaciones, empresas de cable submarino, proveedores de contenidos (por ejemplo, Facebook) y proveedores de servicios de computación en nube (por ejemplo, Google, Microsoft, Amazon). Los propietarios están invirtiendo en nuevos cables submarinos de telecomunicaciones para: aumentar la capacidad para satisfacer el aumento previsto de la demanda de datos móviles, servicios de Internet y servicios en la nube; ampliar la cobertura para dar servicio a nuevas regiones y clientes; y, generar nuevos ingresos. Por lo tanto, esta infraestructura de comunicaciones crítica de la que dependen los consumidores, las empresas y los gobiernos para la conexión y la comunicación diarias es propiedad y está expandida principalmente por empresas del sector privado.

No obstante, algunos gobiernos han invertido en cables. Por ejemplo, el sistema de cable submarino Tonga-Fiji es propiedad y está gestionado por Tonga Cable Limited (TCL), que desarrolló y gestiona el cable con el apoyo financiero del Banco Asiático de Desarrollo y el Banco Mundial. TCL es una empresa pública propiedad del gobierno en un 80%. En China, tres empresas estatales del país - China Mobile, China Telecom y China Unicom - invirtieron en cables submarinos. En Estados Unidos, la Marina estadounidense posee más de 40.000 millas náuticas de diversos cables submarinos (Gallagher y Carter, 2023: 4).

2.1.2. Naturaleza transjurisdiccional de los cables

Los cables submarinos comerciales internacionales cruzan fronteras internacionales y aterrizan en dos o más estados soberanos. Los cables nacionales se conectan a jurisdicciones dentro del mismo país,

a veces cruzando aguas internacionales para conectar puntos de aterrizaje nacionales. La mayoría de los cables cruzan múltiples jurisdicciones (por ejemplo, internacional, nacional, estatal, local).

El alcance geográfico de la jurisdicción sobre los cables submarinos internacionales de telecomunicaciones se basa generalmente en acuerdos internacionales. Estos incluyen, entre otros, el Convenio Internacional para la Protección de los Cables Telegráficos Submarinos de 1884 y la Convención de las Naciones Unidas sobre el Derecho del Mar (CNUDM). La CNUDM establece las fronteras nacionales de las naciones partes, que se extienden hasta 12 millas náuticas desde la línea de base de la costa de la nación, e incluyen la Zona Económica Exclusiva (ZEE), que se extiende hasta 200 millas náuticas desde la línea de base[2]. La CNUDM concede a todas las naciones la libertad de tender y explotar cables submarinos bajo la Alta Mar y en la Plataforma Continental, dentro de la ZEE de una nación costera, con sujeción a los derechos de una nación costera a adoptar medidas razonables para la exploración de la Plataforma Continental, la explotación de sus recursos naturales y la prevención, reducción y control de la contaminación procedente de los conductos (CNUDM, Artículo 79). Así pues, los segmentos comerciales de cable submarino de telecomunicaciones que cruzan los Mares Territoriales de los estados, sus territorios y posesiones están sujetos a la supervisión y regulación del gobierno del Estado.

2 Según la CNUDM, "la línea de base normal para medir la anchura del mar territorial es la línea de bajamar a lo largo de la costa, tal como aparece marcada en las cartas a gran escala oficialmente reconocidas por el Estado ribereño". CNUDM, Artículos 3, 5 y 57.

2.1.2.1. Práctica estatal

a. Estados Unidos

Los cables submarinos comerciales de telecomunicaciones suelen cruzar también jurisdicciones estatales y locales. De conformidad con la federal Submerged Lands Acts de 1953 (SLA, 43 U.S.C. §1301 et seq.), los estados ribereños tienen derecho, por lo general, a una zona que se extiende tres millas geográficas desde su costa oficialmente reconocida (o línea de base) (43 U.S.C. §1301(b))[3]. Para dar cabida a las reclamaciones de determinados Estados, la SLA prevé una ampliación de la frontera en el Golfo de México si un Estado puede demostrar que dicha frontera estaba prevista por la constitución o las leyes del Estado antes o en el momento en que dicho Estado se convirtió en miembro de la Unión, o si ha sido aprobada anteriormente por el Congreso (43 U.S.C. §§1301(b), 1312)[4].

A tenor de la SLA, dentro de sus fronteras mar adentro, los estados ribereños tienen la titularidad y propiedad de las tierras situadas bajo las aguas navegables dentro de los límites de los respectivos Estados, y el derecho y la potestad de gestionar, administrar, arrendar, desarrollar y utilizar dichas tierras y recursos naturales (43 U.S.C. §1311, CRS, 2023 : 6).

3 Una milla geográfica o náutica equivale a 6.080,20 pies, a diferencia de una milla terrestre, que equivale a 5.280 pies.

4 Tras la promulgación de la SLA, el Tribunal Supremo sostuvo que los límites de la costa del Golfo de Florida y Texas se extienden hasta tres leguas marinas, o nueve millas náuticas; otros estados de la costa del Golfo no consiguieron ampliar sus límites (U.S. contra Luisiana, 363 U.S. 1, 66 (1960); U.S. contra Florida, 363 U.S. 121, 129 (1960)).

La circunstancia de atravesar múltiples jurisdicciones, incluidas áreas locales, estatales, federales e internacionales, constituye uno de los retos de la protección de los cables submarinos (Gallagher y Carter, 2023: 12). Cada jurisdicción puede tener leyes, políticas y procesos de revisión diferentes para los cables submarinos de telecomunicaciones. El Grupo de Trabajo 4A del Communications Security, Reliability, and Interoperability Council (CSRIC) estudió los retos jurisdiccionales. El grupo de trabajo llegó a la conclusión de que, mientras que el gobierno federal conserva el poder de regular el comercio, la navegación, la generación de energía, la defensa nacional y los asuntos internacionales en sus Mares Territoriales, los estados y territorios de EE.UU. conservan la autoridad dentro de sus Mares Territoriales para gestionar, desarrollar y arrendar recursos, incluidos los arrendamientos submarinos para cables submarinos (CSRIC V WG4A, 2016: 5). El grupo de trabajo llegó a la conclusión de que el conjunto de normativas federales y estatales y de requisitos tribales puede crear un complejo conjunto de procesos y requisitos para llevar a cabo o hacer un seguimiento de una propuesta de proyecto (CSRIC V WG4A, 2016: 5-6.). Además, cada jurisdicción puede imponer requisitos diferentes que podrían reforzar o debilitar la protección de los cables frente a los daños.

A modo de ejemplo, el grupo de trabajo señaló que Florida prohíbe el aterrizaje de cables en los Cayos, lo que podría conducir al trazado y agrupamiento de cables a lo largo de ciertas rutas, lejos de dichas zonas protegidas (CSRIC V WG4A, 2016: 6). California y Oregón tienen, como condición para su arrendamiento submarino, políticas en vigor para volver a inspeccionar los cables con el fin de garantizar que han permanecido enterrados, para proteger los cables de daños físicos (CSRIC V WG 4ª, 2016: 33). Por lo tanto, las políticas varían según la jurisdicción, y podrían conducir a diferentes niveles de protección para los cables submarinos que aterrizan en Estados Unidos (Gallagher y Carter, 2023: 12).

En el caso de los puntos de aterrizaje de Estados Unidos en los que se solapan las jurisdicciones, el Equipo Analytic Exchange Program (AEP) afirma que puede haber una fuerte dependencia del sector privado para garantizar la seguridad de los cables, ya que las jurisdicciones pueden tener la suposición errónea de que otros organismos están colaborando con el sector privado en cuestiones de seguridad (AEP, 2017: 15).

