ieee.es
Instituto Español de Estudios Estratégicos

Documento
Marco

10/2023 20/12/2023

Rafael García Pérez

España en la red global de cables submarinos

España en la red global de cables submarinos

Resumen:

Este artículo estudia la red de cables submarinos de España y su conexión a las redes globales. En particular, es analizada la profunda transformación que actualmente experimenta en España el sector del cable como consecuencia de la conexión con los nuevos sistemas de cables de gran capacidad. También se examinan los efectos que se derivan de estos cambios en la seguridad de la red, dada la creciente competencia geopolítica en la escena internacional. Por último, se pasa revista al tratamiento normativo que reciben en España los cables submarinos, identificando aquellas áreas que deben ser reforzadas.

Palabras clave:

Cables submarinos, seguridad marítima, infraestructuras críticas, centros de datos, competencia geopolítica.

Spain in the global network of submarine cables

Abstract:

This article studies the Spanish submarine fiber-optic cable system and their connection to global networks. Analyzing the profound transformation, the cable sector is currently undergoing in Spain, the linking with the new high-capacity cable systems is underscored as a main driver. Considering the increasing geopolitical competition on the international arena, the effects of these changes on network security are also examined. Last but not least, the article aims at identifying the areas to be reinforced by the governmental further regulation.

Keywords:

Submarine cables, maritime security, critical infrastructures, data centers, geopolitical competition

Cómo citar este documento:

GARCÍA PÉREZ, Rafael. *España en la red global de cables submarinos*. Documento Marco IEEE 10/2023. https://www.ieee.es/Galerias/fichero/docs_marco/2023/DIEEEM10_2023_RAFGAR_Submarinos.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción[1]

La red global de cables submarinos se ha convertido en objeto público de atención estratégica, y de preocupación por su seguridad, desde hace poco tiempo. Fue en octubre de 2020 cuando los ministros de Defensa de los Estados miembros de la OTAN discutieron un «informe completo sobre el estado de nuestra infraestructura crítica»[2] que incluía una relación exhaustiva de estas instalaciones (puertos, aeropuertos, suministros de combustible, alimentos y telecomunicaciones), donde se detallaba la red de cables submarinos transatlánticos con especial relieve. Este protagonismo era debido a la percepción de creciente amenaza que representan las actividades de la flota rusa en este océano[3]. Pero también era una respuesta al control adquirido por empresas extranjeras (específicamente chinas) sobre algunas de esas infraestructuras, de las cuales depende el funcionamiento de nuestras sociedades, al igual que nuestra defensa.

Desde entonces se ha producido una notable actividad investigadora en medios académicos y de análisis estratégico[4], en muchos casos como material clasificado. Y también se han empezado a adoptar algunos documentos de planeamiento estratégico que proponen desarrollar planes de contingencia y una cooperación más estrecha y sistemática entre los socios atlánticos y la propia Unión Europea (UE) sobre ámbito tan sensible. En enero de 2023, la OTAN y la UE crearon un grupo de trabajo conjunto para proteger estas infraestructuras críticas. Y un mes después la OTAN creó una Célula de Coordinación de Infraestructura Submarina Crítica adscrita al Comando Marítimo[5].

Los cables submarinos están perdiendo la «invisibilidad»[6] en la que se encontraban y comienzan a recibir una atención acorde con su extraordinaria relevancia estratégica.

---

[1] Todos los enlaces se encuentran activos a fecha de cierre del presente documento, 13 de noviembre de 2023. Agradezco a Antonio Notario y a Miguel del Cañizo los comentarios que han realizado al borrador de este texto.

[2] OTAN. «Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers». 22 de octubre de 2020. Disponible en: https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

[3] HINCK, G. «Evaluating the Russian Threat to Undersea Cables», *Lawfare*. 5 de marzo de 2018. Disponible en: https://www.lawfaremedia.org/article/evaluating-russian-threat-undersea-cables

[4] BUEGER, Ch., LIEBETRAU, T. y FRANKEN, J. *Security threats to undersea communications cables and infrastructure – consequences for the EU*. European Parliament, Bruselas, 2022. Disponible en: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

[5] OTAN. «NATO stands up undersea infrastructure coordination cell». 15 de febrero de 2023. Disponible en: https://www.nato.int/cps/en/natohq/news_211919.htm

[6] WALL, C. y MORCOS, P. «Invisible and Vital: Undersea Cables and Transatlantic Security». Center for Strategic and International Studies (CSIS), 11 de junio de 2021. Disponible en: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Importancia de la red

Los cables submarinos de fibra óptica son la infraestructura crítica central de la era digital. Son la vía a través de la cual transita entre el 95 y el 99 % de las comunicaciones digitales que se producen a diario. Frente a otras tecnologías alternativas para la transmisión de datos (inalámbricas o satelitales), los cables ofrecen ventajas comparativas imbatibles en cuanto a capacidad, velocidad y seguridad de transmisión, gracias, entre otras razones, al desarrollo tecnológico reciente que permite la instalación de una nueva generación de cables submarinos de alta capacidad, única tecnología que posibilita atender el extraordinario incremento de demanda de ancho de banda que se está generando (fig. 1) como consecuencia del uso a gran escala de almacenamiento de información en la nube, el desarrollo de redes 5G, el «internet de las cosas» y la inteligencia artificial[7].

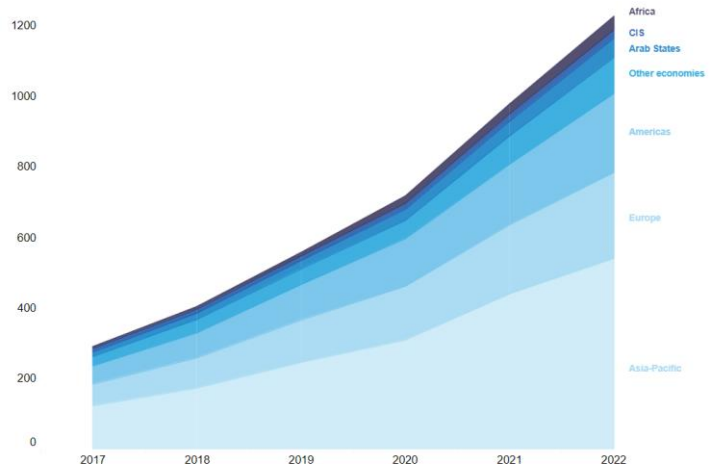

Figura 1. Uso de ancho de banda internacional, por regiones (en Tb/s)[8]
Fuente: https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-international-bandwidth-usage/

Actualmente, se estima que existen en funcionamiento unos 530 sistemas de cable submarino en todo el mundo —más del doble que en 2013—, cuyo crecimiento no cesa[9].

[7] SUBMARINE TELECOMS FORUM. *Industry Report 2022/2023*. Disponible en: https://issuu.com/subtelforum/docs/submarine_telecoms_indsutry_report_issue_11

[8] El terabit por segundo (Tb/s) es una unidad que mide la tasa de transferencia de los datos (1 Tb/s equivale a 1000 gigabits por segundo). No se debe confundir con el terabyte (TB), que es una unidad que mide la capacidad de almacenamiento de datos.

[9] TELEGEOGRAPHY. «Submarine Cable Map». 2023. Disponible en: https://www.submarinecablemap.com/

Estructura de un sistema de cable submarino

Los sistemas de cables submarinos conforman «ecosistemas» complejos en los que participan instalaciones, tecnologías y empresas muy especializadas y muy diferentes entre sí. Fabricantes, instaladores y reparadores conviven con los propietarios y gestores de los sistemas, junto con las grandes tecnológicas, principales suministradoras de los datos que transitan por la red.

El cable, en sí mismo, tiene el calibre aproximado de una manguera. La fibra óptica de su interior va recubierta por sucesivas capas de protección (fig. 2.a). En las zonas más próximas a las costas o de poca profundidad, los cables son recubiertos por una suerte de armadura que los protege de impactos exteriores (los daños producidos por las anclas de los barcos o las labores de pesca son los accidentes más comunes) (fig. 2.b). La capacidad de transmisión de los cables (ancho de banda) ha crecido también de forma exponencial en la última década. Hoy en día suelen estar compuestos por 24 pares de fibras, lo cual habría permitido pasar de una velocidad de transmisión de 4 Tb/s a finales del siglo XX a unos 15 Tb/s en 2012 y, finalmente, a 480 Tb/s en la actualidad.

A B

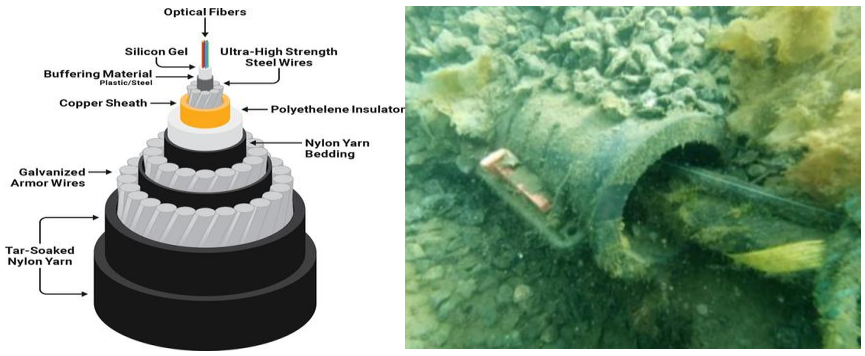

Figura 2. Sección de cable submarino y protección exterior
Fuente: (A) https://www.viavisolutions.com/en-uk/submarine-cable-networks y (B) https://greenpipegroup.com/area-of-use/sub-sea-cable/.

Los sistemas de cable submarino constan de dos partes (fig. 3). La «húmeda» o sumergida está integrada por el propio cable, los repetidores instalados a lo largo de su recorrido para amplificar la señal y las unidades de derivación. La parte «seca» o terrestre es el recorrido que hace el cable en superficie y suele constar de un punto de enlace (registro de playa) que conecta con la estación de desembarco, el lugar físico

donde se realiza la conexión con las redes terrestres y donde residen las capacidades de gestión del cable y los equipos que suministran la electricidad que necesita el sistema para funcionar (los sistemas de larga distancia requieren una capacidad de alimentación de 15.000 voltios)[10]. En sus proximidades suelen instalarse los «puntos de presencia» (*point of presence*, PoP)[11], que se encuentran alojados en los centros de datos *(data centers),* verdadero origen y destino de los cables submarinos.

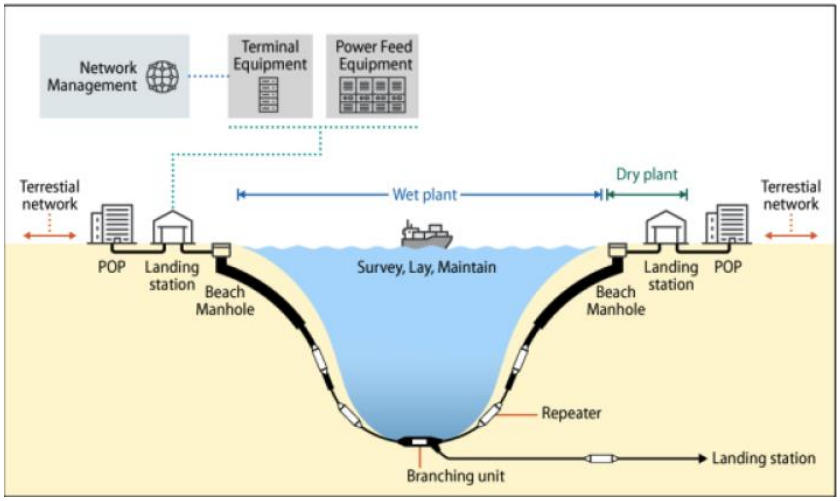

Figura 3. Estructura de un sistema de cable submarino
Fuente: https://crsreports.congress.gov/product/pdf/R/R47237

Las ventajas que ofrece la transmisión de datos a través de cable son incuestionables. En comparación con los satélites ofrece una mayor resistencia ante inclemencias meteorológicas, una latencia[12] significativamente menor y un ancho de banda incomparable, lo cual convierte a esta infraestructura en más fiable, duradera y de mayor capacidad. No obstante, para conectar regiones remotas y sin salida al mar, los satélites representan una opción viable. Empresas como Amazon o SpaceX están desplegando sus propias redes satelitales. Esta última prevé lanzar hasta 12.000 satélites en los

[10] KANEKO, T. *et al.* «Power Feeding Equipment for Optical Submarine Cable Systems», *NEC Technical Journal,* vol. 5, n.º 1. 2010, pp. 28-32. Disponible en: https://www.nec.com/en/global/techrep/journal/g10/n01/pdf/100107.pdf?nid=gihoEN017

[11] Un PoP es un punto de interfaz de red que permite la interconexión entre los usuarios locales y los proveedores de servicios de internet. Los PoP normalmente albergan servidores, enrutadores, conmutadores de red, multiplexores y otros equipos de interfaz de red. Suelen ubicarse en los centros de datos.

[12] La latencia es el tiempo que tarda en transmitirse un paquete de datos dentro de la red. Esto es, el tiempo que transcurre desde que un usuario hace una solicitud al servidor y el momento en que recibe la respuesta.

próximos años (habrá que ver cómo se resuelven los problemas que planteará semejante saturación en las órbitas disponibles). En todo caso, estos satélites estarán conectados a los puntos de interconexión de internet (*Internet exchange point,* IXP), que suelen estar localizados, como los PoP, en las cercanías de los puntos de desembarco de los grandes sistemas de cables submarinos. La función de los cables submarinos, como red troncal de transmisión, parece por el momento insustituible[13], lo cual determina el extraordinario crecimiento que se augura a este sector en la presente década[14].

Seguridad de la red

Los sistemas de cable submarinos son infraestructuras vulnerables a distintos tipos de amenazas: físicas, digitales y, recientemente, también las derivadas de la competencia geopolítica.

Cada año se producen más de un centenar de accidentes que afectan a la integridad del sistema. Se trata de casos en los que los cables se dañan o se cortan por completo, lo que afecta a su capacidad de transmisión. La mayor parte de estos accidentes son causados por actividades pesqueras, dragados o por el impacto de anclas. Existe una industria específica destinada a la reparación de cables submarinos, cuyos servicios son demandados constantemente para el mantenimiento de las redes, lo cual conduce a una saturación de los barcos que prestan estos servicios, con la consecuente repercusión sobre tarifas y plazos para realizar las reparaciones[15]. Los fenómenos geológicos (terremotos o erupciones volcánicas) son más infrecuentes, pero sus consecuencias sobre la red suelen ser más trascendentes.

[13] BOBIS, T. «¿Satélite o cables submarinos?», *MCPro.* 4 de marzo de 2020. Disponible en: https://www.muycomputerpro.com/2020/03/04/satelite-o-cables-submarinos-el-futuro-de-internet-es-la-interconexion.

[14] Se prevé que el mercado mundial de cables submarinos de fibra óptica, estimado en 18.200 millones de dólares en 2022, alcance los 48.000 millones de dólares en 2030, con un crecimiento cercano al 13 % anual durante el periodo 2022-2030 (GLOBAL INDUSTRY ANALYSTS. *Submarine Optical Fiber Cables: Global Strategic Business Report.* Enero de 2023. Disponible en: https://www.researchandmarkets.com/reports/2666991/submarine_optical_fiber_cables_global_strategic)

[15] BURNETT, D.R. «A Reboot of Wartime Submarine Fiber Optic Cables», *SubTel Forum Magazine,* n.º 127. 2022, p. 56. Disponible en: https://issuu.com/subtelforum/docs/subtel_forum_127

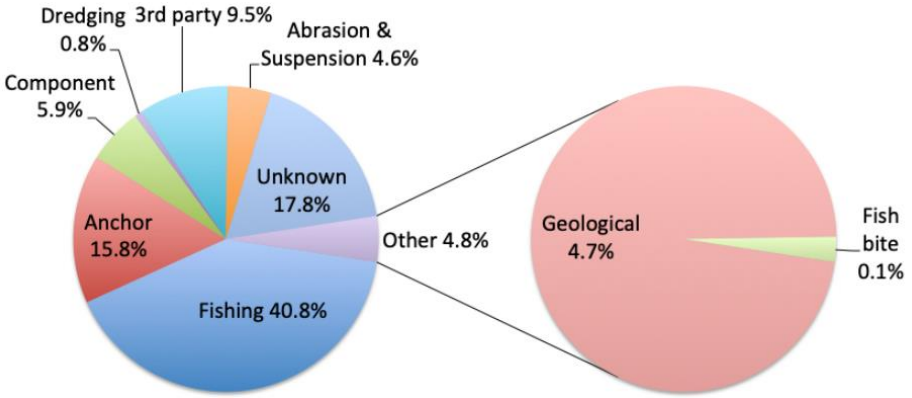

Figura 4. Causas de accidentes en los cables submarinos (1959-2021)
Fuente: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf

Existen también acciones deliberadas para dañar los sistemas de cables. Estas acciones pueden ser realizadas por actores no estatales, normalmente se centran en ataques cibernéticos y son llevadas a cabo por activistas *hackers* o grupos organizados de delincuencia digital (grupos de *ransomware*)[16]. En general, representan una amenaza de menor entidad, pero no por ello desdeñable[17], para las redes y sistemas operativos de los cables submarinos.

El principal desafío lo representan aquellas otras amenazas que encarnan las acciones de sabotaje y espionaje perpetradas por actores estatales. El posible impacto de estos ataques, que pueden ser considerados de «zona gris», resulta muy variable: desde interrupciones intermitentes del servicio hasta cortes completos del tráfico que pueden tardar días o semanas en resolverse. El ataque contra el gaseoducto submarino Nord Stream, perpetrado en septiembre de 2022 por los servicios de inteligencia ucranianos[18], supuso la destrucción completa de esta infraestructura. En el caso de los cables, la resiliencia de la red global depende fundamentalmente de la redundancia de los sistemas

[16] El *ransomware* es un tipo de virus informático o código malicioso que impide la utilización de los sistemas que infecta. El ciberdelincuente toma el control del sistema infectado y lo «secuestra», exigiendo el pago de un rescate por su restitución.
[17] El único ejemplo conocido de ciberataque contra cables submarinos se produjo en abril de 2022, cuando el Gobierno de Estados Unidos reveló que había frustrado un ataque contra uno de los cables que conectan Hawái (TEMPLE-RASTON, D. y POWERS, S. (2022). «Who tried to hack Hawaii's undersea cable? », *The Record.* 27 de abril de 2022. Disponible en: https://therecord.media/who-tried-to-hack-hawaiis-undersea-cable).
[18] EUROPA PRESS. «Una investigación apunta a que un oficial militar ucraniano coordinó el ataque al gaseoducto Nord Stream». 12 de noviembre de 2023. Disponible en: https://www.europapress.es/internacional/noticia-investigacion-apunta-oficial-militar-ucraniano-coordino-ataque-gaseoducto-nord-stream-20231112051830.html

en funcionamiento (esto es, de la existencia de cables alternativos para transmitir la información) y de la protección y resistencia de la propia red. Los ataques pueden producirse en toda la extensión del sistema, tanto en la zona sumergida como en la terrestre (especialmente en el entorno de las estaciones de aterrizaje), siendo estas zonas las más expuestas a las acciones de sabotaje físico, dada su mayor accesibilidad[19].

La protección de los sistemas de cable al llegar a tierra no siempre cuenta con las garantías de seguridad necesarias. Las playas (una tormenta puede dejar al descubierto un tramo de cable sobre la arena), los registros de playa (semejantes a un registro de alcantarilla) y, en menor medida, las estaciones de desembarco suelen ser puntos extremadamente vulnerables a las acciones de sabotaje. A ello se suma el hecho de la concentración de cables en un mismo punto. Dado que los desembarcos deben realizarse en terrenos arenosos que reúnan unas características específicas, los diferentes sistemas tienden a concentrar sus enlaces con las redes terrestres en un único punto, donde convergen todas las instalaciones técnicas de la parte «seca» del sistema.

La fácil accesibilidad y la concentración de cables convierten a los puertos de desembarque en el elemento más vulnerable de los sistemas de cables. Ejemplo de ello fue la interrupción del servicio ocurrida en Marsella en 2022.

Por sus características geográficas específicas, Marsella se ha convertido en uno de los grandes nodos de la red global (ocupa la séptima posición en el tráfico mundial de datos). En su puerto desembarcan 15 sistemas de cable (17 si sumamos los cables que pasan por La Seyne-sur-Mer y Toulon) que conectan a 53 países, con una población total de 4500 millones de personas.

El 19 de octubre de 2022 tres cables[20] fueron cortados en las proximidades de Marsella[21], en una arqueta terrestre. El sabotaje no llegó a producir interrupciones de tráfico, aunque

[19] LONG, M. L. «Information Warfare in the Depths: An Analysis of Global Undersea Cable Nerworks», *Proceedings*, vol. 149/5/1.433. Mayo de 2023. Disponible en: https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks

[20] Los cables que unen Marsella y Lyon, Marsella y Milán y el cable submarino Marsella-Barcelona (UPDATE NEWS. «Varios cortes de cables submarinos en Marsella provocan fallos en internet». 25 de octubre de 2022. Disponible en: https://www.upday.com/es/varios-cortes-de-cables-submarinos-en-marsella-provocan-fallos-en-internet).

[21] Unos meses antes se había producido el corte de otros tres cables en Île-de-France y Fresnes-en-Woëvre (Grand Est), siguiendo procedimientos semejantes (01NET. «Des câbles sabotés provoquent

causó pérdidas de paquetes de datos y un aumento de latencia. El servicio pudo restablecerse en pocas horas al conservar la compañía gestora el control sobre el sistema y la capacidad para redirigir el tráfico.

A medida que crece el volumen de información que transita por los cables y, en consecuencia, la importancia estratégica de la red global, crece también la competencia entre las grandes potencias por su control, que proyectan sobre esta infraestructura sus designios geopolíticos. Los actores estatales pueden determinar qué sistema de cable se construye o cuál no, qué regiones enlazan o qué proveedores y socios participan. Siguiendo una lógica de dependencia y exclusión, dos actores relevantes, Estados Unidos y China, dirimen su competencia geopolítica también en este ámbito. Dado que el sector se encuentra en manos de compañías privadas, la influencia política sobre las empresas resulta determinante para llevar a cabo sus propósitos, preservando la integridad de la red propia y la seguridad de los datos transmitidos, al tiempo que se trata de convertir en vulnerables las del competidor.

Estados Unidos ha identificado a China y Rusia como fuente de posibles amenazas a la red de cables submarinos[22]. Cada uno de estos actores entraña desafíos de distinta naturaleza.

La creciente relevancia mundial alcanzada por empresas chinas como HMN Technologies (antes Huawei Marine), uno de los principales fabricantes de cable submarino, u operadoras como China Mobile, China Telecom y China Unicom, todas ellas de titularidad estatal, hace temer a Washington posibles cambios en los patrones de enrutamiento en la red, lo cual tendría un efecto directo sobre el tráfico al favorecer el acceso a determinados contenidos, y también sobre los negocios internacionales, pudiendo generar dependencia tecnológica entre los países que enlazan los sistemas de cables[23].

---

des problèmes de connexion à Internet dans plusieurs villes de France». 27 de abril de 2022. Disponible en: https://www.01net.com/actualites/des-cables-sabotes-provoquent-des-problemes-de-connexion-a-internet-dans-plusieurs-villes-de-france-2056037.html).

[22] SCHADLOW, N. y HELWIG, B. «Protecting undersea cables must be made a national security priority», *Defense News.* 1 de julio de 2020. Disponible en: https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/

[23] SHERMAN, J. (2021). *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*. Atlantic Council. Disponible en: https://www.atlanticcouncil.org/wp-

Las autoridades estadounidenses se muestran convencidas de que existe la capacidad tecnológica para interferir las comunicaciones a través de la red por medio de «puertas traseras» *(backdoors), software* malicioso insertado en los sistemas de cable durante el proceso de fabricación e instalación. O incluso extrayendo directamente los datos desde el fondo del mar. Esta última posibilidad resulta tan difícil con los medios técnicos disponibles que no existe conocimiento público de que ningún país pueda hacerlo en la actualidad[24], pero, al existir el antecedente de la operación Ivy Bells[25], no puede descartarse por completo.

Por su parte, Rusia plantea un tipo de amenaza más convencional sobre la integridad de la red de cables. Ha sido minuciosamente documentada la atención que la Marina rusa presta a los cables submarinos en el Atlántico Norte[26]. Y se atribuye a una acción suya el corte de la red de investigación marina de un observatorio oceánico noruego (en 2021) capaz de registrar el paso de submarinos furtivos por el mar del Norte[27].

Rusia, aunque también China, dispone de los medios precisos para realizar un ataque contra cables submarinos en aguas profundas: submarinos, embarcaciones sumergibles, embarcaciones de superficie con capacidad para cartografiar y alcanzar el fondo oceánico desplegando sumergibles autónomos o tripulados[28]. Un ataque coordinado, a gran escala, contra los cables que unen a Europa con Estados Unidos tendría un gran impacto en la economía y la seguridad de los Estados miembros de la OTAN[29].

content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf

[24] WALL, C. y MORCOS, P. *Op. cit.*

[25] La operación Ivy Bells fue una misión estadounidense de espionaje llevada a cabo durante la Guerra Fría que permitió realizar escuchas telefónicas en las líneas de comunicación submarinas soviéticas en el mar de Ojotsk (SONTAG, S. y DREW, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*. Harper Collins, Nueva York, 2000).

[26] HINCK, G. *Op. cit.*

[27] Los cables que unen los sensores con las estaciones de control en tierra fueron cortados y luego extraídos, lo cual alimentó las sospechas de que se trataba de un sabotaje deliberado (NEWDICK, T. «Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut», *The Drive.* 11 de noviembre de 2021. Disponible en: https://www.thedrive.com/the-war-zone/43094/norwegian-undersea-surveillance-network-had-its-cables-mysteriously-cut).

[28] INSIKT GROUP. *The Escalating Global Risk Environment for Submarine Cables. Recorded Future*. 27 de junio de 2023, pp. 13-15. Disponible en: https://go.recordedfuture.com/hubfs/reports/ta-2023-0627.pdf

[29] MATIS, M. *The Protection of Undersea Cables: A Global Security Threat*. U. S. Army War College (Strategy Research Paper), 2012. Disponible en: https://apps.dtic.mil/sti/pdfs/ADA561426.pdf

«Guerra fría» chino-estadounidense por los cables submarinos

En el plano estratégico, lo que está en juego es la integridad de la red de cables ante los daños que pueda recibir por ataques deliberados de actores estatales o no, bien como sabotaje, en un contexto de acciones encubiertas de «zona gris», bien como ataque en el marco de un conflicto armado. Pero en el plano geopolítico lo que se dirime es que Estados Unidos siga siendo el principal centro mundial de tráfico en la red.

A comienzos del siglo XXI la mayor parte del tráfico mundial de internet se canalizaba a través de Estados Unidos[30], en 2019 representaba el 23 %[31]. El descenso progresivo de la primacía estadounidense ha ido en paralelo al incremento del acceso de otros países a la red global (tabla 1).

Las empresas estadounidenses han tratado de responder a este desafío construyendo nuevos sistemas de mayor capacidad y procurando controlar las rutas que albergan los principales tráficos, al tiempo que intentan excluir la participación de compañías chinas[32].