Un reto de supervisión en las políticas de protección de cables derivado de su naturaleza transversal es el interés y el compromiso de múltiples agencias y comités del Congreso. Los cables están relacionados con el medio ambiente, los asuntos exteriores, la seguridad nacional, el comercio, el ejército y otras cuestiones, y pueden entrar dentro de las responsabilidades e intereses de múltiples agencias federales, que están autorizadas, dotadas y supervisadas por varios comités del Congreso. Por ejemplo, en un informe del Senado que acompaña a la Ley de Autorización de la Defensa Nacional para el año fiscal 2024, el Comité reconoció que las instalaciones militares dependen de infraestructuras críticas (por ejemplo, energía, agua, telecomunicaciones) no controladas por el Departamento de Defensa (DOD). El Comité escribió que apreciaba la creación por parte del DOD de un Centro de Análisis de Infraestructuras Críticas Densas (CIDAC) durante el año fiscal 2023,

que debe participar en el intercambio de información sobre amenazas y vulnerabilidades con los propietarios privados de infraestructuras críticas (Gallagher y Carter, 2023: 12). El interés transversal de los cables puede complicar la elaboración de propuestas federales de protección global. Por ejemplo, las políticas de separación espacial de los cables (por ejemplo, exigir distancias de separación entre los cables y otras infraestructuras marinas) podrían afectar a la ubicación de otras infraestructuras marinas, como los parques eólicos marinos, que es una prioridad de la Administración Biden. Otra complicación a la hora de lograr un planteamiento global pueden ser los diferentes enfoques, intereses y preocupaciones de los gobiernos estatales y locales que albergan lugares de desembarco de cables. Por ejemplo, las políticas federales para proteger los puntos de desembarco de cables (por ejemplo, la soldadura de las tapas de las alcantarillas) podrían estar prohibidas o ser diferentes de las políticas adoptadas por los gobiernos estatales y locales (Gallagher y Carter, 2023: 12).

Las entidades federales con funciones en los cables de telecomunicaciones comerciales submarinos en Estados Unidos participan en la concesión o revisión de permisos limitándose al ámbito jurisdiccional de sus autoridades y a las leyes específicas que son responsables de aplicar. La revisión de un organismo puede centrarse en determinados segmentos de cables submarinos comerciales de telecomunicaciones (por ejemplo, segmentos que atraviesan un parque nacional) o en determinados aspectos de un proyecto de cable (por ejemplo, propiedad extranjera). Dada la distinta ubicación de los cables submarinos comerciales de telecomunicaciones y de los propietarios y operadores implicados, los organismos y entidades que pueden tener que revisar un proyecto de cable también variarán. Los diputados preguntaron a los organismos federales sobre su papel a la hora de garantizar la seguridad de los cables submarinos de telecomunicaciones (U.S. Congress, Subcommittee on National Security, 2019: 116-43), reconociendo los retos que plantea el número de departamentos y organismos implicados, sus jurisdicciones superpuestas y sus mandatos individuales.

Tanto los grupos de trabajo del CSRIC como los autores del informe AEP han reconocido que las políticas y normas varían según las jurisdicciones y recomiendan la cooperación público-privada para desarrollar y promover la adopción de las mejores prácticas, políticas y normas para proteger el aterrizaje de cables en Estados Unidos (CSRIC IV WG8, 2014: 8-9). El Grupo de Trabajo 4A del CSRIC señalaba a este respecto que en otras partes del mundo, los cables submarinos y otras infraestructuras marinas coexisten bastante bien en estrecha proximidad debido a una relación de trabajo bien establecida entre las industrias, así como la aplicación de las recomendaciones y directrices establecidas de la industria, tales como las del Comité Internacional de Protección de Cables y la Asociación Europea de Cables Submarinos (anteriormente Subsea Cables UK) (CSRIC V WG4A, 9).

Tanto los grupos de trabajo del CSRIC como los autores del informe de la AEP señalaron que existían políticas y estándares de la industria para proteger los cables y alentaron a la industria a adoptar las mejores prácticas. El equipo de AEP declaró que los proveedores de servicios y los clientes deben asegurarse de llevar

a cabo la debida diligencia con las diversas partes involucradas en la colocación, mantenimiento y reparación del cable submarino, ya que las mejores prácticas de seguridad no están estandarizadas en toda la industria, ni en los Estados Unidos ni a nivel internacional (AEP, 2017: 17). Estas incluyen las ICPC's 2022 Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables (ICPC, 2022). El Comité recomienda acciones que los gobiernos pueden tomar para fomentar el despliegue y la protección de cables de telecomunicaciones submarinos y mantener la continuidad de las comunicaciones en caso de daños. Los grupos de trabajo del CSRIC instan al gobierno de EE. UU. a reconocer los estándares de la industria y las mejores prácticas para proteger los cables, y a fomentar el uso de estos estándares y mejores prácticas en los Estados Unidos y en todo el mundo (Gallagher y Carter, 2023: 28).

El Servicio de Investigación del Congreso estadounidense es partidario de que en los casos en que la Comisión Federal de Comunicaciones (FCC) remita solicitudes de cable al Comité, el Comité puede imponer requisitos para proteger físicamente el cable y la estación de aterrizaje del cable contra ataques o daños, requisitos de ciberseguridad y requisitos de presentación de informes. La FCC puede reiterar algunos de esos requisitos en su acuerdo de licencia (por ejemplo, ubicación de infraestructura específica, documentación de interconexión del sistema, derechos de acceso, equipos utilizados en el sistema de cable) para reducir el riesgo de daño físico a los cables (Congressional Research Service, 2022: 4). Por tanto, algunos cables que aterrizan en los Estados Unidos son examinados en busca de riesgos físicos y de seguridad, pero no todas las solicitudes se remiten o revisan con tanto detalle, sólo aquellas que representan un riesgo para la seguridad nacional de los Estados Unidos. De este modo, los cables que aterrizan en los Estados Unidos pueden tener diferentes requisitos de seguridad y niveles de protección.

El Congreso podría ordenar a una agencia o grupo de trabajo interinstitucional, en consulta con la industria, que evalúe los riesgos, desarrolle estándares y mejores prácticas, y exija o aliente a los propietarios del sector privado a adoptar ciertas políticas de protección[5] (Gallagher y Carter, 2023: 29).

El Grupo de Trabajo 4A del CSRIC ha señalado que a concentración de cables puede generar "puntos de estrangulamiento" y aumentar el riesgo de que un solo ataque, accidente o peligro natural pueda afectar a múltiples proveedores de telecomunicaciones simultáneamente, interrumpiendo o degradando potencialmente las comunicaciones de muchos usuarios, incluidos los usuarios gubernamentales, aumentando los riesgos para la seguridad nacional (CSRIC V WG4A, 2016: 11). En su Final Report-Clustering of Cables and Cable Landings de 2016, el grupo de trabajo CSRIC recomendó la cooperación interinstitucional e interjurisdiccional para promover la diversificación de las rutas de cables de telecomunicaciones submarinos, aumentar la redundancia y evitar el aterrizaje de cables en solo unas pocas áreas de Estados Unidos. Las compañías de cable pueden diseñar

5 Como ejemplo, la Administración de Seguridad del Transporte (TSA), a través de un enfoque de colaboración público-privada, desarrolló una guía para propietarios y operadores de oleoductos para mejorar la seguridad de los oleoductos.

sus sistemas de cable para garantizar que cada nodo de la red (es decir, cada punto de conexión) se conecte a al menos otros dos nodos de la red, ofreciendo oportunidades para redirigir el tráfico cuando sea necesario e implementar acuerdos con otros propietarios de cable para transferir tráfico entre redes durante cortes (Gallagher y Carter, 2023: 32).

Se dice que este enfoque ha mejorado la resiliencia global de la red comercial de telecomunicaciones submarinas, aunque persisten las vulnerabilidades. Por ejemplo, la interrupción del servicio debido a la interrupción del cable en Svalbard se evitó debido a que el tráfico se desvió a un cable paralelo (Rainbow, 2022), mientras que la interrupción del servicio en Tonga interrumpió el servicio durante cinco semanas debido a una falta de redundancia de la red. Pero puede haber vulnerabilidades locales debido a la agrupación geográfica incluso cuando hay redundancia de red: el ataque deliberado frente a la costa sur de Francia afectó a tres sistemas de cables submarinos e interrumpió y degradó el servicio durante varias horas (Zscaler, 2022).