[30] WINSECK, D. «The Geopolitical Economy of the Global Internet Infrastructure», *Journal of Information Policy*, vol. 7. 2017, pp. 228-267. Disponible en: https://www.jstor.org/stable/10.5325/jinfopoli.7.2017.0228

[31] STRONGE, T. «Does 70% of the World's Internet Traffic Flow through Virginia?», *TeleGeoghaphy Blog.* 30 de mayo de 2019. Disponible en: https://blog.telegeography.com/does-70-of-the-worlds-internet-traffic-flow-through-virginia#:~:text=We%20think%20the%20Loudoun%20County,Mauldin's%20SubOptic%202019%20mythbusting%20session

[32] HILLMAN, J. E. *Securing the Subsea Network A Primer for Policymakers*. Center for Strategic and International Studies (CSIS), Washington, 2021. Disponible en: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210309_Hillman_Subsea_Network_1.pdf?1c7RFgLM3w3apMi0eAPl2rPmqrNNzvwJ

Tabla 1. Uso mundial de internet en 2023 (estimación respecto población, en %)

Regiones	% población mundial	Tasa de Penetración	Crecimiento 2000-2023	% tráfico mundial Internet
África	17,6	43,2	13.233	11,2
Asia	54,9	67,0	2452	54,2
Europa	10,6	89,2	611	13,9
América Latina / Caribe	8,4	80,5	2858	9,9
América del Norte	4,7	93,4	222	6,5
Oriente Medio	3,4	77,1	6194	3,8
Oceanía / Australia	0,5	70,1	301	0,6

Fuente: https://www.internetworldstats.com/stats.htm

Un instrumento decisivo para lograrlo es el Comité para la Evaluación de la Participación Extranjera en el Sector de Servicios de Telecomunicaciones de los Estados Unidos (creado en 2020), más conocido como Team Telecom. Su misión oficial es proteger la seguridad nacional frente a la participación extranjera en el sector de las telecomunicaciones[33]. Pero en su corta existencia este comité ha realizado una labor implacable impidiendo las conexiones por cable con China desde territorio estadounidense (entre Los Ángeles y Hong Kong)[34] y excluyendo a las empresas chinas de la construcción de sistemas de cable internacionales (como ha sido el caso del SeaMeWe-6)[35].

[33] JALINOUS, F., BRADY, R. y CROWLEY, M. «Team Telecom Two-Year Anniversary», *White & Case.* 25 de abril de 2022. Disponible en: https://www.whitecase.com/insight-alert/team-telecom-two-year-anniversary

[34] El Pacific Light Cable Network (PLCN) fue una asociación entre Alphabet (Google), Meta (Facebook) y Peng Group, de China, para instalar un sistema de 12.800 kilómetros con una capacidad de 120 Tb/s, la ruta transpacífica de mayor capacidad en aquel momento. El cable se completó en 2018, pero, tras las advertencias del Team Telecom, las empresas estadounidenses se retiraron, abandonando la sección entre Luzón y Hong Kong y redirigiendo el cable hacia Singapur (LEPRINCE-RINGUET, D. «Facebook and Google drop plans for underwater cable to Hong Kong after security warnings», *ZDNet.* 11 de enero de 2022. Disponible en: https://www.zdnet.com/home-and-office/networking/facebook-and-google-drop-plans-for-underwater-cable-to-hong-kong-after-security-warnings/). Otros dos proyectos de cables fueron igualmente suspendidos.

[35] El consorcio que proyectó el cable SeaMeWe-6, de 19.000 kilómetros de longitud y que enlazará el sudeste de Asia con Europa, adjudicó el contrato a la estadounidense SubCom tras haber seleccionado

Aunque los argumentos esgrimidos por las autoridades estadounidenses para justificar tales decisiones se centran en los riesgos de seguridad que entrañan, no debería descartarse una lógica económica subyacente a la referida estrategia, dirigida a excluir del mercado a un competidor tecnológico directo. Hay evidencias de que estas acciones de boicot han logrado frenar la expansión extraordinaria lograda por HMN Tech. De suministrar el 18 % de los cables submarinos que entraron en servicio en los últimos cuatro años, ha pasado a participar actualmente en el 7 % de los cables en desarrollo en todo el mundo[36].

Existe un riesgo real de que la rivalidad estratégica entre grandes potencias por el control de las tecnologías de vanguardia, desde los chips[37] hasta los cables submarinos, pueda crear una suerte de división del mundo en bloques opuestos con una interconexión limitada, lo cual tendría consecuencias trascendentes para todos.

Como se ha señalado, la difusión de nuevas tecnologías va a impulsar la demanda global de ancho de banda en los próximos años. Este crecimiento será más significativo en las economías en desarrollo de regiones como África (una de las más desatendidas en las conexiones a la red), América del Sur u Oriente Medio. Un tercio de estos países carece aún de las infraestructuras básicas necesarias para su conexión a la red (cables, puntos de intercambio o centros de datos), por lo que cabe esperar un extraordinario crecimiento en los próximos años[38].

Su posición geográfica sitúa a la península ibérica en una encrucijada estratégica en las conexiones de cable submarino intercontinentales. Los recientes desarrollos, con la instalación de sistemas de última generación, están transformado la relevancia internacional de España y Portugal, convirtiendo a ambos Estados en un nodo importante

inicialmente a la empresa china HMN Tech (PREGO, C. «Los cables submarinos no se libran de la creciente tensión entre China y EEUU: Pekín da un paso atrás en el ambicioso Sea-Me-We 6», *Xataca.* 12 de febrero de 2023. Disponible en: https://www.xataka.com/otros/cables-submarinos-no-se-libran-creciente-tension-china-eeuu-pekin-da-paso-atras-ambicioso-sea-me-we-6).

[36] Las estimaciones se basan en la longitud total del cable tendido, no en el número de proyectos (SUBMARINE TELECOMS FORUM. *Industry Report 2022/2023,* n.º 11. 23 de octubre de 2022. Disponible en: https://issuu.com/subtelforum/docs/submarine_telecoms_indsutry_report_issue_11).

[37] MILLER, Ch. *La guerra de los chips. La gran lucha por el dominio mundial*. Península, Barcelona, 2023.

[38] Por ejemplo, el potencial de África en este campo es significativo. Con el 17 % de la población mundial, solo alberga el 1 % de la capacidad de los centros de datos instalados (ABUDHO, B. y BEARD, S. *Africa Horizons 2023-2024*. Knight Frank, 2023, pp. 8-9. Disponible en: https://content.knightfrank.com/research/1741/documents/en/africa-horizons-202324-10427.pdf).

de interconexión de la red global, susceptible de conformar un gran *hub* digital en el sur de Europa.

La red española de cable submarino (nacional y regional)

En la actual red de cable submarino de fibra óptica que opera en territorio español se pueden distinguir dos estructuras que se complementan y corresponden a etapas de desarrollo diversas, con operadores distintos (nacionales e internacionales) y diferente alcance en sus conexiones (regional o intercontinental).

En la primera de estas estructuras se encuentran los cables ópticos tendidos entre finales del siglo XX y la segunda década del actual por empresas locales, cuya función es conectar los territorios extrapeninsulares con el continente. La segunda estructura (que se analiza más adelante) está formada por las conexiones peninsulares a los grandes sistemas de cables intercontinentales, promovidos en los últimos tiempos por las grandes empresas tecnológicas y que permiten una conexión directa de alta capacidad con América, África, Oriente Medio y Asia Oriental.

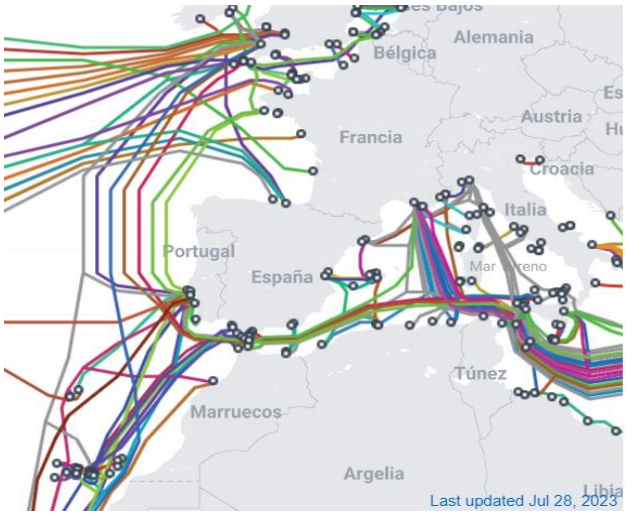

Figura 5. Cables submarinos que conectan la península ibérica
Fuente: https://submarine-cable-map-2023.telegeography.com/

Las principales empresas que operan en esta red son Telefónica (y su participada Telxius), Canalik, Islalink y GTD España. Su principal activo son los cables que conectan la Península con los archipiélagos y las ciudades autónomas de Ceuta y Melilla.

Canarias

El archipiélago canario constituye una plataforma estratégica con múltiples conexiones a las redes global, nacional y regional de cables submarinos. En la red de cables interinsulares el principal operador es Telefónica, con cables que conectan a todas las islas entre sí. Tenerife y Gran Canaria cuentan con tres cables de interconexión de esta empresa.

Tras la liberalización del mercado de las comunicaciones, a partir de 1996, nuevos operadores comenzaron a tender y explotar sus propias líneas. La primera empresa en romper el monopolio fue la compañía balear Islalink, a través de la sociedad Canalink, que en 2013 fue adquirida por el Cabildo de Tenerife. Canalink conecta Tenerife y Gran Canaria a través de dos cables submarinos y cuenta con uno más entre Tenerife y La Palma. Esta empresa desempeña un papel crucial en el acceso del archipiélago a las redes globales. El tercer operador es la compañía Cable Submarino de Canarias (Subcan), con dos cables operativos entre Tenerife y Gran Canaria.

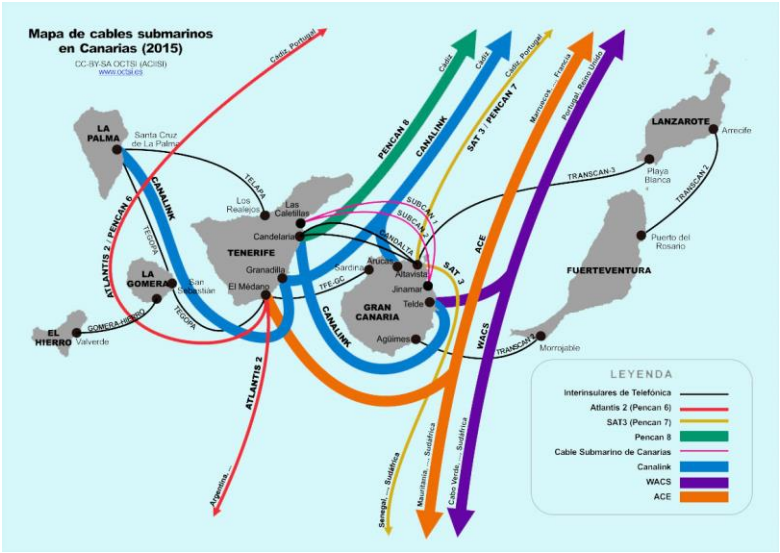

Figura 6. Mapa de los cables submarinos en el archipiélago canario (2015)
Fuente: https://www.octsi.es/datos/cables-submarinos-en-canarias

Las conexiones entre el archipiélago canario y la Península se realizan a través de dos operadores, Telefónica y Canalink, que explotan sus propias redes. Telefónica opera la red Pencan (Península-Canarias), que consta en la actualidad de tres cables.

Tanto Pencan-6 como Pencan-7 están concebidos como la sección española de los grandes sistemas transatlánticos, Atlantis-2 y SAT-3 respectivamente.

Atlantis-2 entró en servicio en marzo de 2000. Con una longitud total de más de 13.000 kilómetros, enlaza Argentina (Las Toninas) con Portugal (Lisboa) y cuenta con numerosos puntos de aterrizaje en diferentes países. Telefónica participó en el consorcio internacional promotor del sistema, asumiendo la sección española del proyecto. En el tramo comprendido entre El Médano (Tenerife) y Conil (Cádiz), el sistema resultante se denomina Pencan-6. Este cable está próximo a su obsolescencia.

Telefónica participó en un consorcio internacional semejante para construir el sistema de cable SAT-3, operativo desde 2002. Con una longitud superior a los 14.000 kilómetros, este cable conecta Portugal (Sesimbra) con Sudáfrica (Melkbosstrand) a través de la costa occidental africana. En el tramo comprendido entre Altavista (Las Palmas de Gran Canaria) y Chipiona (Cádiz), el sistema resultante es conocido como Pencan-7. Ambos cables (Pencan 6 y 7) son capaces de soportar una capacidad de 100 Gbit/s.

El más reciente de todos los sistemas que conectan el archipiélago con la Península es Pencan-8, operativo desde marzo de 2011. Se trata de un cable de 1347 kilómetros cuyas estaciones de aterrizaje se sitúan en Candelaria (Tenerife) y Conil (Cádiz). Este sistema de gran magnitud (320Gbit/s) triplica la capacidad total conjunta ofrecida por los anteriores cables.

Por su parte, la compañía Canarias Submarine Link cuenta con el cable Canalink, de alta capacidad (8Tb/s), operativo desde 2011. Este sistema, de 2000 kilómetros de longitud total, está compuesto por varias secciones. La primera de ellas enlaza Rota (Cádiz) con Granadilla (Tenerife) y Arucas (Gran Canaria). En marzo de 2012 se instaló un ramal de 150 kilómetros que enlazó Marruecos (en Asilah, Tánger) a través de una unidad de derivación submarina[39].

[39] GUTIÉRREZ, J. J. «Tenerife echa el cable a África», *Diario de Avisos.* 21 de enero de 2012. Disponible en: https://www.diariodeavisos.com/2012/01/tenerife-echa-el-cable-a-africa/.

Además de los mencionados, en el archipiélago aterrizan otros cables internacionales, más modernos y de mayor capacidad. WACS (2012) parte de Londres y aterriza en Yzerfontein (al oeste de Ciudad del Cabo). Cuenta con catorce puntos de aterrizaje, doce a lo largo de la costa occidental de África (incluyendo Cabo Verde y las islas Canarias) y dos más en Europa (Reino Unido y Portugal). El cable es propiedad de un grupo de empresas sudafricanas.

ACE (Africa Coast to Europe), construido en 2012, es una iniciativa de France Telecom, que lidera un consorcio en el que participan sus filiares regionales y otros socios locales (veinte empresas en total). ACE conecta veinticuatro países, tres europeos (Francia, Portugal y España, en las islas Canarias) y el resto africanos, desde Mauritania hasta Sudáfrica.

Los sistemas Equiano y 2Africa, ambos de última generación y gran capacidad, son analizados más adelante.