El ICPC señala que los operadores diseñan rutas teniendo en cuenta las redundancias, pero también señala que los operadores diseñan rutas para seguir la ruta viable más corta entre los puntos de aterrizaje que presenten el menor costo y riesgo para el cable, ajustando los factores técnicos, económicos y regulatorios, según lo consideren necesario (ICPC, 2022: 7). A lo largo de los años, el ICPC ha recopilado información sobre 2464 averías y reparaciones de cables, que abarcan 126 jurisdicciones ribereñas, utilizando datos de 12 acuerdos de mantenimiento de cables (ENISA, 2023: 18). El Comité Recomienda que los gobiernos adopten e implementen marcos regulatorios para optimizar las rutas y los aterrizajes, y garantizar que las rutas y los aterrizajes sean geográficamente diversos. El Servicio de Investigación del Congreso estadounidense es partidario de que si el Congreso está interesado en aumentar la diversidad geográfica de los sitios de aterrizaje de telecomunicaciones submarinas comerciales en los Estados Unidos para mejorar la resiliencia y la redundancia de la red, puede considerar asignar a una agencia federal la responsabilidad de realizar una evaluación de riesgos para identificar las áreas más vulnerables o las telecomunicaciones submarinas más vulnerables. También puede considerar si una agencia o agencias deberían apoyar el desarrollo de planes de resiliencia de cables de telecomunicaciones submarinos para garantizar la continuidad de las comunicaciones (Gallagher y Carter, 2023: 33).

No sólo se están produciendo rápidamente avances tecnológicos, sino que los actores adversarios disponen cada vez más de equipos avanzados para operaciones submarinas. La conciencia y la acción insuficientes respecto de las vulnerabilidades persistentes de esta infraestructura representan una amenaza significativa para la seguridad nacional y los intereses comerciales.

b. Unión Europea

Por lo que respecta a la UE, la red de cables de datos submarinos es presentada por el informe solicitado por el Parlamento Europeo (y finalmente emitido en junio de 2022) sobre las Security threats to undersea communications cables and infrastructure-consequences for the EU como la principal infraestructura crítica de la era digital (Bueger, Liebetrau y Franken,

2022: 12). Las autoridades nacionales de la UE tienen la responsabilidad de supervisar las redes públicas de comunicaciones y la infraestructura básica de Internet, en virtud del Código Europeo de Comunicaciones Electrónicas (EECC) y la Directiva sobre seguridad de las redes y sistemas de información (Directiva NIS2). Los Estados miembros de la UE han incorporado el EECC a sus legislaciones nacionales, y en cada país hay autoridades nacionales que supervisan a los operadores de redes y servicios públicos de comunicación para garantizar que adoptan las medidas de seguridad adecuadas y notifican los incidentes con repercusiones importantes.

En virtud del EECC (Artículo 40(3)), las autoridades nacionales envían anualmente informes resumidos sobre estos incidentes significativos a ENISA y a la Comisión Europea. En los últimos años, las autoridades nacionales han notificado a ENISA 12 incidentes con cables submarinos, todos ellos involuntarios, accidentales. Sin embargo, debido a su carácter transfronterizo, que a menudo se extiende por aguas internacionales, no siempre está claro quién tiene el mandato de supervisión de los cables submarinos (ENISA, 2023: 6). Además, muchos incidentes con cables submarinos no alcanzan el umbral de notificación, porque los cables submarinos suelen ser redundantes, lo que significa que un incidente con un solo cable no suele causar una interrupción importante. La Estrategia de Seguridad Marítima actualizada de la UE también incluye acciones para proteger las infraestructuras marítimas críticas, incluidas las comunicaciones submarinas, incluidas las ciberamenazas y los ataques físicos (ENISA, 2023: 6).

La protección del cable es un tema de creciente preocupación en los debates públicos y en las estrategias de seguridad nacional en países como Francia, Portugal e Irlanda.

En Francia, la Secretaría General de Defensa y Seguridad Nacional, una organización interministerial dependiente del Primer Ministro de Francia, desempeña un papel importante a la hora de garantizar y coordinar la perspectiva de seguridad nacional de la protección de cables submarinos. La Secrétariat général de la mer coordina todas las tareas administrativas relacionadas con la protección de los cables submarinos. Además, la Armada francesa desempeña un papel importante en la protección de las instalaciones de cables en aguas francesas en colaboración con empresas privadas. Empresas como Orange Marine y Alcatel Subsea Network, líderes mundiales en el tendido y mantenimiento de cables submarinos, realizan ellos mismos controles periódicos para detectar y localizar posibles fallos. Otras autoridades públicas francesas también tienen mandatos en materia de protección de cables submarinos, como la Agencia Nacional de Ciberseguridad francesa (ANSSI), el Estado Mayor Conjunto de Defensa francés, el Ministerio para Europa y de Asuntos Exteriores y la Dirección General de Seguridad Exterior del Ministerio de Defensa (ENISA, 2023: 6).

En Portugal, varias entidades son responsables de la supervisión de los cables submarinos, incluida la Autoridade Nacional de Comunicações - ANACOM. Las diferentes entidades involucradas se coordinan entre sí.

ANACOM ha desarrollado medidas de protección para mitigar los riesgos de se-

guridad de los cables submarinos y facilitar sus reparaciones. ANACOM se centra en tres áreas:

- Un portal electrónico para facilitar la concesión de licencias (ventanilla única) para obtener permisos para instalar, mantener o reparar cables submarinos.
- Un sistema integrado de detección ambiental y sísmica mediante SMART Cables (detección húmeda),
- Investigación de varios métodos de detección en seco (SoP, Phase Detección, DAS).
- Próximamente se pondrá en marcha un servicio de protección y supervisión de cables submarinos (ENISA, 2023: 8). Una entidad pública nacional certificada producirá avisos y alertas a los buques que se encuentren cerca de rutas de cables submarinos dentro de la Zona Económica Exclusiva portuguesa. Este será un servicio público gratuito, disponible las 24 horas del día (ENISA, 2023: 8).

La ley portuguesa de infraestructuras críticas adoptada en 2022 proporciona el marco legal para identificar, designar, proteger y aumentar la resiliencia de las infraestructuras críticas, consolidando en la legislación nacional la transposición de la Directiva 2008/114/CE del Consejo. El sector de las telecomunicaciones está dentro del ámbito de esta legislación y, aunque la clasificación de infraestructuras críticas nacionales está actualmente en curso, los cables submarinos podrían entrar en el ámbito de esta clasificación (ENISA, 2023: 9).

En otros estados, la conciencia gubernamental es bastante limitada. Los estados han propuesto diferentes modelos de cómo gobiernan los cables. En países como Francia y Portugal, la seguridad de los cables es una cuestión clave para las fuerzas navales. Otros, como Malta, dependen de sistemas de gobernanza bajo liderazgo civil. Sin embargo, en otros, como Dinamarca, la gobernanza de los cables está liderada por la industria. El hecho de que los cables a menudo crucen diferentes mandatos, responsabilidades y jurisdicciones plantea un importante desafío de gobernanza transeuropea. De este modo, el informe resalta la exigencia de un diálogo dentro de la UE sobre las mejores prácticas que rigen y protegen los cables a nivel estatal (ENISA, 2023: 9).

Aunque la CNUDM ofrece reglas claras para la jurisdicción y la formación de zonas marítimas, existen áreas de reclamos contrapuestos. La mayor parte de los cables submarinos se encuentran en Alta Mar, donde casi no existe protección legal –aparte del artículo 113-115 de la CNUDM–. Sin embargo, los estados pueden ejercer más privilegios regulatorios respecto de los cables submarinos dentro de sus Mares Territoriales y Zonas Económicas Exclusivas. Si la jurisdicción sobre los cables submarinos no está clara, las medidas regulatorias competitivas o las acciones militares pueden amenazar su seguridad. Las únicas zonas marítimas en disputa que preocupan en la UE que contienen sistemas de cables son el Mar Egeo (Grecia versus Turquía) y el Mar Levantino (Grecia y Chipre versus Turquía). Aunque los reclamos territoriales están motivados principalmente por derechos de extracción de petróleo y gas, los sistemas de cable como MedNautilus y el proyecto BlueMed cruzan estas zonas en disputa y podrían estar sujetos a diferentes percepciones de la jurisdicción estatal

entre los miembros y no miembros de la UE (ENISA, 2023: 23).