Baleares

La red de cable submarino del archipiélago balear difiere de la existente en Canarias tanto por densidad como por su conexión internacional. Las diferencias referidas evidencian la relevancia que el factor geoestratégico tiene en la construcción de estas redes. A pesar de ocupar una posición privilegiada en el centro geográfico del Mediterráneo occidental, los principales cables que atraviesan esta región no disponen de puntos de desembarco en la costa balear, de forma que sus islas han quedado relativamente aisladas de la tupida red de cables que atraviesan el Mediterráneo.

Telefónica ha sido el proveedor tradicional de estos servicios en Baleares a través de los sistemas Penbal (Península-Baleares) en sus sucesivas versiones. En la actualidad se encuentran operativos Penbal 4 (1990), que enlaza Valencia con Ibiza y Mallorca, y Penbal 5 (1995), entre Gavá (Barcelona) y Ses Covetes (Mallorca). Ambos cables fueron actualizados a comienzos del presente siglo, aumentando su capacidad y su vida útil.

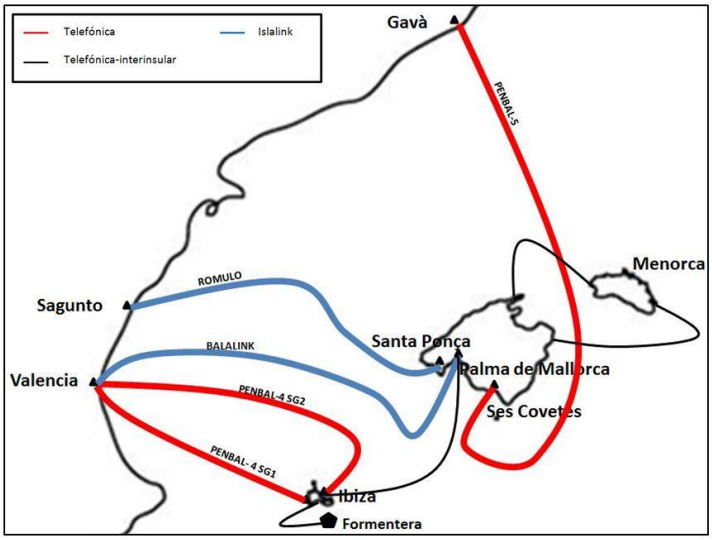

Figura 7. Mapa de los cables submarinos en el archipiélago balear (2017)
Fuente: https://blog.cnmc.es/2017/09/05/que-cables-submarinos-conectan-el-territorio-espanol-enganchados-a-los-cables-submarinos-ii/

El operador interinsular de cable submarino más importante es Red Eléctrica (Redeia es su denominación actual), a través de su participada Reintel, principal operador de fibra oscura de España. Redeia es el promotor del proyecto Rómulo, un enlace submarino para transportar electricidad desde la Península hasta las islas Baleares. El cable, que transporta una corriente eléctrica de alto voltaje, lleva asociado un sistema de fibra óptica en todo su recorrido, tanto sumergido como terrestre. En su primera fase (2012) conectó la subestación de Morvedre (Sagunto) con Santa Ponsa (Mallorca). El sistema fue ampliado hasta completar la interconexión entre todas las islas: enlaces Mallorca-Ibiza (2013), Mallorca-Menorca (2020) e Ibiza-Formentera (2023).

El tercer operador insular es la empresa balear Islalink, responsable de Balalink (2001), el primer sistema de cable submarino construido en España por un operador independiente. Este enlaza Valencia con Palma de Mallorca. Islalink cuenta además con dos sistemas adicionales que proporcionan en total tres rutas de conexión a la isla de Mallorca y dos rutas a Ibiza. El sistema se prolonga en tierra, creando una red que abarca todo el territorio mallorquín. Desde el sur de la isla parte también el cable ALPAL-2 (2002), que enlaza con Argel.

Ceuta, Melilla y norte de África

Las conexiones entre la Península y las ciudades de Ceuta y Melilla, Argelia y Marruecos se realizan a través de diversos sistemas de cables de fibra óptica. Telefónica es el operador tradicional de los cables que prestan servicio a las ciudades autónomas, con sendos sistemas redundantes para evitar posibles desconexiones, como las ocurridas en 2007 y 2010 tras ser seccionado el cable Almería-Melilla por accidentes de tráfico marítimo.

La conexión submarina a través del Estrecho resulta particularmente difícil, debido a las condiciones orográficas del fondo oceánico (hasta 1600 metros de profundidad), las fuertes corrientes y la intensa actividad de tráfico marítimo. Los accidentes resultan mucho más frecuentes en esta área que en el resto de la red española.

Ceuta cuenta con una densa red de conexión por cable. Telefónica dispone de dos sistemas: Lince (2008), que enlaza con La Línea de la Concepción, y CEE (2014), que enlaza con Estepona. En 2020, la empresa de matriz chilena GTD España construyó un moderno sistema de doble trazado y alta capacidad (460Tb/s), denominado Dos Continentes I & II, que refuerza la conexión de Ceuta enlazando con Tarifa (I) y La Línea de la Concepción (II). A esta red se le sumará en 2025 el cable de fibra óptica asociado al cable eléctrico submarino que la compañía Redeia proyecta construir entre San Roque y Ceuta, que permitirá reforzar el suministro energético de la ciudad, que depende hasta el momento de una central térmica alimentada por diésel.

Por su parte, Melilla cuenta con una interconexión de fibra óptica mucho más limitada, reducida a dos sistemas: el veterano ALME (1990), propiedad de Telefónica, cuya vida útil se ha logrado prolongar hasta la actualidad, y el enlace Roquetas de Mar-Melilla, propiedad del gobierno de la ciudad autónoma y del que es concesionario Telefónica por un periodo de treinta años. Se trata de un cable de alta capacidad (240 Gbt/s, frente a los 90 de ALME), en servicio desde 2014.

A pesar de la redundancia que ofrecen los dos cables, la conexión de Melilla con la Península resulta precaria por su vulnerabilidad. Esta situación podría mejorarse en caso de establecerse una conexión eléctrica submarina con un sistema de fibra óptica

asociado, infraestructura demandada desde la ciudad pero cuya realización no se contempla por el momento[40].

Las conexiones de cables a través del estrecho de Gibraltar se complementan con los escasos enlaces directos existentes entre España y Marruecos. Se reducen a tan solo dos sistemas, el construido por Maroc Telecom y Telefónica en 1994, que enlaza las localidades de Estepona y Tetuán, y la conexión marroquí al cable Canalink (2012), que une el archipiélago canario con la Península a través de Rota (Cádiz).

Más modernas y de mayor capacidad son las conexiones que enlazan con Argelia, que cuentan con el veterano sistema ALPAL-2 (2002), entre Mallorca y Argelia, y el nuevo sistema ORVAL (2020), de 40 Tb/s, promovido por Algerie Telecom, que une Orán con Valencia y cuenta con un ramal de desembarco en Argel.

Portugal

Los nuevos cables submarinos de alta capacidad tendidos en los últimos años han modificado el carácter nacional/territorial de los puntos de desembarco que hasta entonces distinguía a estas instalaciones. La proyección en tierra de estas conexiones submarinas hasta alcanzar su actual destino, que no son ya las redes telefónicas nacionales sino los centros de datos, ha trasformado a la península ibérica en una plataforma logística integrada para los servicios en la red, debido precisamente a la alta conectividad lograda, gracias a la conexión intercontinental ofrecida por estos nuevos cables, y a la interconexión establecida entre ellos gracias a la prolongación en tierra de los sistemas de cable. De esta forma, la Península se está convirtiendo en un nodo relevante de la red global, capaz de atraer la instalación de un creciente número de centros de datos. De aquí la necesidad de conocer también la conexión de Portugal a la red de cables submarinos, porque, en la práctica, estas conexiones actúan junto a las españolas como una plataforma única integrada.

El territorio peninsular de Portugal dispone de cuatro puntos de desembarco de cables internacionales: Sines (en el Alentejo Litoral), Sesimbra (junto a Setubal), Seixal (frente

[40] MELILLA HOY. «Melilla en Verde lamenta que ni la Ciudad ni el Estado planteen la conexión eléctrica con la Península». 17 de enero de 2023. Disponible en: https://melillahoy.es/melilla-en-verde-lamenta-que-ni-la-ciudad-ni-el-estado-planteen-la-conexion-electrica-con-la-peninsula/

a Lisboa, en la orilla meridional del estuario del Tajo) y Carcavelos (en las proximidades de Lisboa).

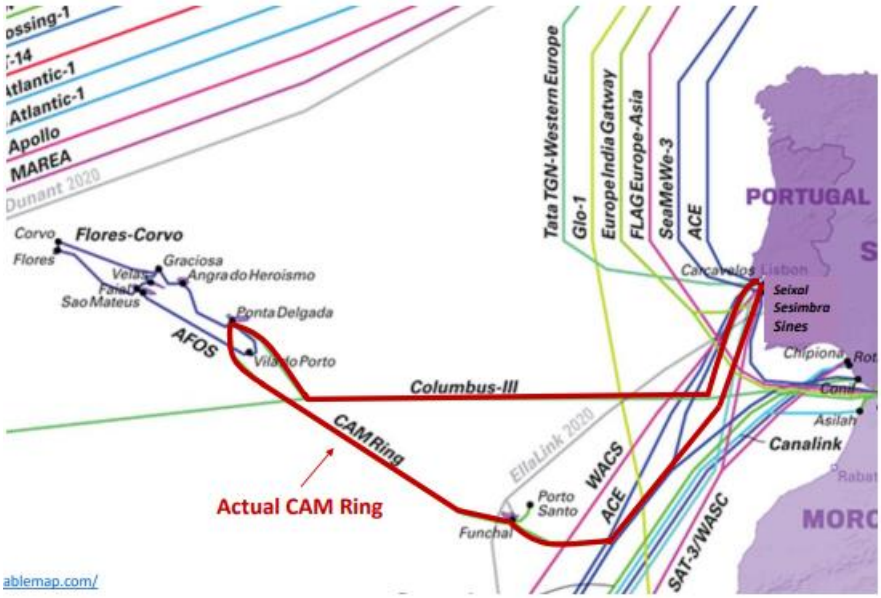

Figura 8. Mapa de los cables submarinos en territorio portugués (2021)
Fuente: https://anacom.pt/streaming/CabosSubmarinos_Aveiro_9abril.pdf?contentId=1615782&field=ATTACHED_FILE

En Sines los cables Ellalink y Medusa enlazan en sendas estaciones de amarre. La más reciente, propiedad de la empresa Start Campus, tiene previsto establecer un gran *hub* de centros de datos, con 495 MW de potencia instalada. La segunda estación de amarre se localiza en Sesimbra, donde desembarcan los cables SeaMeWe-3, SAT-3/WACS, Europe India Gateway y un segundo enlace de Medusa, así como también los nuevos grandes sistemas transatlánticos de Google: Equiano y Nuvem. Por su parte, Seixal recibe los cables Main One, SeaMeWe-3 y Tata TGN-Europa Occidental. Finalmente, en la estación de Carcavelos enlazan los dos cables que conectan el territorio peninsular con los archipiélagos de Azores (Columbus III Azores-Portugal, 1999) y Madeira (Continente-Madeira, 2000) y los cables ACE y 2Africa.

La extraordinaria localización estratégica de Portugal ha favorecido que fuera su territorio, y no el español, el que tradicionalmente acogiera los enlaces con los grandes sistemas internacionales de cable procedentes de los cuatro puntos cardinales, principalmente Asia Oriental (SeaMeWe-3, EIG) y África (SAT-3/WASC, Main One,

WACS, ACE), con sus prolongaciones hacia el Reino Unido, y también con el continente americano (Columbus III), aunque en este caso haya ocupado una posición periférica en los enlaces transatlánticos.

La llegada de los nuevos cables de última generación (Ellalink, 2Africa, Equiano y Medusa, a los que se sumará Nuvem en 2026) refuerza y mejora esa posición que tradicionalmente ocupaba Portugal en las conexiones del sur de Europa. Está prevista, además, la construcción de nuevos sistemas, que, a pesar de tener un alcance más limitado, no dejan de ser relevantes y densifican la red portuguesa, que gana en redundancia. Se trata de los proyectos Octopus y Pisces.

Octopus es un proyecto promovido por las empresas Abu Dhabi National Energy Company PJSC (Taqa) y Octopus Energy Group para tender el que será el cable eléctrico de alta tensión más largo del mundo entre Marruecos (en la región de Guelmim-Oued Noun, antiguo Sidi Ifni) y Reino Unido (Devon). El cable, cuya entrada en servicio no se ha precisado, está pensado para suministrar energía renovable generada en Marruecos al mercado británico, que afronta un grave problema para conectar sus propias fuentes renovables a la red eléctrica nacional. El sistema llevará asociado un cable de fibra óptica y su recorrido irá en paralelo a la costa de Portugal y a la cantábrica española. Aunque no han sido identificados posibles puntos de desembarco en la Península, se prevé que al menos uno se realice en territorio portugués.

El proyecto Pisces es una iniciativa promovida por el Gobierno irlandés para conectar el corredor norte de la red transatlántica de cables (situado al norte de las islas británicas, con destino a Escandinavia) con el corredor sur (península ibérica), convirtiendo así a Irlanda en un nodo de interconexión principal en las rutas atlánticas. El proyecto, que se encuentra en sus etapas iniciales, prevé el tendido de un cable troncal entre Galway y Sines, con una derivación para enlazar con Nantes y Bilbao.

En lo que respecta a la red nacional, Portugal presenta obvias similitudes con España al tratarse de Estados con territorios insulares. Esta circunstancia, multiplicada en el caso de España por su dispersión en tres costas, obliga a concentrar los esfuerzos en garantizar la conectividad con los territorios extrapeninsulares. En el caso de Portugal estas redes son algo menos densas y modernas que las españolas, pero se encuentran en proceso de renovación. En un futuro próximo está prevista la construcción por parte

del Gobierno portugués, a través de la empresa Infraestructuras de Portugal, de un nuevo anillo que permita modernizar la conexión entre los archipiélagos de Azores y Madeira y el continente (CAM-2). Se espera que este pueda entrar en servicio en 2024.

En la red portuguesa, en contraste con la española, destaca el tendido de cables submarinos que conectan localidades situadas en el propio continente (Bugio, Sagres y Olisipo), inexistentes en España. Acaso pueda atribuirse esta preferencia a la configuración del territorio, que hace más rentable la configuración submarina frente a las conexiones terrestres.

El más reciente de todos ellos es Olisipo, un sistema de cable submarino de altísima capacidad (4,3 Petabits/s, esto es, 4300 Tb/s) que unirá de forma directa los centros de datos de Sines con Altice, en Lisboa, a través de la estación de desembarco de Carcavelos. Contará también con dos enlaces con las estaciones de Sesimbra y Sexal. De esta forma, el cable conectará todos los puntos de aterrizaje de cables submarinos internacionales en Portugal con los principales centros de datos establecidos en el país creando una región *cloud* integrada, esto es, con independencia del canal empleado (cable o punto de desembarco) toda la información recibida o enviada desde Portugal actuará como un destino único, lo cual multiplica su capacidad para atraer a nuevos operadores.

Figura 9. Mapa del cable Olisipo (2023)
Fuente: https://ella.link/2023/07/18/olisiposubmarinecablesystem/

Las nuevas conexiones peninsulares a la red global y sus consecuencias

Portugal ha creado las condiciones necesarias para que los nuevos cables de última generación puedan seguir llegando a sus costas (Ellalink, 2Africa, Equiano, Medusa y Nuvem). La novedad radica en que esta nueva generación de cables también alcanza el territorio español (Marea, Ellalink, Grace Hopper, 2Africa, Medloop, Anjana, Medusa), lo cual supone un llamativo contraste con respecto de la situación existente hace tan solo una década. Se trata de un cambio transcendental que es consecuencia tanto la transformación de la industria del cable, fruto de nuevos desarrollos tecnológicos, como de la acción empresarial realizada por la industria de las telecomunicaciones para convertir a España, y por extensión a la península ibérica, en un nodo relevante de la red global en el sur de Europa.

Un dato técnico ofrece una de las claves para comprender la nueva centralidad que está adquiriendo España como destino preferente de los nuevos sistemas de cable submarinos. Las aplicaciones estándar de latencia máxima permitida se sitúan en 65 milisegundos, lo cual implica que pueden operar en una distancia media de unos 5500 kilómetros[41]. Si trazamos una circunferencia con ese radio tomando como centro la península ibérica, en su interior se incluyen partes importantes de América del Norte, América del Sur, el norte de África y la práctica totalidad de Europa.

A medida que se desarrollan redes de interconexión en unos mercados crecientemente descentralizados, la conectividad internacional tiende a concentrarse en determinadas áreas de acceso interregional, situadas a una distancia relativamente próxima. De esta forma, España y Portugal han logrado una posición estratégica en la red global tanto para la recepción de contenidos como para su distribución posterior a través de la red.

Hasta 2018 los cables que conectaban la península ibérica con el resto del mundo habían sido instalados a comienzos del siglo XXI. Teniendo en cuenta que la vida media estimada de estos sistemas es de unos veinticinco años, resulta inevitable su sustitución. Pero, aparte de su obsolescencia, el factor que contribuye a su inviabilidad operativa es la creciente demanda de datos, que obliga a disponer de un ancho de banda cada vez mayor. La respuesta que la industria está dando a este rápido y extraordinario crecimiento es la construcción de nuevos sistemas de cable con mucha más capacidad de ancho de banda. Y la península ibérica ha conseguido mejorar su posición competitiva

[41] GUILLEUMA, J. M. «Spain, The Data Center Kingdom», *Colliers.* 5 de septiembre de 2022. Disponible en: https://www.colliers.com/en-es/news/el-reino-de-los-data-centers

en los últimos años gracias al desembarco de estos cables en su territorio, hasta el punto que se estima que el 70 % de los datos que lleguen a Europa lo harán a través de España[42].

Al comparar la capacidad de transmisión de datos de una y otra generación de cables (tabla 2) se aprecia la magnitud del cambio que se está produciendo y se pueden avanzar las consecuencias de esta transformación revolucionaria, que ofrece las condiciones necesarias para que la península ibérica se convierta en un nodo significativo de la red global.

[42] LORENZO, A. «Irene Cano, directora general de Meta España y Portugal: "España es el destino preferido por los empleados de Meta para trabajar a distancia"», *El Economista.* 14 de junio de 2022. Disponible en: https://revistas.eleconomista.es/digital/2022/junio/irene-cano-directora-general-de-meta-espana-y-portugal-espana-es-el-destino-preferido-por-los-empleados-de-meta-para-trabajar-a-distancia-LG11423228

Tabla 2. Capacidad de los cables submarinos internacionales en España y Portugal (en Tb/s)

Anterior generación de cables					Nueva generación de cables			
Cable	**Amarres**	**Año**	**Tb/s**		**Tb/s**	**Año**	**Amarres**	**Cable**
FLAG Europa - Asia	RU-Japón Estepona	1997	10		224	2018	Virginia (EUA) - Sopelana	Marea
SeaMeWe-3	Corea del Sur - Australia - RU Portugal	1999	4,6		40	2020	Orán - Valencia	ORVAL
Columbus III	Florida - Sicilia Azores	1999	0,32		100 (inicial)	2021	Brasil - Portugal Tenerife	EllaLink
SAT-3/ WASC	Portugal - Sudáfrica	2001	0,8		352	2022	N, York - Sopelana	Grace Hopper
Tata TGN	RU - Portugal Bilbao	2002	3,84		144	2023	Sudáfrica - Portugal Tenerife	Equiano
ALPAL-2	Mallorca - Argelia	2002	0,16		480	2023	RU - Barcelona Tenerife y Gran Canaria	2Africa
Main One	Portugal-Sudáfrica	2010	10		400	2023	Génova - Barcelona	Medloop
EIG	RU - India Portugal	2011	28		480	2024	Carolina del Sur-Santander	Anjana
WACS	RU - Sudáfrica Portugal	2012	14,5		480	2025	Egipto - Portugal Barcelona	Medusa
ACE	Francia - Sudáfrica Portugal	2012	12,8		480	2026	Carolina del Sur-Portugal	Nuvem

Fuente: Elaboración propia.

Puntos de aterrizaje

La llegada de una nueva generación de cables submarinos exige la creación de infraestructuras terrestres compatibles con la hiperescala de capacidad que proporcionan. Ello requiere la construcción de nuevas estaciones de amarre, del tendido de una nueva red terrestre de alta capacidad y, finalmente, la creación y ubicación de centros de datos en los nuevos nodos de interconexión. Todos estos elementos completan el «ecosistema» de infraestructuras digitales que hace funcional la nueva red global de cables submarinos: un proceso de transformación vertiginoso impulsado por un conjunto de empresas particularmente activas y con singular protagonismo internacional, en el que España se encuentra sumida en la actualidad.

El territorio español dispone de numerosos puntos de aterrizaje para cables submarinos, pero las diferencias entre estas instalaciones son tan notables como las que separan los cables de última generación de los anteriores. En el formato tradicional, el tráfico del cable submarino concluía en el punto de aterrizaje en la costa, donde se conectaba a la red terrestre para enlazar con el punto de presencia (*point of presence,* PoP) del operador, normalmente localizado en un gran centro urbano. La red terrestre era independiente del sistema submarino.

El extraordinario aumento de capacidad de la nueva generación de cables ha modificado esta estructura tradicional. El ancho de banda que permiten los nuevos repetidores de gran capacidad *(ultra-large repeater bandwidth)* y la reducción del espaciado entre canales permiten conectar los sistemas submarinos con los terrestres directamente a través de las estaciones de desembarco (*cable landing stations,* CLS)[43].

Tales avances han permitido la creación de sistemas integrados (submarino y terrestre) que ofrecen una conexión directa de PoP a PoP, reduciendo la latencia de forma considerable. Este sistema híbrido necesita, en consecuencia, una estación de desembarque adaptada, que no requiere de grandes dimensiones, pero sí de una fuente de energía suficiente para alimentar los repetidores bajo el mar y asegurar, además, su suministro autónomo en caso de accidente.

[43] COURTOIS, O. y BARDELAY-GUYOT, C. «Architectures and management of submarine networks», en CHESNOY, J. (ed.), *Undersea Fiber Communication Systems* (2.ª ed.). Academic Press, 2016, pp. 343-380. Disponible en https://doi.org/10.1016/B978-0-12-804269-4.00009-X

Los nuevos sistemas híbridos de conexión directa entre PoP constan de tres segmentos en su enlace entre el cable submarino y la red terrestre:

a) El registro de playa *(beach manhole),* una pequeña arqueta enterrada, situada en la misma playa, donde termina el cable submarino y se une a un cable terrestre.

b) El tramo terrestre, normalmente muy corto, enlaza la playa con la estación de aterrizaje del cable.

c) Y, finalmente, la propia estación, donde se alojan el repetidor terrestre y los equipos de alto voltaje que alimentan el cable submarino y donde se produce la conexión al sistema terrestre que llega directamente al PoP. En su entorno se localizan los centros de datos, aunque estos también tienden a situarse en las cercanías de grandes centros urbanos, que pueden encontrarse a centenares de kilómetros (fig. 10).

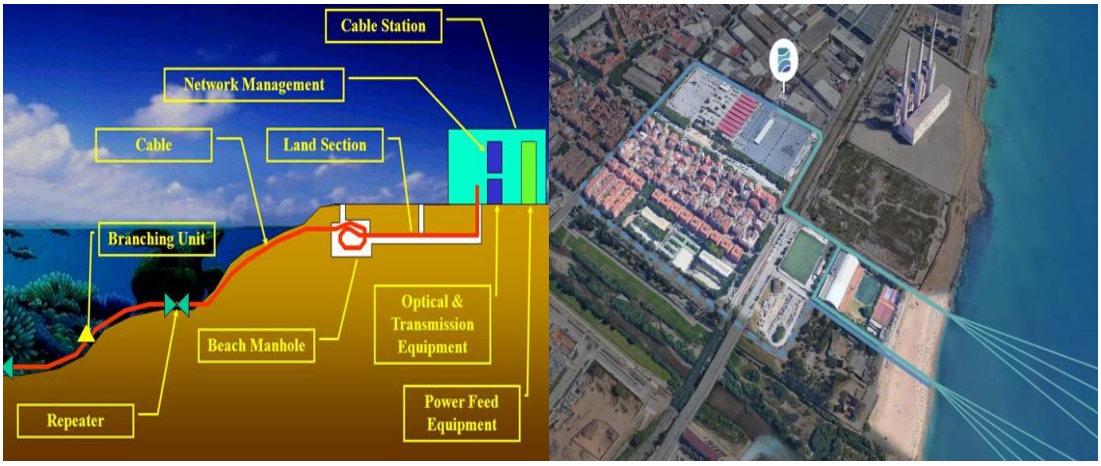

Figura 10. Esquema de tramo terrestre y localización de estación de desembarque
Fuente: https://barcelonacls.com/

En la península ibérica se han construido en los últimos años instalaciones de estas características para la conexión terrestre de los nuevos cables submarinos. En la costa cantábrica se encuentran en Sopelana, donde desembarcan los cables Marea y Grace Hoppe. Propiedad de Telxius, las citadas instalaciones están asociadas al centro de datos que esta misma compañía ha localizado en Derio, en las cercanías de Bilbao. En

el futuro, la estación de aterrizaje proyectada en Santander (Telxius) para acoger al cable Anjana también conectará con este centro.

Derio está concebido como un *hub* de comunicaciones que combina las funciones de una estación de amarre con las de un PoP internacional para prestar servicio a operadores, hiperescaladores y proveedores de contenidos, asegurando la conexión con las redes terrestres continentales que enlazan con los principales nodos europeos[44]. Se comunica también, de modo directo, con el centro de datos que Telxius posee en Virginia Beach (EE. UU.).

En la costa atlántica, la principal instalación se sitúa en Sines (Portugal), donde el tendido del nuevo cable Olisipo permite crear una región *cloud* que integra los puntos de aterrizaje de todos los cables que llegan a territorio continental portugués con los centros de datos.

En las islas Canarias destaca la estación de El Médano, propiedad de Canlink, cuya conexión con los nuevos sistemas Equiano y 2Africa está prevista. Esta se encuentra asociada al centro de datos D-ALIX, en Granadilla (Tenerife)[45].

En la costa mediterránea destaca la Barcelona Cable Landing Station (BCLS)[46], localizada en Sant Adrià de Besòs y propiedad de AFR-IX. Esta estación dispone de ocho puertos para recibir otros tantos cables submarinos[47] y de cuatro accesos distintos a las principales infraestructuras de telecomunicaciones de la ciudad. Sus instalaciones acogen un centro de control de la red (*network operation center,* NOC), desde donde se monitorizarán los cables de forma permanente para que no se produzcan incidencias y garantizar su seguridad.

También está planificada la construcción en el puerto de Alicante de una moderna estación de aterrizaje con capacidad para alojar cuatro cables submarinos y un centro de datos con 1,5 MW de potencia instalada. Medusa será el primer cable que albergue.

[44] TELXIUS. «Hub de comunicaciones Derio». Disponible en: https://telxius.com/
[45] En El Médano ya desembarcan los cables ACE, Atlantis 2-Pencan 6, Tegopa y Tenerife-Gran Canaria. Canalink (INSTITUTO TECNOLÓGICO Y DE ENERGÍAS RENOVABLES (ITER). Disponible en: https://www.iter.es/portfolio-items/canalink/).
[46] LA VANGUARDIA. «La Barcelona Cable Landing Station de Sant Adrià de Besòs ya tiene su primer cliente». 10 de enero de 2023. Disponible en: https://www.lavanguardia.com/local/barcelones-nord/20230110/8672854/barcelona-cable-landing-station-sant-adria-besos-primer-cliente.html
[47] Los desembarcos actuales son Medusa, en su derivación hacia Marsella; Medloop, directamente desde Génova, y 2Africa, el punto terminal de este gran anillo africano.

El proyecto tiene prevista su prolongación, mediante enlace terrestre, hacia Valencia y Madrid. El segmento submarino y el terrestre reciben el nombre común de Barracuda SCS[48].

Tanto en Sines como en Barcelona y El Médano-Granadilla, el proyecto se complementa con la instalación de plantas de generación de energía renovable[49] para satisfacer la alta demanda energética de los centros de datos. La combinación de conectividad con la red global y disponibilidad energética que ofrecen estas instalaciones les permite aspirar a convertirse en importantes puntos de localización de nuevos centros de datos.