Por otro lado, el informe se limita a recordar que desde un punto de vista legal, los estados no tienen jurisdicción sobre cables fuera del Mar Territorial y la Zona Contigua. En Alta Mar, así como en las ZEE, el estatuto jurídico de los cables y los derechos y la responsabilidad de su protección es ambiguo (ENISA, 2023: 27).

Al mismo tiempo, el informe advierte que los fallos en los cables que pueden afectar la conectividad de la UE pueden ocurrir en jurisdicciones de estados no miembros de la UE, en particular el Reino Unido, Egipto y otros estados de la región MENA[6], África occidental o América del Sur. Ante esta situación lo ideal sería que un mecanismo de notificación fuera más allá de los estados miembros de la UE. La UE podría pedir al Servicio Europeo de Acción Exterior (EEAS) que considere si se pueden desarrollar marcos a nivel bilateral o regional (por ejemplo, para el Mediterráneo y el Atlántico Sur) y cómo hacerlo (ENISA, 2023: 52). En este sentido, el Gobierno irlandés, a través de su membresía en la Asociación para la Paz (PfP) liderada por la OTAN, está considerando profundamente la participación en la Célula de Coordinación de Infraestructura Submarina Crítica de la OTAN, así como en proyectos PESCO relevantes de la UE (Leahy, 2023; Phelan, 2023). La Célula de Coordinación de Infraestructura Submarina Crítica facilitará el compromiso con la industria y reunirá a partes interesadas militares y civiles clave para compartir mejores prácticas, aprovechar tecnologías innovadoras e impulsar la seguridad de la infraestructura submarina (OTAN, 2023). Fundamentalmente, al tratarse de una iniciativa de la OTAN, el Reino Unido es por defecto un actor importante, mientras que Irlanda sólo tiene un acuerdo de asociación básico con la alianza. Esto ilustra cómo la superposición de membresías en la UE y la OTAN se está volviendo importante pero también problemática (McCabe y Flynn, 2023: 11).

3. Propiedad multinacional y sector privado

Como ya se ha señalado, los cables submarinos de telecomunicaciones son principalmente de propiedad privada, ya sea de un único propietario o de un consorcio de propietarios de cables. Los propietarios privados diseñan y operan los cables pensando en la protección (por ejemplo, enterrando los cables, fortificando las estaciones de aterrizaje). Suelen ser capaces de redirigir el tráfico a rutas alternativas en caso de fallo del cable e informan de que han experimentado pocos cortes de comunicación prolongados por daños en los cables (Gallagher y Carter, 2023: 11). A diferencia de los buques, los cables submarinos no están bajo la bandera de un solo Estado y, por tanto, la propiedad legal se divide entre varios copropietarios, lo que da lugar a un caleidoscopio jurídico de jurisdicciones y nacionalidades (Burnett, 2021: 1668). Esto también significa que no existe ningún requisito gubernamental estatutario para restablecer el tráfico si un cable resulta dañado o interrumpido (Burnett, 2021: 1665).

Se ha reconocido que la base jurídica para que los Estados ribereños protejan los cables submarinos tendidos en zonas situadas fuera de su soberanía es discutible (Liao, 2019: 457). Dentro del Mar Terri-

6 Middle East and North Africa.

torial, el título de un Estado ribereño para regular y proteger los cables submarinos reside en su soberanía (jurisdicción territorial) (O´Connell, 1984: 820). La CNUDM establece que un Estado ribereño podrá adoptar leyes y reglamentos relativos al paso inocente a través del Mar Territorial, con respecto a la protección de cables y tuberías y que podrá además establecer condiciones para los cables o tuberías que entren en su territorio o Mar Territorial (artículos 21(1)(c) y 79(4) CNUDM).

Los derechos y responsabilidades de un Estado ribereño en el ejercicio de su jurisdicción no están del todo claros. La CNUDM contiene disposiciones jurisdiccionales permisivas que, por ejemplo, no imponen la obligación de proteger los cables en el Mar Territorial. No obstante, y a pesar de la probabilidad de que dichos cables sean propiedad privada de entidades extranjeras, los Estados ribereños tienen un claro interés nacional en ejercer esta jurisdicción para proteger los cables. Sin embargo, en ausencia de un deber positivo de protección, será difícil atribuir la responsabilidad de los daños al Estado ribereño. La jurisdicción territorial, sólo se extiende hasta el límite de las 12 millas. Por poner sólo algunos ejemplos, la mayor parte del cable Australia-Japón, de 12.700 km, o del cable de telecomunicaciones Pacific-Crossing 1, de 21.000 km, que une Japón y EE.UU., o de cualquiera de los cables de 7.000 km entre EE.UU. y el Reino Unido, queda claramente fuera de la jurisdicción nacional (Guilfoyle, Paige, McLaughlin, 2022: 662).

Fuera del Mar Territorial, los esfuerzos normativos se han centrado en la atribución de responsabilidad por daños a los cables, centrándose en el Estado del pabellón del buque infractor, en lugar de atribuir la jurisdicción a un Estado ribereño o a un usuario de cables (Kaye, 2010:189). Esta posición no ha cambiado sustancialmente con la ampliación histórica de los derechos de los Estados ribereños sobre la Plataforma Continental después de 1945 y a través de la Zona Económica Exclusiva a partir de la década de 1970. El primer instrumento internacional pertinente fue el anterior Convenio de París de 1884 para la protección de los cables telegráficos submarinos. El artículo 2 tipifica como delito punible romper o dañar un cable submarino, deliberadamente o por negligencia culpable, de manera que pueda interrumpir u obstruir la comunicación telegráfica, total o parcialmente, sin perjuicio de cualquier acción civil por daños y perjuicios.

El Convenio establece la jurisdicción del Estado del pabellón sobre tales delitos y, con carácter subsidiario, el enjuiciamiento por el Estado de la nacionalidad del delincuente. El Convenio excluye del ámbito de aplicación de este delito los casos en los que los daños a un cable se deban a personas que actúen con el objeto legítimo de salvar sus vidas o su buque, y los actos realizados de conformidad con el derecho de la guerra, cuando sea aplicable (artículo. 15 Convenio de París). El artículo 10 establece una facultad poco frecuente de visita en Alta Mar por parte de buques de guerra extranjeros para recabar pruebas en virtud del Convenio cuando los oficiales al mando de buques de guerra, [u otros buques comisionados] tengan razones para creer que una infracción de la presente Convención ha sido cometida por un buque que no sea buque de guerra, podrán exigir del capitán o patrón la presentación de los documentos oficiales que prueben la nacionalidad de dicho buque. Además, dichos funciona-

rios podrán preparar declaraciones formales de los hechos, cualquiera que sea la nacionalidad del buque incriminado.

Al menos se produjo una inspección de este tipo cuando, en 1959, un buque de guerra estadounidense que investigaba una rotura en un cable del Atlántico frente a Terranova abordó el arrastrero soviético Novorossiisk y registró sus documentos (Guilfoyle, Paige, McLaughlin, 2022: 663). Sin embargo, el Convenio de París sólo prevé la visita en Alta Mar, no la detención ni siquiera la búsqueda (O´Connell, 1984: 821). Su utilidad práctica se ve dificultada por su bajo nivel de ratificación, ya que sólo cuenta con 36 partes (National Oceanic and Atmospheric Administration, 2019).

No obstante, algunas de sus disposiciones se transpusieron a la Convención de Ginebra sobre Alta Mar de 1958 (63 partes) y a la CNUDM (168 partes). El artículo 27 de la Convención de Alta Mar y el artículo 113 de la CNUDM estipulan que todo Estado adoptará las leyes y reglamentos necesarios para disponer que la rotura o lesión por un buque que enarbole su pabellón o por una persona sujeta a su jurisdicción de un cable submarino situado en Alta Mar, realizada deliberadamente o por negligencia grave, de forma que pueda interrumpir u obstruir las comunicaciones telegráficas o telefónicas constituirá un delito punible.

Sin embargo, el artículo 113 sólo prevé una competencia prescriptiva. La acción contra un nacional en virtud de dicha ley tendría que esperar a su regreso a su propia jurisdicción; y aunque un buque de las fuerzas del orden podría emprender acciones de ejecución contra un buque mercante que enarbole el mismo pabellón en Alta Mar y que sea sospechoso de tal delito, tal caso es muy improbable (basándose como se hace en la proximidad aleatoria de los dos buques co-nacionales) (Guilfoyle, Paige, McLaughlin, 2022: 663-664).