La red terrestre

En la estructura de negocio tradicional, la explotación del cable submarino llegaba hasta la costa y la distribución de los datos por el territorio quedaba en manos de los socios locales, normalmente las compañías de telecomunicaciones tradicionales. Los nuevos cables, sin embargo, «se prolongan» tierra adentro, creando una continuidad física en la infraestructura cuyo destino final son los centros de datos. Para que ello sea posible, resulta necesaria la construcción de nuevas líneas terrestres de cable. Estas infraestructuras son desarrolladas, en la mayoría de los casos, por empresas especializadas, propietarias de las grandes redes troncales continentales y que en ocasiones se asocian con las compañías dueñas de los cables submarinos para su prolongación en tierra.

Las principales empresas de este sector con presencia en España son Exa, Colt y Telxius. En la figura 11 se muestran sus respectivas redes peninsulares.

[48] QIU, W. «VDPC to Build Barracuda Submarine Cable System and Cable Landing Station in Alicante». Submarine Cable Networks, 16 de abril de 2023. Disponible en: https://www.submarinenetworks.com/en/systems/asia-europe-africa/barracuda/vdpc-to-build-barracuda-submarine-cable-system-and-cable-landing-station-in-alicante

[49] 1,2 GW de generación fotovoltaica en Sines y 1,07 GW en Barcelona, y 10,5 MW de generación eólica en Granadilla.

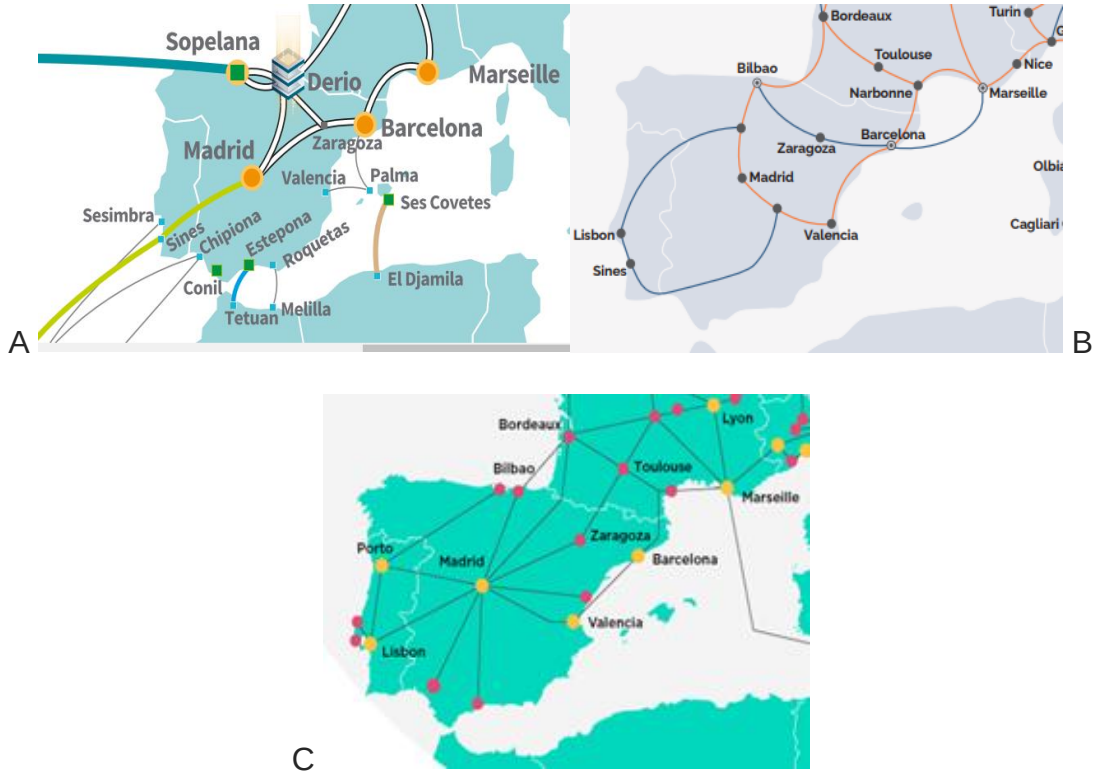

Figura 11. Redes terrestres de fibra óptica en la península ibérica
de las compañías Telxius (a), Exa (b) y Colt (c)
Fuente: https://telxius.com/network/Telxius_map.pdf; https://exainfra.net/media-centre/resources/exa-network-map/?gclid=Cj0KCQiAr8eqBhD3ARIsAIe-buMAzbViG4xvPlCcjAxThEtpr7KPP2uqM4aMo09oDgeaFD4KBjo_jp0aAnmaEALw_wcB; https://www.colt.net/es/our-network/coverage-maps/

Los centros de datos

Un centro de datos *(data center)* es una instalación que alberga los servidores físicos (o virtuales), conectados interna y externamente a través de redes de cable. Se trata de un espacio físico que sirve para almacenar, transferir y acceder a la información digital.

Los grandes centros de datos son las instalaciones nodales a través de las cuales se produce la interconexión de la red global de cables submarinos. En los últimos años, el número de estos centros ha crecido de forma significativa en los países del sur de Europa, convirtiéndose esta región en una alternativa a las localizaciones tradicionales en el continente, situadas en las ciudades de Fráncfort, Londres, Ámsterdam y París, conocidas como mercados FLAP (acrónimo de las iniciales de estas cuatro ciudades).

Los mercados FLAP han sido el punto de atracción dominante para la locación de los centros de datos, debido a la interconectividad que ofrecen, sus condiciones de mercado, la seguridad jurídica y la confiabilidad en el suministro energético. Si bien su capacidad

de atracción no manifiesta signos de debilidad, estas regiones enfrentan crecientes dificultades para satisfacer la demanda: escasez de terrenos adecuados para la construcción de nuevas instalaciones, precios elevados y falta de disponibilidad de energía renovable[50]. El resultado es que los plazos de construcción se alargan, la competencia por el suelo se recrudece y los costes se disparan. La creciente saturación permite explicar la emergencia que han experimentado otras regiones europeas como localización alternativa para estas instalaciones.

En este contexto, donde la península ibérica ocupaba una posición marginal hasta hace bien poco, España ha logrado adquirir una creciente importancia como punto de destino para la localización de centros de datos, debido a diversos factores[51]. El más determinante ha sido, sin duda, la conectividad ofrecida por los nuevos cables submarinos de última generación. La red que configuran estos cables convierte la Península en un destino favorable para la instalación de nuevos centros destinados a la prestación de servicio en el tráfico de datos entre Europa, América y África.

También hay que considerar la capacidad de nuestro país para ofrecer suministro eléctrico de generación renovable, en cumplimiento del objetivo europeo de reducir las emisiones de CO_2 en al menos un 55 % para 2030[52]. España ha logrado un extraordinario avance en este campo y podría alcanzar en 2023 el 50 % de la generación eléctrica total mediante energías renovables[53].

Los centros de datos son grandes consumidores de energía eléctrica, hasta el punto de que la unidad de medida que se ha adoptado para evaluar su capacidad es la potencia eléctrica que consumen. Se estima que el consumo medio de estas instalaciones supone cerca de 200 teravatios-hora por año. En la medida en que se prevé que sus necesidades de suministro eléctrico sigan creciendo, esta magnitud se elevará quince veces más en

[50] DATA CENTER DYNAMICS. «Are FLAP-D markets reaching saturation point and where's the next hot place to build?». 30 de noviembre de 2022. Disponible en: https://www.datacenterdynamics.com/en/broadcasts/building-at-scale-europe/2022/episode-3-ondemand/
[51] CBRE. *Data Centers en España. Informe 2021*. Disponible en: www.cbre.es/insights/reports/informe-data-centers-espana-2021
[52] CONSEJO EUROPEO. Pacto Verde Europeo, objetivo 55. Disponible en: https://www.consilium.europa.eu/es/policies/green-deal/fit-for-55-the-eu-plan-for-a-green-transition/
[53] RED ELÉCTRICA. «Las energías renovables podrían alcanzar el 50% del 'mix' de generación eléctrica en España en 2023» (nota de prensa). 23 de marzo de 2023. Disponible en: https://www.ree.es/es/sala-de-prensa/actualidad/nota-de-prensa/2023/03/las-energias-renovables-podrian-alcanzar-50porciento-del-mix-de-generacion-electrica-en-espana-en-2023

2030 y los centros de datos se convertirán en un elemento crítico de la red eléctrica al representar un 8 % de la demanda total[54].

Entre 2016 y 2021 los mercados FLAP duplicaron su capacidad instalada y alcanzaron de forma conjunta los 2000 MW, siendo Londres el nodo principal con 711 MW. La potencia instalada en España en la actualidad asciende a 113 MW, de los cuales 103 MW están localizados en el área metropolitana de Madrid. Se estima que en los próximos años se producirá un incremento medio anual del 43 %, lo cual permitiría a esta metrópoli alcanzar los 621 MW en 2026, registrando un crecimiento muy superior a la media estimada para los FLAP[55].

En 2021 el Reino Unido era el país europeo con más centros de datos (452), seguido de Alemania (443). España, con 122 centros, se sitúa entre los diez primeros países de Europa[56], destacando Madrid como principal nodo por delante de otras ciudades europeas como Dublín, Estocolmo, Milán, Varsovia o Zúrich, que también se han convertido en enclaves alternativos a los FLAP. El sector en España se encuentra en plena expansión. Se estima que atraerá una inversión directa superior a los 10.000 millones de euros hasta 2026, de los cuales más de un 60 % se localizarán en Madrid[57].

Esa preferencia por la capital se explica por su posición geográfica, por la conectividad ganada con la llegada de los nuevos cables submarinos y por la interconexión a través de la red terrestre que ofrece (fig. 12).

[54] RIBALTA, D. «¿Cómo se mide la eficiencia energética en un *data center*?», *Adam Blog*. 23 de enero de 2020. Disponible en: https://adam.es/blog/como-medir-eficiencia-energetica-data-center/#:~:text=%C2%BFC%C3%B3mo%20se%20calcula%20el%20PUE,IT%20dentro%20del%20data%20center

[55] JIMÉNEZ, M. «El sector del *data center* eleva a 6837 millones su inversión directa en nuevos centros en España hasta 2026», *Cinco Días.* 31 de marzo de 2022. Disponible en: https://cincodias.elpais.com/cincodias/2022/03/31/companias/1648738965_952353.html

[56] ESTATISTA. «Número de *data centers* en los países de Europa 2021». Disponible en: https://es.statista.com/estadisticas/1223845/centros-de-datos-en-los-paises-de-europa/

[57] MILLÁN ALONSO, S. «Madrid absorberá una inversión directa en centros de datos por más de 6120 millones», *Cinco Días.* 23 de mayo de 2023. Disponible en: https://cincodias.elpais.com/companias/2023-05-23/madrid-absorbera-una-inversion-directa-en-centros-de-datos-por-mas-de-6120-millones.html

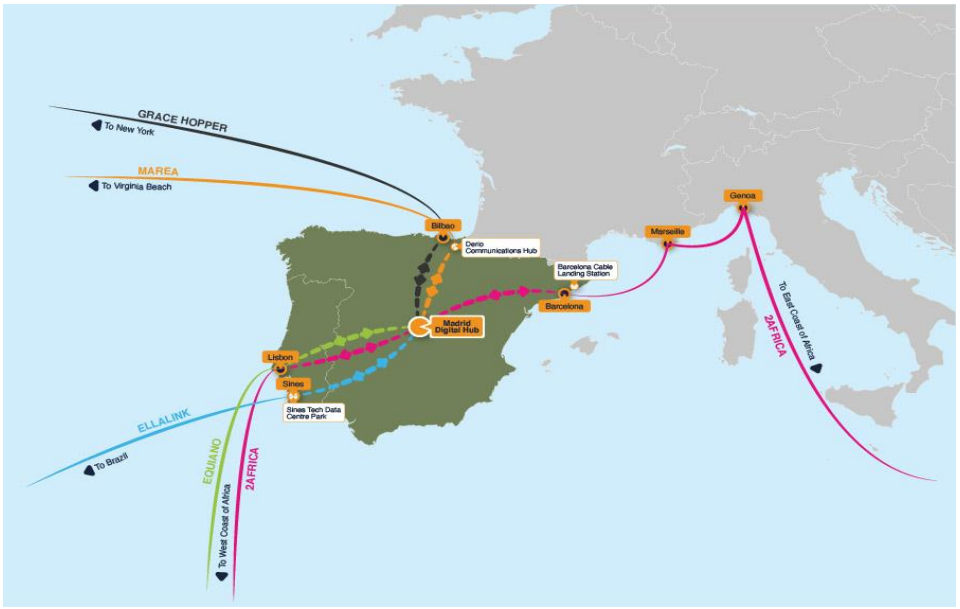

Figura 12. Conectividad de cables submarinos en la península ibérica
Fuente: https://www.interxion.com/es/blogs/2021/02/cables-submarinos-la-transformacion-digital-de-la-peninsula-iberica

Madrid se sitúa en el centro de un aspa que permite conectar las terminales de los puntos de aterrizaje de los principales cables submarinos que unen la Península con América del Norte, desde Sopelana (Vizcaya) —Marea y Grace Hopper— y próximamente también desde Santander —Anjana— y Sines —Nuvem—; América del Sur, desde Sines (Portugal) —Ellalink—; África, desde Lisboa —Equiano y 2Africa—, y el África índica y el Mediterráneo oriental —2Africa— a través de la conexión en Barcelona.

Gracias a la combinación de sistemas de cable submarino y terrestre que permiten las nuevas estaciones de desembarco, se consigue una comunicación directa de ciudad a ciudad o, lo que es lo mismo, de centro de datos a centro de datos. Tomemos como ejemplo el cable Ellalink. Este sistema permite enlazar Sao Paulo y Río de Janeiro con Lisboa y Madrid a través de una conexión directa cuyo destino final en la Península son tres áreas donde se concentran múltiples centros de datos: Sines, Lisboa y Madrid. Solo en esta última ubicación, un centro de datos, propiedad de la empresa Interxion, permite la conexión con más de 150 redes y proveedores de contenidos[58]. Todo ello con un nivel de latencia particularmente bajo.