No hay equivalente a la disposición del Convenio de París sobre los poderes de visita en la CNUDM. La disposición sobre el ejercicio de la jurisdicción del Estado del pabellón y la jurisdicción sobre la conducta de los nacionales en relación con actos ocurridos en Alta Mar se aplica igualmente en la Zona Económica Exclusiva de terceros Estados en virtud del artículo 58(2) de la CNUDM.

El marco jurídico establecido por el artículo 113 tiene dos consecuencias notables. En primer lugar, no existe una obligación equivalente para los Estados ribereños de adoptar dicha legislación nacional en las zonas sujetas a su soberanía territorial o a sus derechos soberanos (Liao, 2019: 461). En segundo lugar, no es evidente que los Estados ribereños estén facultados para ejercer una jurisdicción prescriptiva o coercitiva dentro de la ZEE o en la superficie de sus Plataformas Continentales (fuera del Mar Territorial) sobre los cables de telecomunicaciones (Kaye, 2010: 190). De hecho, dado que el tendido de dichos cables en la ZEE no se trata como un derecho del Estado ribereño, sino como una libertad de Alta Mar perteneciente a terceros Estados, se establece una posible relación de competencia (Liao, 2019: 462) el ya citado apartado 2 del artículo 79.

No obstante, la doctrina ha señalado la creciente propensión de los Estados a prescribir zonas de protección de cables dentro de sus ZEE en las que se prohíben determinadas actividades (Guilfoyle, Paige, McLaughlin, 2022: 664). La Comi-

sión de Derecho Internacional examinó una propuesta de zonas de protección de este tipo en torno a oleoductos submarinos en el marco de sus trabajos sobre el derecho del mar en 1956 y fue rechazada por el Relator Especial JPA François por considerar que constituiría una nueva injerencia en la libertad de navegación y de pesca que, por consiguiente, no está justificado (International Law Commission, 1956: 12).

Si bien se ha afirmado que la base jurídica de tales zonas en áreas situadas fuera del Mar Territorial es cuestionable (Liao, 2019: 465), mucho depende del alcance preciso de tales zonas y de los poderes que los Estados ribereños ejerzan dentro de ellas (Guilfoyle, Paige, McLaughlin, 2022: 664). Por ejemplo, dentro de la ZEE, un Estado ribereño tiene la facultad general de imponer "términos y condiciones" relativos a la pesca en la ZEE que los nacionales extranjeros "deberán cumplir", incluidas, entre otras, las condiciones de concesión de licencias, las restricciones de los artes de pesca y las medidas de ejecución (artículo 62(4) CNUDM)[7].

En cuanto a la práctica estatal en este sentido, Nueva Zelanda cuenta con un régimen legal adaptado en virtud del cual se han declarado numerosas zonas de protección de cables, pero que sólo pueden aplicarse a los buques con pabellón neozelandés, a los nacionales neozelandeses (incluso cuando operan en un buque extranjero) o dentro del Mar Territorial (Kaye, 2010: 200; Guilfoyle, Paige, McLaughlin, 2022: 665; Submarine Cables and Pipelines Protection Act 1996 (New Zealand) sections 4, 12–13). La protección es responsabilidad de los propietarios de los cables, pero también cuenta con el apoyo de funcionarios de protección designados por el gobierno y la policía marítima (New Zealand Ministry of Transport). Así pues, el gobierno neozelandés crea zonas de protección, ayuda a los propietarios y operadores privados de cables mediante la supervisión y el nombramiento de personas (oficiales de protección) encargadas de vigilar la seguridad y hacer cumplir las leyes de protección, e impone multas y sanciones a los infractores. Nueva Zelanda también se dedica a la educación, integrando su información sobre las zonas de protección de cables en las orientaciones marítimas, el material educativo y los sitios web gubernamentales que proporcionan información sobre las zonas protegidas, las actividades prohibidas y las sanciones.

Por su parte, el régimen australiano de zonas de protección de cables establecido en virtud de la Ley de Telecomunicaciones de 1997 puede prohibir o restringir una serie de actividades pesqueras y otras actividades económicas dentro de dichas zonas (todas las cuales entran dentro de la autoridad de un Estado ribereño sobre su ZEE) (Telecommunications Act 1997 (Australia), Schedule 3A, cl. 10–11).

La legislación australiana contempla una serie de delitos adicionales por dañar negligente o deliberadamente un cable submarino dentro de una zona de protección declarada. Tal y como ponen de manifiesto Guilfoyle, Paige, McLaughlin trayendo a colación a Kaye, el hecho de que estos últimos delitos sean aplicables *prima facie* contra ciudadanos y buques extranjeros ha sido calificado de cuestionable desde el punto de vista del derecho internacional(Kaye, 2010:199-200). No obstante, cabe destacar que la

7 Este artículo enumera los poderes de reglamentación en una lista larga pero no exhaustiva.

Ley de Telecomunicaciones de 1997 parece contemplar la aplicación únicamente mediante una orden de restricción o una sanción civil, y dichos procedimientos contra ciudadanos y buques extranjeros requieren además el consentimiento del Fiscal General de la Commonwealth (Telecommunications Act 1997 (Australia) sections 317ZC and 317ZE.) Así pues, no se plantea la cuestión de la aplicación en el mar más allá del Mar Territorial, lo que mitiga la posibilidad de que se considere que la Ley de Telecomunicaciones ejerce una jurisdicción de aplicación exorbitante. El régimen también parece diseñado para garantizar que si Australia adopta medidas en virtud de su legislación que puedan dar lugar a la responsabilidad del Estado, esa decisión debe ser tomada deliberadamente por el Fiscal General (Guilfoyle, Paige, McLaughlin, 2022: 665).

Por lo que respecta a Estados Unidos, el reciente estudio efectuado por el Servicio de Investigación del Congreso, trae a colación el informe de 2016, *Clustering of Cables and Cable Landings* del grupo de trabajo CSRIC, que recomendó que la FCC fomentara el desarrollo de zonas de protección de cables alrededor de los cables submarinos existentes para proteger la infraestructura de comunicaciones de otras actividades marítimas (CSRIC V WG4A, 2016: 12.). Asimismo el Servicio de Investigación del Congreso alude directamente a Australia y Nueva Zelanda (Gallagher y Carter, 2023: 29-30).

Aunque las protecciones limitan las actividades que podrían dañar los cables, también pueden limitar otras actividades productivas en las aguas costeras y crear responsabilidades y costes añadidos para los gobiernos. También pueden dar lugar a la agrupación de cables, lo que podría crear riesgos de seguridad. Su aplicación puede ser un reto en algunas geografías donde hay mucho tráfico marítimo, infraestructuras existentes (por ejemplo, cables eléctricos, parques eólicos) y otras actividades (por ejemplo, la pesca) (Gallagher y Carter, 2023: 31).

Algunos países también han adoptado una *cabotage law*, en virtud de la cual sólo los buques con pabellón local pueden trabajar en aguas territoriales. También hay casos en los que, aunque no sea una disposición de la CNUDM, se solicitan permisos para la instalación o reparación dentro de la Zona Contigua (24 millas náuticas) o dentro de la ZEE (200 millas náuticas), lo que puede dificultar la instalación de cables submarinos al atravesar estas zonas Este es el caso, por ejemplo, de los cables entre Cuba y Guyana, que atraviesan la ZEE de Venezuela, país con estrictos procesos al respecto (ENISA, 2023: 11).

Los propietarios del sector privado tienen un interés económico en proteger los cables de los daños, principalmente para preservar su base de clientes, cuyos pagos por el uso del cable son la principal fuente de sus ingresos (Gallagher y Carter, 2023: 4). Tradicionalmente, la mayoría de los estados europeos han optado por un compromiso político más limitado y enfoques de gobernanza menos sólidos en relación con la seguridad de la infraestructura submarina. Esto se debió en parte a un régimen legal internacional ambiguo, pero también al bajo nivel de amenaza percibido (Bueger y Liebetrau, 2023: 1). Esencialmente, era políticamente más fácil y económicamente viable externalizar la responsabilidad al sector privado para gestionar y mantener la infraestructura submarina, independientemente del nivel de capacidad nacional de seguridad

marítima o de las asociaciones de defensa (McCabe y Flynn, 2023: 2).

4. Implicaciones geopolíticas

El mercado del cable submarino corre el riesgo de dividirse en bloques oriental y occidental por el temor al espionaje y las tensiones geopolíticas (Gross, Heal, Campbell, Clark, Bott, de la Torre Arenas, 2023). Los conflictos futuros involucrarán no solo a los países y las fronteras, sino también al ciberespacio, que es esencialmente un frágil mosaico de cables submarinos y centros de datos. A medida que las principales potencias compiten por el acceso a los centros de datos y los espacios cognitivos, se intensificará un mayor enfoque en la seguridad de los cables submarinos (Tsuchiya, 2023). Los continuos cambios en la geopolítica internacional obligan a los distintos actores a revisar y redefinir sus alianzas estratégicas. Hechos recientes como la pandemia de la COVID-19, la renovada presencia de China en Latinoamérica frente a la pérdida de influencia de Estados Unidos en la región, el Brexit y la invasión de Rusia a Ucrania, son parte de un escenario internacional en permanente evolución (Ríos, 2023: 5).

La creación de AUKUS (2021) reconoce que el mundo se encuentra en pleno siglo marítimo, en el que las rutas marítimas y los cables submarinos representan las líneas de vida físicas y digitales de la prosperidad global. La estabilidad marítima es esencial para el orden internacional, y la guerra de Ucrania ha demostrado lo rápido que ambas pueden convertirse en objetivo de regímenes revisionistas. Ya se trate de cables marítimos en las Shetland o de buques cerealeros saliendo del Mar Negro, la interrupción de los bienes comunes marítimos es una forma de coaccionar a los Estados. Las capacidades subacuáticas, como los submarinos de última generación, representan una poderosa póliza de seguros para prevenir, o mitigar, los riesgos para ambos (Bassi, Ryan, Curtis, 2023).

Agathe Demarais, directora de previsiones globales de The Economist Intelligence Unit, señala que, pese a las crecientes tensiones, el comercio entre EEUU y China sigue creciendo. No obstante, está por ver si será posible mantener esta dinámica, logrando que las restricciones vinculadas a la tecnología estratégica de alta gama no afecten a los sectores normales. El objetivo de EE.UU. de preservar el comercio, pero con más excepciones para la seguridad nacional es difícil de alcanzar (Demarais, 2023).

La Comisión Europea ya promueve las inversiones en infraestructura de cable submarino a través de la estrategia Global Gateway. La estrategia europea para financiar proyectos internacionales en competencia con la iniciativa china Belt and Road, destinó unos 30.000 millones de euros a proyectos de conectividad digital, como cables de fibra óptica submarinos y terrestres, sistemas de comunicación segura basados en el espacio y centros de datos, conectando a la UE con sus socios globales. Por su parte, se espera que China, prepare el terreno para la visita de Putin a Pekín en octubre para participar en el tercer Foro sobre la iniciativa Belt and Road. En julio, hubo un aumento notable en los intentos tanto de Estados Unidos como de China de establecer una relación más estable. Tras la visita del secretario de Estado estadounidense, Antony Blinken, a Beijing a finales de ju-

nio, hubo una serie de visitas posteriores a China de la secretaria del Tesoro, Janet Yellen , el representante especial sobre el clima, John Kerry, y el experto en China, Henry Kissinger (Schochet y Carr, 2023). A pesar de estos encuentros cara a cara, una cosa queda clara: las relaciones seguirán turbulentas en el futuro previsible. En consecuencia, examinar las ventajas estratégicas de cada lado se vuelve crucial. Estos activos potenciales incluyen redes de alianzas, bases en la región del Indo-Pacífico, relaciones comerciales con países y mucho más. En ese contexto, el mayor acceso de China a los cables submarinos marinos y su posible manipulación requieren mayor atención y una estrategia conjunta. Aunque estos cables submarinos son parte integral de las comunicaciones globales, no están exentos de la competencia entre China y Estados Unidos. Como destacó un informe de Reuters de principios de este año, Estados Unidos ha intervenido en seis acuerdos privados de cables submarinos en Asia-Pacífico durante los últimos cuatro años para garantizar que China no gane el contrato (Schochet y Carr, 2023). Estas intervenciones del gobierno estadounidense impidieron que la empresa china HMN Technologies Co Ltd y su consorcio obtuvieran los contratos del proyecto. El predecesor de HMN Tech fue el gigante chino de las telecomunicaciones Huawei Technologies Co Ltd, una empresa que durante mucho tiempo ha sido blanco del escrutinio del gobierno de Estados Unidos. Está claro que Estados Unidos ve estos cables como una amenaza potencial a la seguridad en términos de vulnerabilidad de espionaje y en caso de que estalle un conflicto con China (Schochet y Carr, 2023). Como afirmó James Kraska, profesor de Derecho Marítimo Internacional en la Escuela de Guerra Naval de EE. UU., en una entrevista con MarketPlace, existen reglas mínimas con respecto a los cables submarinos en caso de conflicto (Kraska, 2023).

A pesar de la limitada atención prestada a la importancia de los cables submarinos, Estados Unidos ha iniciado algunas medidas para abordar el asunto, como intentar impedir que China gane contratos para poseer y construir cables submarinos. Además, en menor medida, el Congreso ha tomado conciencia de esta acuciante cuestión. En marzo de 2023, la Cámara de Representantes de Estados Unidos aprobó el proyecto de ley del congresista Brian Mast para proteger la superioridad estadounidense en capacidades de cables submarinos del alcance económico y militar de China. El proyecto de ley de control de cables submarinos exige que la administración Biden desarrolle una estrategia que limite la capacidad de China para acceder a bienes y tecnología que podrían utilizarse en la producción de cables (Schochet y Carr, 2023). Por otro lado, los socios del Quad, India y Australia, intensifican el trabajo en cables submarinos en medio de las incursiones chinas. Una de las primeras reuniones a las que asistió el Ministro de Asuntos Exteriores, S. Jaishankar, después de aterrizar en Nueva York para la 78ª Asamblea General de las Naciones Unidas la semana pasada fue con sus colegas del Quad, seguida de conversaciones bilaterales con su homólogo australiano Penny Wong y el Ministro de Asuntos Exteriores japonés, Yoko Kamikawa. Ambos países también reconocieron la urgente necesidad de apoyar redes de cables submarinos de calidad en el Indo-Pacífico, que son clave para el crecimiento y la prosperidad globales y conllevan un mayor valor del comercio,

a través de transacciones financieras e información, que el valor de los bienes transportados por mar. Fue en la Cumbre de Líderes de Quad 2023 a principios de este año cuando los líderes anunciaron la Asociación Quad para la Conectividad y Resiliencia del Cable, que representa un compromiso compartido con los cables submarinos como una prioridad para la infraestructura regional (Sharma, 2023).

Falta una planificación de resiliencia para un ataque concertado. Es posible que los gobiernos no sepan realmente qué cables se utilizan, quién o para qué. El derecho internacional en este ámbito es confuso, más adecuado al papel periférico que desempeñaron los cables en los años 70 y 80, más que al estatus indispensable que tienen hoy. Tampoco existe un mecanismo internacional para cambiar las prioridades del tráfico crítico si es necesario, ni para priorizar las reparaciones. Esto siempre ha estado en los registros de riesgos de las empresas, pero nadie trabajó en ello porque parecía demasiado remoto. Muchas grandes empresas no saben en detalle qué cables utilizan, para qué servicios y, especialmente, en qué cables confían sus contratistas externos (Ellison, 2023).