[58] DATA CENTER MARKET (DCM). «El cable Ellalink establece su punto de interconexión en Madrid». 20 de octubre de 2020. Disponible en: https://www.datacentermarket.es/mercado/el-cable-ellalink-establece-su-punto-de-interconexion-en-madrid/

De esta forma, Madrid se ha convertido en un gran puerto de interconexión donde convergen los cables submarinos de gran capacidad que alcanzan las costas peninsulares. Esta localización privilegiada ha determinado que las grandes compañías tecnológicas hayan elegido el centro de la Península para instalarse: Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM y Meta (esta última en Talavera de la Reina), así como Oracle, que también ha elegido Madrid para instalar una de las dos bases (la otra se encuentra en Alemania) de su denominada «nube soberana europea» en asociación con Telefónica[59]. Al igual, grandes proveedores de contenido, como Netflix o Disney, han decidido establecer sus centros en el centro peninsular[60].

Estas grandes empresas tecnológicas han elegido el área metropolitana de Madrid para establecer sus centros creando con ello una región *cloud*, esto es, un conjunto de centros de datos desplegados dentro de un área geográfica limitada que actúan de forma independiente y que están interconectados a través de una red regional, lo cual les permite disponer de una latencia muy baja en la transferencia de datos.

La llegada de la nueva generación de cables submarinos ha favorecido el crecimiento del número de centros de datos en nuestro país y ha reforzado la posición regional de los puntos neutros de intercambio (*internet exchange point*, IXP) ya instalados[61].

Desde 2016, el ancho de banda del sur de Europa ha triplicado su capacidad[62]. Y seguirá creciendo a mayor ritmo cuando entren en servicio los cables de alta capacidad en construcción. Estos desarrollos han convertido a la península ibérica en un nodo estratégico de interconexión en la red global y abren la posibilidad de que pueda convertirse en un *hub* que ofrece nuevas rutas y una interconexión creciente, diversificada y de baja latencia.

[59] EUROPA PRESS. «Oracle implantará en España una de las dos regiones de su nube soberana europea de la mano de Telefónica». 15 de junio de 2023. Disponible en: https://www.europapress.es/economia/noticia-oracle-implantara-espana-dos-regiones-nube-soberana-europea-mano-telefonica-20230615131012.html
[60] INTERXION. «En Madrid no hay playa, pero hay puerto digital». 6 de julio de 2022. Disponible en: https://www.interxion.com/es/blogs/2022/07/madrid-puerto-digital
[61] Los puntos neutros son centros a través de los cuales los proveedores de servicios de internet intercambian datos entre sus respectivas redes. Los principales centros en España son ESpanix, DE-CIX, CATnix y Nixval.
[62] TELEGEOGRAPHY. «The Interconnection Landscape in Southern Europe». 2021. Disponible en: https://www.de-cix.net/en/resources/white-papers/the-southern-european-interconnection-landscape

Los cables submarinos en los documentos estratégicos de España y la protección de las redes terrestres

Pese a tratarse de una infraestructura crítica relevante, la reflexión estratégica de España sobre los cables submarinos es reciente y fragmentada: el país no dispone de una visión integral sobre su seguridad que contemple las partes tanto «húmeda» como «seca» de los sistemas, ni su indudable aportación a la prosperidad y riqueza nacional. En todo caso, esta situación no constituye ninguna excepción con respecto a los países de nuestro entorno y guarda relación con la «invisibilidad» en la que ha permanecido la red de cable submarino hasta que la OTAN llamó la atención sobre su seguridad a finales de 2020.

Puede afirmarse que la atención estratégica prestada a los sistemas de cables submarinos se ha centrado hasta fechas recientes en la protección de las infraestructuras físicas en tierra, la integridad de la red de comunicaciones y la ciberseguridad, con un tratamiento disperso que requiere de una perspectiva integrada.

Comencemos por analizar los documentos estratégicos españoles[63]. La primera referencia relevante a los cables submarinos se produce en 2013 en la Estrategia de Seguridad Marítima Nacional (p. 14), donde son mencionados en una relación de los intereses nacionales en el ámbito naval que deben ser atendidos. Pero en la Estrategia de Seguridad Nacional de ese mismo año no se incluye referencia alguna, aunque sí que se habla sobre ellos en la actualización de 2017 de este mismo documento, donde los cables son mencionados en relación con la vulnerabilidad del espacio marítimo a propósito del tráfico de información digital (p. 66). Hasta la versión de 2021, la Estrategia de Seguridad Nacional no prestará una atención específica a la seguridad de los cables submarinos frente a los ataques cibernéticos (p. 33) y para preservar la integridad física de la infraestructura (p. 62).

En los informes anuales de Seguridad Nacional se aprecia una secuencia temporal semejante. Los cables submarinos aparecen mencionados por primera vez en la edición de 2017, en el apartado correspondiente a la seguridad marítima, primero para categorizar la protección de los cables submarinos como un reto genérico para la

[63] Los documentos citados a continuación están disponibles en la página del Departamento Nacional de Seguridad (DNS) de Presidencia del Gobierno: https://www.dsn.gob.es/es/estrategias-publicaciones

seguridad (p. 57) y, a continuación, para destacar la relevante atención mostrada por el G7. Vuelven a ser mencionados los cables submarinos en la edición de 2020. Primero asociados a las amenazas de potenciales ataques cibernéticos (p.124), pero también al hablar de la responsabilidad del Estado en la protección de los espacios de soberanía (p. 150). En la edición del *Informe de Seguridad Nacional* de 2021 vuelve a haber una referencia, que destaca su relevancia estratégica en las comunicaciones y los tráficos financieros (p. 123). Pero será en la edición de 2022, con la guerra de Ucrania ya iniciada, cuando el número de referencias se multiplique (pp. 9, 55, 109 y 112). A las amenazas identificadas se le suman los efectos de la competencia geopolítica. El texto, haciéndose eco del informe del Parlamento Europeo, reclama una actuación colectiva para mejorar «la gobernanza europea de la protección y la resiliencia de los cables»[64].

La creciente preocupación por la red de cables submarinos queda reflejada en la Estrategia de Seguridad Marítima de la Unión Europea revisada y su Plan de Acción, recientemente aprobados por el Consejo en octubre de 2023[65], documentos a los que deberá seguir, posiblemente antes de concluir 2023, la Estrategia Nacional de Seguridad Marítima de España[66], donde sin duda se recogerán las líneas estratégicas definidas a escala europea. La UE identifica seis «objetivos estratégicos» y fija una línea de acción «clave» con el propósito de «aumentar la resiliencia y la protección de las infraestructuras marítimas críticas, como gasoductos, cables submarinos, puertos, instalaciones de energía en alta mar y terminales de gas natural licuado (GNL) presentes en todas las cuencas marítimas de la UE, así como intensificar la cooperación en el desarrollo de un plan regional de vigilancia de las infraestructuras submarinas y en alta mar»[67].

[64] BUEGER, Ch., LIEBETRAU, T. y FRANKEN, J. *Op. cit.*, p. 9.
[65] UNIÓN EUROPEA. Consejo de Asuntos Generales. 24 de octubre de 2023. Disponible en: https://www.consilium.europa.eu/es/meetings/gac/2023/10/24/
[66] Así fue aprobado por el Consejo Nacional de Seguridad Marítima (DEPARTAMENTO DE SEGURIDAD NACIONAL. Reunión del Consejo Nacional de Seguridad Marítima. 10 de noviembre de 2022. Disponible en: https://www.dsn.gob.es/gl/actualidad/sala-prensa/reuni%C3%B3n-del-consejo-nacional-seguridad-mar%C3%ADtima-4).
[67] CONSEJO EUROPEO / CONSEJO DE LA UNIÓN EUROPEA. «Seguridad marítima: el Consejo aprueba la Estrategia revisada de la UE y el Plan de Acción» (Comunicado de prensa). 24 de octubre de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/10/24/maritime-security-council-approves-revised-eu-strategy-and-action-plan/#

Este Plan de Acción viene a reforzar las recomendaciones emitidas por el propio Consejo a finales de 2022[68]. El documento reconoce la necesidad de que los Estados realicen evaluaciones de riesgo específicas para los cables submarinos y valoren las opciones disponibles para mitigar esos riesgos (II.10). También se invita a la Comisión a que realice un estudio «exhaustivo» para cartografiar sus capacidades y duplicaciones, identificar sus puntos vulnerables, las amenazas y los riesgos para la disponibilidad de los servicios y evaluar el impacto de la interrupción en el funcionamiento de los cables submarinos transatlánticos para los Estados miembros y la Unión en su conjunto (II.21a). Obviamente, manteniendo esta información protegida, dada la sensibilidad de los datos. Finalmente, se recomienda a los Estados que «sean conscientes» de la necesidad de cooperar con «proveedores y socios de confianza» en el tendido y mantenimiento de los cables y de planificar la sustitución de los sistemas de mayor antigüedad para garantizar la prestación del servicio (III.27).

Por parte de la UE estas recomendaciones ya se han empezado a aplicar. La Agencia de Ciberseguridad de la UE ha publicado un informe[69] sobre la seguridad de los cables submarinos. Aunque en él se reconoce que apenas existen evidencias sobre ataques deliberados contra los sistemas de cables, se recomienda realizar un seguimiento de las actividades marítimas civiles, identificando comportamientos anómalos a través de la vigilancia naval, tanto submarina como en superficie, para prevenir posibles ataques físicos y ciberataques. Destacan también en el informe la vulnerabilidad de los puntos de estrangulamiento, donde se concentran un gran número de cables (como son los puntos de desembarco), y la alerta sobre las limitadas capacidades de reparación con las que se cuenta en caso de un sabotaje a gran escala.

A la vista de este despliegue normativo, puede afirmarse que los Estados europeos y, en general, los aliados de la OTAN han identificado los cables submarinos como una vulnerabilidad estratégica y están poniendo los medios necesarios para protegerla convenientemente. Desde el sabotaje al Nord Stream, la OTAN ha intensificado las

[68] CONSEJO DE LA UNIÓN EUROPEA. «Recomendación del Consejo de 8 de diciembre de 2022 sobre un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas (2023/C 20/01)», *Diario Oficial de la Unión Europea,* C 20/2. 20 de enero de 2023.
[69] ENISA. «Subsea Cables – What is at Stake?». European Union Agency for Cybersecurity, 2023. Disponible en: https://www.enisa.europa.eu/publications/undersea-cables

patrullas en el mar Báltico con vuelos de vigilancia y reconocimiento marítimo, aviones AWACS, drones y una flota de cuatro cazaminas[70].

Esta reciente atención se corresponde con una preocupación por asegurar la protección integral de los sistemas de cables, incluyendo la hasta ahora desatendida zona «húmeda». La parte correspondiente a la infraestructura física de la llamada zona «seca» sí ha recibido una atención específica (aunque insuficiente) desde comienzos de siglo, tras los atentados de 2001 en Estados Unidos y de 2004 en Madrid. En el caso de España, resulta necesario, y urgente, que los sistemas de cables submarinos reciban una consideración formal en tanto «infraestructura crítica»[71].

La protección de las instalaciones consideradas como «críticas» se encuentra regulada por la Ley 8/2011 (que traspone la Directiva 2008/114/CE del Consejo, sobre identificación y designación de infraestructuras críticas europeas) y el Real Decreto 704/2011, de 20 de Mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas[72], donde se identifican doce sectores estratégicos[73] y se crea un Catálogo Nacional de Infraestructuras Estratégicas[74], de carácter secreto.

La protección de estas instalaciones corresponde a los denominados «agentes críticos», que forman parte del Sistema Nacional de Protección de las Infraestructuras Críticas, coordinado desde el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Entre ellos se encuentran los «operadores críticos», que son las entidades u

[70] OTAN. «NATO steps up Baltic Sea patrols after subsea infrastructure damage». 19 de octubre de 2023. Disponible en: https://www.nato.int/cps/en/natohq/news_219500.htm.
[71] La Ley 8/2011 define las «infraestructuras críticas» como aquellas «infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales» (Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas, *BOE,* n.º 102, de 29 de abril de 2011).
[72] Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, *BOE,* n.º 345, de 23 de diciembre de 2008; Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el reglamento de protección de las infraestructuras críticas, *BOE,* n.º 121, de 21 de mayo de 2011.
[73] Administración, alimentación, energía, espacio, sistema financiero y tributario, agua, industria nuclear, industria química, instalaciones de investigación, salud, transporte y tecnologías de la información y las comunicaciones (CARO BEJARANO, M. J. «La protección de las infraestructuras críticas» [Documento de Análisis IEEE, 21/2011]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf).
[74] El Catálogo Nacional de Infraestructuras Estratégicas es el registro administrativo que contiene información completa sobre todas las infraestructuras estratégicas ubicadas en el territorio español. Se nutre de la información que los operadores de infraestructuras facilitan al Centro Nacional para la Protección de las Infraestructuras Críticas (Ley 8/2011, art. 4).

organismos (tanto del sector público como privado) responsables de las inversiones o del funcionamiento diario de la instalación, red o sistema (Ley 8/2011, art. 2.m). Estos operadores se encargan de la elaboración de los Planes de Seguridad del Operador y de los planes de protección específicos de sus empresas, además de prestar asistencia técnica a la Secretaría de Estado de Seguridad[75].

Dentro de este marco normativo, disponemos desde 2017 de un Plan Estratégico Sectorial de las Tecnologías de la Información y de la Comunicación[76], donde no se mencionan los cables submarinos. Se trata de un plan único que incluye los múltiples servicios que engloban las TIC: telecomunicaciones, comunicación audiovisual e informática y sociedad de la información. Pese a prestar servicios diferenciados, los tres subsectores se interconectan a través de las redes de telecomunicaciones, que son comunes y transversales a todos ellos. Desde la perspectiva que adopta el Plan Estratégico Sectorial, la infraestructura de redes no es considerada como un subsector específico, sino que es englobada en el conjunto de elementos físicos íntimamente relacionados con los agentes que participan en el sector de las TIC.