Uno de los grandes riesgos en este momento es avanzar hacia redes bifurcadas. ¿Crea esto un sistema en el que no hay conectividad, con una guerra casi fría, entre el bloque del Este y el del Oeste? La experta en política económica exterior de China en el Centro de Análisis Naval, Herlevi, manifiesta que no se ha llegado a ese punto todavía pero le preocupa que esa sea la dirección en la que nos dirigimos (Herlevi, 2023). Mientras tanto, un nuevo análisis muestra que fluyen más datos entre Estados Unidos y China que en cualquier otro momento de la historia, incluso si la ruta entre los dos es a menudo menos directa que antes. Varias personas en la industria señalan que los datos aún pueden ser interceptados incluso si la infraestructura que los transporta no está construida por empresas chinas. Si bien durante la última década el sector fue remodelado por una mayor inversión de empresas tecnológicas estadounidenses, estaba surgiendo una historia paralela. En 2015, el gobierno chino anunció una iniciativa estratégica para invertir enormes cantidades en capacidades de comunicaciones, vigilancia y comercio electrónico de los países en desarrollo a cambio de influencia diplomática. Los cables de Internet fueron clave para esta Ruta de la Seda Digital, que transcurrió en paralelo a la Iniciativa de la Franja y la Ruta de Beijing, que ha inyectado cientos de miles de millones para la construcción de carreteras, ferrocarriles y puertos en todo el mundo en desarrollo (Cheng y Zeng, 2023: 6-9).

5. Conclusiones

Los cables submarinos comerciales son vitales para las comunicaciones (voz, datos, Internet) y las transacciones financieras de todo el mundo. El aumento del uso de datos por parte de consumidores, empresas y organismos gubernamentales ha incrementado la dependencia cotidiana de los cables submarinos. Los daños en los cables podrían interrumpir o degradar las comunicaciones y amenazar la seguridad nacional y los intereses económicos de los Estados. Los recientes incidentes han aumentado la concienciación sobre la importancia de los cables y han estimulado los llamamientos para aumentar su

protección. Los gobiernos podrían examinar las interrupciones de los cables en sus Estados y considerar si es necesaria una mayor protección por parte del gobierno, de los propietarios del sector privado o a través de la coordinación público-privada.

Los proveedores de servicios y los clientes deberían asegurarse de que llevan a cabo la diligencia debida en relación con las distintas partes implicadas en la colocación, mantenimiento y reparación del cable submarino, ya que las mejores prácticas de seguridad no están normalizadas en todo el sector a escala internacional.

La geopolítica cada vez más tensa y la transformación geoeconómica presenta para los estados y la industria desafíos y oportunidades relacionados con los cables submarinos que han pasado a la vanguardia de la discusión y la preocupación a nivel mundial. La industria del cable debe convertirse en un formador de políticas y no en un político en el marco inestimable del ICPC.

Los países deben priorizar la seguridad nacional, la seguridad de los datos y la privacidad mediante la implementación de políticas y marcos regulatorios apropiados que excluyan completamente a los proveedores no confiables de todo el ecosistema de TIC, incluidas las redes inalámbricas, los cables terrestres y submarinos, los satélites, los servicios en la nube y los centros de datos. Es sorprendente que muchos Estados miembros de la UE olviden en gran medida las implicaciones geopolíticas y de seguridad nacional de la red de cable submarino. Además, los Estados europeos rara vez se ocupan del impacto significativo de la infraestructura de cables de datos submarinos en los flujos internacionales de información, la seguridad y la economía. Sin embargo, la creciente conciencia sobre la cuestión de la protección de los cables también indica que existen oportunidades para mejorar la conciencia, los mecanismos de gobernanza y la resiliencia dentro de las estructuras y agencias existentes de los Estados miembros.

Dado que los Estados no parecen haber previsto ni apreciado el carácter crítico de los cables submarinos para sus comunicaciones internacionales, a menudo no existe un organismo líder que coordine políticas eficaces sobre los cables submarinos.

La CNUDM rara vez aborda cuestiones de protección y limita la jurisdicción de los Estados ribereños para mejorar la protección.

A nivel nacional no siempre está claro qué autoridad debe tener competencias para supervisar los cables submarinos y recibir informes de incidentes relacionados con ellos. Es importante que los Estados aclaren a nivel nacional quién tiene la responsabilidad y el mandato para la protección y seguridad de los cables submarinos. También es importante que las autoridades nacionales pertinentes empiecen a intercambiar buenas prácticas sobre la protección de los cables submarinos. Este intercambio de buenas prácticas debería tener en cuenta las buenas prácticas del sector energético sobre la protección y la seguridad de los cables eléctricos submarinos, así como las buenas prácticas de las autoridades responsables de la seguridad física de las infraestructuras críticas.

¿Cómo evalúan los estados la seguridad nacional (por ejemplo, qué características y componentes de un cable submarino se tendrían en cuenta en el contexto de la seguridad nacional) durante la revisión del interés público del organismo especí-

ficamente o en la aplicación de sus autoridades de concesión de permisos de forma más amplia?

Un mayor multilateralismo podría incluir la formación conjunta, el intercambio de inteligencia, el desarrollo tecnológico, el mantenimiento de equipos o, posiblemente, la adquisición conjunta y la puesta en común de activos. Este enfoque también cuenta con el apoyo del ICPC, que recomienda que los estados realicen ejercicios navales y juegos de guerra en los que participe la industria del cable submarino para poner a prueba los protocolos en un entorno internacional (ICPC 2009).

Mientras que los buques de guerra (por ejemplo, los submarinos) y otros buques de Estado destinados a fines no comerciales gozan de inmunidad soberana, los cables submarinos utilizados con fines militares/gubernamentales no comerciales no gozan explícitamente (NATO Cooperative Cyber Defence Centre of Excellence, 2019:5) de inmunidad soberana, sin embargo las disposiciones pertinentes de la CNUDM y otros convenios internacionales relativos a la protección de los cables submarinos se aplican igualmente (Ashley Roach, 2014: 343). ¿Qué aporta la inmunidad soberana a la protección?

6. Bibliografía (selección)

Bassi, J. et al. (2023). "AUKUS Is More Than Submarines: Its Advanced Capabilities Pillar Will Also Require Fundamental Shifts", *Just Security*, https://www.justsecurity.org/87195/aukus-is-more-than-submarines-its-advanced-capabilities-pillar-will-also-require-fundamental-shifts/ (última consulta el 31 de octubre de 2023).

Bilde, D. (2023). "Parliamentary Question for written answer E-001227/2023 to the Commission Rule 138", *European digital sovereignty and undersea cable network security* (*European Parliament*), https://www.europarl.europa.eu/doceo/document/E-9-2023-001227_EN.html#def6 (última consulta el 31 de octubre de 2023).

Borrell, J. (2023). "EU-CELAC Summit: Press remarks by High Representative/Vice-President Josep Borrell upon arrival", *European Union External action*, https://www.eeas.europa.eu/eeas/eu-celac-summit-press-remarks-high-representativevice-president-josep-borrell-upon-arrival_en (última consulta el 31 de octubre de 2023).

Bueger, C. Liebetrau, T. et al. (2022). "Security threats to undersea communications cables and infrastructure - consequences for the EU, In-Depth analysis Requested by the SEDE sub-committee", *Policy Department for External Relations, Directorate-General for External Policies of the Union, PE 702.557*.

Bueger, C., Liebetrau, T. (2023). "Critical maritime infrastructure protection: what's the trouble?", *Marine policy*, vol.155, pp. 1-8.

Burnett, D.R. (2021). "Submarine cable security and international law", *International law studies*, vol. 97, pp. 1659–1682.

Cheng, J., Zeng, J. (2023). "Digital Silk Road" as a Slogan Instead of a Grand Strategy", *Journal of Contemporary China*, pp. 1-17.

Comisión Europea, Parlamento Europeo y Consejo. (2023). *Declaración europea sobre los derechos y principios digitales para la década digital (2023/C 23/01)*, https://digitalstrategy.ec.europa.eu/es/

library/europeandeclaration-digital-rights-and-principles (última consulta el 31 de octubre de 2023).

Consejo de la Unión Europea. (2023). "Declaration of the EU-CELAC Summit", *Consejo Europeo y Consejo de la Unión Europea*, https://ec.europa.eu/commission/presscorner/detail/en/statement_23_3924. 2023 (última consulta el 31 de octubre de 2023).

Congressional Research Service. (2022). "National Security Review Bodies: Legal Context and Comparison", pp. 1-7.

CSRIC V, Working Group 4A, Submarine Cable Resiliency. 2016. *Final Report—Clustering of Cables and Cable Landings*, https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG4A_Report-Intergovernmental-Interjurisdictional-Coordination_June2016.pdf, pp. 1-47 (última consulta el 31 de octubre de 2023).

CSRIC IV, Working Group 8, Submarine Cable Routing and Landing. (2014). *Final Report—Protection of Submarine Cables through Spatial Separation*, pp. 1-59, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf (última consulta el 31 de octubre de 2023).

European Union Agency for Cybersecurity. (2023). "Subsea cables-what is at stake", pp. 1-33.

Demarais, A. (2023). "Despite tensions, US-China trade keeps growing", https://twitter.com/AgatheDemarais/status/1661401671849713664?sma=newsletter_geopolitica (última consulta el 31 de octubre de 2023).

Ellison, C. (2023). en H. Tomás, "Threats to undersea cables should worry business as well as government", *Financial Times*, https://www.ft.com/content/1addaf05-49d9-4172-8eff-eabb2ac01a16 (última consulta el 31 de octubre de 2023).

Gallagher, J.C. et al. (2023). "Protection of Undersea Telecommunication Cables: Issues for Congress", *Congressional Research Service (CRS), Report R47648*, pp. 1-53.

Gallagher, J.C. (2022). "Undersea Telecommunication Cables: Technology Overview and Issues for Congress", *CRS Report R47237*, 2022, pp. 1-22.

Gross, G., Heal et al. (2023). "How the US is pushing China out of the internet´s plumbing", *Financial Times*, https://ig.ft.com/subsea-cables/ (última consulta el 31 de octubre de 2023).

Guilfoyle, D. et al. (2022). "The final frontier of cyberspace: the seabed beyond national jurisdiction and the protection of submarine cables", *International and Comparative Law*, vol. 71, pp. 657-696.

Herlevi, A. (2023). en G. Gross et al., "How the US is pushing China out of the internet's plumbing", *Financial Times*, https://ig.ft.com/subsea-cables/ (última consulta el 31 de octubre de 2023).

ICPC. (2023). "Plenary Highlights", *International Cable Protection Committee 1999 – 2023*, https://www.iscpc.org/events/2023-plenary-meeting/?print (última consulta el 31 de octubre de 2023).

International Trade Administration. (2023). "Chile Telecommunications Subsea Fiber-Optic Cables", *Market Intelligence*, https://www.trade.gov/market-intelligence/chile-telecommunications-subsea-fiber-optic-cables (última consulta el 31 de octubre de 2023).

Kaye, S. (2010). "The Protection of Platforms, Pipelines and Submarine Cables

under Australian and New Zealand Law", en N. Klein, J. Mossop and D. Rothwell (eds.), *Maritime Security: International Law and Policy Perspectives from Australia and New Zealand*. Londres: Routledge, pp. 186-201.

Kirk, L. (2022) "Mysterious Atlantic Cable Cuts Linked to Russian Fishing Vessels," *euobserver*, https://euobserver.com/nordics/156342 (última consulta el 31 de octubre de 2023).

Leahy, P. (2023). "Ireland likely to join NATO project to protect undersea cables", *Irish Times*,https://www.irishtimes.com/politics/2023/05/14/ireland-likely-to-join-nato-project-to-protect-undersea-cables/ (última consulta el 31 de octubre de 2023).

Liao, X. (2019). "Protection of Submarine Cables against Acts of Terrorism", *Ocean Yearbook*, vol. 33, pp. 456-472.

Maurel, R. (2023). *Comparative law of digital infrastructures and activities* (Collective work under the direction of Raphaël Maurel), forcoming.

McCabe, R. Flynn, B. (2023). "Under the radar: Ireland, maritime security capacity, and the

governance of subsea infrastructure", *European Security*, pp. 1-21.

North Atlantic Treaty Organization (NATO). (2023). "Press Conference", https://www.nato.int/cps/en/natohq/opinions_215694.htm selectedLocale=en (última consulta el 31 de octubre de 2023).

O'Connell, D.P. (1984). *The International Law of the Sea. Oxford University Press*, vol 2. Oxford : Clarendon Press.

Phelan, C. (2023). "Ireland to consider joining EU/NATO-led mission to protect undersea cables", *Irish Examiner*, https://www.irishexaminer.com/news/politics/arid-41152948.html (última consulta el 31 de octubre de 2023).

Public-Private Analytic Exchange Program (AEP). (2017). "Threats to Undersea Cable Communications", pp. 4-46, https://www.hsdl.org/?abstract&did=870379 (última consulta el 31 de octubre de 2023).

Rainbow, J. (2022). "Space Norway Plots Recovery Mission for Failed Subsea Cable", *Space News*, https://spacenews.com/space-norway-plots-recovery-mission-for-failed-subsea-cable/ (última consulta el 31 de octubre de 2023).

Ríos, G., Rodriguez E. (2023). "Relaciones América Latina y el Caribe–Unión Europea: fortaleciendo una alianza estratégica", *Banco de Desarrollo de América Latina y el Caribe (CAF)*, pp. 1-59.

Schia, N.N., Gjesvik. L. et al. (2023). "The Subsea Cable Cut at Svalbard January 2022: What Happened", *Norwegian Institute of International Affairs, Policy Brief*, https://www.nupi.no/en/publications/cristin-pub/the-subsea-cable-cut-at-svalbard-january-2022-what-happened-what-were-the-consequences-and-how-were-they-managed (última consulta el 31 de octubre de 2023).

Schochet, N. y Carr, E. (2023). "Navigating China-US Subsea Cable Competition", *The Diplomat*, https://thediplomat.com/2023/08/navigating-china-us-subsea-cable-competition/ (última consulta el 31 de octubre de 2023).

Sharma, A. (2023). "Quad partners India and Australia intensify work on undersea cables amid Chinese inroads", *India Narrative*, https://www.indianarrative.com/world-news/quad-partners-india-and-australia-intensify-work-on-undersea-cables-

amid-chinese-inroads-152267.html (última consulta el 31 de octubre de 2023).

Tsuchiya, M. (2023). "2023 Plenary Highlights", *International Cable Protection Committee 1999 – 2023*, https://www.iscpc.org/events/2023-plenary-meeting/ (última consulta el 31 de octubre de 2023).

United Nations Open-ended Informal Consultative Process on Oceans and the Law of the Sea. (2023). "Advance unedited reporting material on the topic of focus of the twenty-third meeting of the United Nations Open-ended Informal Consultative Process on Oceans and the Law of the Sea", *Twenty-third meeting: "New Maritime Technologies: Challenges and Opportunities" 5 to 9 June 2023*, https://www.un.org/depts/los/consultative_process/icp23/ICP2023AdvanceUneditedReportingMaterial.pdf (última consulta el 31 de octubre de 2023).

U.S. Congress. (2019). House Committee on Armed Services, Subcommittee on Intelligence and Emerging Threats and Capabilities meeting jointly with House Committee on Oversight and Reform, Subcommittee on National Security, *Securing the Nation's Internet Architecture*, 116th Cong., 1st sess., H.A.S.C. No. 116-43.

Von der Leyen, U. (2023). "Statement by President von der Leyen at the Partnership for Global Infrastructure and Investment event in the framework of the G20 Summit", *European Commission*, https://ec.europa.eu/commission/presscorner/detail/en/statement_23_4420 (última consulta el 31 de octubre de 2023).

TeleGeography. (2023). "Submarine Cable Frequently Asked Questions," https://www2.telegeography.com/submarinecable-faqs-frequently-asked-questions (última consulta el 31 de octubre de 2023).

The White House. (2023). "FACT SHEET: President Biden and Prime Minister Modi Host Leaders on the Partnership for Global Infrastructure and Investment", *Memorandum of Understanding on the Principles of an India – Middle East – Europe Economic Corridor (statements and releases)*, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/09/fact-sheet-president-biden-and-prime-minister-modi-host-leaders-on-the-partnership-for-global-infrastructure-and-investment/ (última consulta el 31 de octubre de 2023).

Zscaler. (2022). "European Cable Cut May Impact Transoceanic Routes", https://trust.zscaler.com/zscloud.net/posts/12256 (última consulta el 31 de octubre de 2023).