En el tercer capítulo del plan se efectúa un análisis estratégico del conjunto de amenazas potenciales que suponen un riesgo para la tipología de infraestructuras identificadas como básicas en la provisión de servicios esenciales, y se incluye un mapa de vulnerabilidades. El cuarto capítulo ofrece una orientación sobre las medidas estratégicas (organizativas, técnicas, de continuidad de operación y de recuperación ante desastres) que pueden adoptarse para mitigar el riesgo y alcanzar un óptimo nivel de protección de las infraestructuras que asegure la continuidad en la provisión de servicios tras un eventual incidente de carácter deliberado.

Resulta absolutamente necesario que una futura revisión de este plan incluya, con la atención apropiada, la protección debida de los sistemas de cables submarinos.

En lo referente a la dimensión cibernética, la atención a los sistemas de cable ha seguido unas pautas semejantes. En la Estrategia Nacional de Ciberseguridad de 2019 tampoco

[75] Cada operador debe designar a un responsable de seguridad, que sirva de enlace con la Secretaría de Estado de Seguridad, y un delegado de seguridad, que cumpla como enlace operativo y de información con las autoridades competentes en todo lo referente a la seguridad concreta de la infraestructura crítica (RD 704/2011, arts. 34.2 y 35).
[76] SICILIA SAN JOSÉ, M. «Plan estratégico sectorial de las tecnologías de la información y de la comunicación», *Seguritecnia,* n.º 448. 2017, pp. 50-54. Disponible en: https://www.seguritecnia.es/revistas/seg/448/54/index.html

son mencionados los cables de forma explícita, aunque quedan englobados en la denominación genérica de «infraestructura digital», atendiendo a la ciberseguridad de las «redes y sistemas de información». Los cables submarinos se incluyeron por primera vez en dos disposiciones de la nueva Ley General de Telecomunicaciones[77] de 2022: artículo 6.9 (comunicación al MINECO de todo proyecto de instalación y explotación de nuevos cables informando sobre su titular, gestor, trazado y principales características)[78] y disposición adicional 23.ª (establecimiento de un plazo de dos meses para presentar esta información sobre cables ya instalados).

Aparte de las cuestiones relativas a la preservación de su integridad y seguridad, los sistemas de cables submarinos han entrado en la planificación estratégica de desarrollo económico y reciben una atención específica dentro de la Agenda Digital 2030, desarrollada por el Ministerio de Asuntos Económicos y Transformación Digital (MINECO)[79]. La agenda España Digital es una estrategia, iniciada en 2020, para lograr la transformación digital del país, aprovechando el potencial que incorporan las nuevas tecnologías con el fin de impulsar el crecimiento económico. En su primer año de funcionamiento se hizo público el Plan para la Conectividad y las Infraestructuras Digitales[80], donde las infraestructuras digitales de carácter transfronterizo, los puntos de intercambio de tráfico de internet, los centros de datos y los cables submarinos adquieren un protagonismo singular. En este último caso, se promueve la participación de empresas españolas en consorcios internacionales para lograr la incorporación del país a las rutas alternativas de interconexión global que deriven en el amarre de nuevos cables submarinos en España (p. 65). Además, se favorecerá la obtención de fondos europeos del programa de financiación para interconexiones transnacionales de

[77] Ley 11/2022, de 28 de junio, General de Telecomunicaciones, *BOE,* n.º 155, de 29 de junio de 2022.
[78] Los datos a aportar por los titulares y gestores de los cables están especificados en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación (*BOE,* n.º 76, de 30 de marzo de 2022).
[79] MINECO. *España Digital 2026*. 2023. Disponible en: https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital.aspx
[80] MINECO. «Plan para la conectividad y las infraestructuras digitales de la sociedad, la economía y los territorios», Agenda Digital 2030. 2020. Disponible en: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210129_Plan_Conectividad.pdf

infraestructuras de datos y cable submarino CEF-2 (Connecting Europe Facility)[81], teniendo como objetivo privilegiado las conexiones con Portugal[82].

Con carácter general, puede concluirse que carecemos de un marco jurídico específico para la gestión, protección y seguridad de los cables submarinos. Se ha asumido, y aplicado, una perspectiva centrada en la ciberseguridad, consecuencia de las múltiples evidencias sobre ciberataques cometidos en las últimas décadas por agentes estatales y privados. Pero el ciberespacio, como recurso de poder y nuevo dominio de competencia estratégica, no es una entidad abstracta, requiere necesariamente del soporte de múltiples elementos físicos, entre ellos los cables submarinos: infraestructuras físicas que pertenecen a actores públicos y privados y que pueden ser objeto de actos criminales o de espionaje, o convertirse en objetivo militar en caso de guerra. Sin un marco legal eficaz, nacional e internacional, que regule los sistemas de cable submarino, sin un reconocimiento formal en tanto que «infraestructura crítica», sin una visión estratégica integrada que tenga la seguridad nacional como principio rector, resulta muy difícil garantizar la seguridad de los datos que se transmiten y la propia integridad de la infraestructura.

La responsabilidad de España en la protección y seguridad de los cables submarinos

Los cables submarinos tienen un tratamiento jurídico complejo y, una vez más, fragmentado. Los cables submarinos, incluso aquellos de propiedad estatal destinados a la defensa y que son utilizados para trasladar información reservada, carecen de

[81] La segunda generación de este programa (2021-2027) tiene como objetivo apoyar las inversiones en infraestructuras de conectividad digital de interés común. El programa cuenta con un presupuesto de 2065 millones de euros (EUROPEAN CLIMATE, INFRASTRUCTURE AND ENVIRONMENT EXECUTIVE AGENCY. Connecting Europe Facility 2021-2027 Adopted. 2021. Disponible en: https://cinea.ec.europa.eu/news-events/news/connecting-europe-facility-2021-2027-adopted-2021-07-20_en).

[82] Ambos países «avanzarán en la constitución de una alianza en el ámbito de las infraestructuras digitales transfronterizas de datos, incluyendo centros de proceso de datos y cables submarinos, fortaleciendo la posición de la península ibérica como hub de interconexión digital del sur de Europa» (XXXI CUMBRE HISPANO-PORTUGUESA. «Declaración conjunta». 10 de octubre de 2020, párr. 39. Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/Declaracio%cc%81n_XXXI_Cumbre_Hispano_portuguesa.pdf).

inmunidad soberana[83]. Esto se traduce, sencillamente, en que fuera de las áreas marítimas bajo jurisdicción nacional las intervenciones físicas de los cables submarinos para recoger los datos transmitidos a través de ellos (denominadas operaciones de extracción) «no constituyen una violación de la soberanía»[84]. Además, dado que los cables submarinos pasan a través de aguas internacionales, no pueden ser protegidos exclusivamente por la legislación nacional de un Estado, ni por sus Fuerzas Armadas[85].

El régimen jurídico internacional de los cables se regula a través de dos convenios: la Convención para la Protección de Cables Submarinos Telegráficos de 1894, aún en vigor y que cuenta con 36 Estados parte[86], y la Convención de las Naciones Unidas sobre el Derecho del Mar (CONVEMAR)[87]. En particular, esta última reconoce el principio consuetudinario de «mar abierto»[88], estableciendo en alta mar la libertad de navegación, sobrevuelo, pesca, construcción de islas artificiales, investigación científica y, específicamente, la libertad de tendido de cables y tuberías submarinas en el lecho del océano, asumiendo la obligación de no afectar a los cables y tuberías instalados por otros Estados previamente (art. 112). Los artículos 113 y 114 se refieren a la ruptura o deterioro de un cable submarino y el artículo 115 establece el derecho de indemnización por las pérdidas causadas cuando se provocan daños a dichos cables. Esta es la atención que reciben los cables en la convención. Además, las entidades a las que se reconocen esas libertades y obligaciones son exclusivamente los Estados, únicos sujetos de derecho internacional, cuando el «ecosistema» actual de los cables submarinos es mucho más complejo y está integrado por agentes de naturaleza diversa, predominantemente privados[89]: una pluralidad de actores que deberían ser tomados en

[83] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. *Strategic importance of, and dependence on, undersea cables*. Noviembre de 2019, p. 5. Disponible en: https://www.ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.
[84] «Tapping operations beyond waters subject to the sovereignty of the coastal or archipelagic State do not constitute a violation of sovereignty» (SCHMITT, M. N. [ed.]. «Commentary to *Rule* 54 ¶ 17»,*Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013, p. 257. Disponible en: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf). No obstante, la regla 45 establece como principio: «Cyber operations on the high seas may only be carried out for peaceful purposes, unless otherwise provided by international law».
[85] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. *Op. cit.*, pp. 1-2.
[86] International Convention on the Protection of Submarine Cables, with additional Article. Disponible en: https://verdragenbank.overheid.nl/en/Verdrag/Details/001885.html
[87] NACIONES UNIDAS. Convención sobre el Derecho del Mar. 1982. Disponible en: https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf
[88] «La alta mar está abierta a todos los Estados, sean ribereños o sin litoral» (CONVEMAR, art. 87.1).
[89] SUNAK, R. *Undersea Cable: Indispensable, Insecure*. Policy Exchange, Londres, 2017, p. 9. Disponible en: https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

consideración si se pretende construir un régimen de gobernanza internacional para los cables.

Resulta evidente que ni CONVEMAR, ni el Convenio de 1894 y menos aún el Manual de Tallin constituyen instrumentos jurídicos suficientes para cumplir con esa función. Urge, por tanto, establecer un convenio internacional específico para proteger y regular estas infraestructuras submarinas convenientemente y explorar las posibilidades que ofrecen los acuerdos técnicos, bilaterales o multilaterales, que puedan celebrarse en materia de defensa. Sin un marco legal eficaz que regule los cables submarinos, va a ser muy difícil asegurar la integridad de los datos que se transmiten a través de ellos y, en definitiva, garantizar la propia infraestructura.

A la vista del régimen jurídico internacional en vigor, el tendido de cables submarinos en alta mar, sean de titularidad pública o privada, solo se encuentra sometido en la práctica a la obligación de no afectar en su trazado a otros cables existentes. En el caso de la zona económica exclusiva y plataforma continental de un Estado, se deberán respetar además las disposiciones legales de ese Estado para la protección de sus recursos naturales. El Estado solo tiene plenos derechos soberanos sobre los recursos referidos en estas zonas marinas, el mar territorial, las playas y la zona marítimo-terrestre. Todos ellos tienen consideración de «bien de dominio público» (art. 132, Constitución Española). En consecuencia, la instalación de un cable submarino en las últimas zonas mencionadas sí requiere de concesión administrativa, y las tareas de tendido, reparación y retirada, de las preceptivas autorizaciones[90]. Además, en la medida en que tales actividades se desarrollan en el mar, el buque que las realice deberá contar con los permisos de navegación correspondientes[91]. En la zona de tierra, colindante con la ribera del mar, para la construcción de canalizaciones y de los registros de playa, también será necesario respetar la servidumbre de paso que establece la Ley de Costas, y se deberá contar con las autorizaciones de la administración estatal o autonómica correspondiente[92].

[90] Ley 22/1988, de 28 de julio, de Costas, *BOE,* n.º 181, de 29 de julio; Real Decreto 876/2014, de 10 de octubre, por el que se aprueba el Reglamento General de Costas, *BOE,* n.º 247, de 11 de octubre.
[91] Ley 14/2014, de 24 de julio, de Navegación Marítima, *BOE,* n.º 180, de 25 de julio; Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, *BOE,* n.º 253, de 20 de octubre.
[92] PARDAVILA, B. y LLUCH, L. «Cables submarinos de telecomunicaciones: aproximación a su régimen jurídico en España», *Actualidad Administrativa*, n.º 7-8. 2022.

Como se observa, la responsabilidad directa del Estado solo puede ejercerse sobre aquellas áreas bajo su soberanía, pero los cables representan un dominio único sin interrupción que atraviesa áreas bajo jurisdicción de varios Estados y amplias zonas de aguas internacionales, donde no se les aplica el principio de inmunidad, como sí ocurre con los buques de Estado. Además, la vulnerabilidad que representa esta situación, bien sea por el acceso al tráfico de datos o por la inseguridad de la propia infraestructura, no queda limitada únicamente a los Estados con los que enlaza el cable, sino que se extiende a múltiples territorios, con diferente intensidad, debido a la estructura en red[93].

Dado el peso del sector privado en el negocio del cable, la seguridad de las redes recae fundamentalmente bajo la responsabilidad de las empresas propietarias o gestoras de los sistemas. Los centros de operaciones y supervisión de la red (*network operations centers,* NOC) constituyen el elemento principal para cumplir con esa función. El Estado puede desarrollar una estrecha cooperación con los centros, pero, en última instancia, su autoridad quedará limitada a imponer una cierta visión estratégica conjunta sobre la gestión de estos, que tenga la seguridad nacional como principio rector.

El objetivo expuesto no siempre podrá lograrse por la dependencia existente de la tecnología y las inversiones de las grandes compañías tecnológicas estadounidenses (conocidas bajo el acrónimo GAFAM)[94], propietarias únicas de los sistemas de cable de última generación que están enlazando con la península ibérica. El modelo de negocio de los cables submarinos ha cambiado en los últimos años de forma radical. Las empresas proveedoras de contenidos, hasta hace poco los principales clientes de la infraestructura, se han convertido en los propietarios de los nuevos sistemas de cables de última generación. Ello ha dejado a las compañías tradicionales de telecomunicaciones en una posición marginal dentro del mercado del cable submarino. Las GAFAM concentran la mayor parte de la inversión mundial en redes de cables submarinos de los últimos años, a través de consorcios empresariales muy reducidos *(club-cables),* integrados por una o dos de estas compañías, y ocasionalmente con alguna telecom local, que actúa como *landing-partner* en el punto de conexión con la costa (Telxius-Telefónica, en el caso de España). La elección de estos socios locales

[93] SCHMITT, M. N. *Op. cit,* p. 18.
[94] GAFAM: Google, Amazon, Facebook, Apple y Microsoft.

está determinada por las circunstancias específicas de cada caso, pero la tendencia es que desaparezcan del negocio[95].

El impacto de las GAFAM en el sector del cable submarino está siendo revolucionario: tiende a eliminar a los operadores tradicionales e integra la gestión marítima y terrestre de cable, reestructurando la red a través de los centros de datos, de los cuales también son propietarias. ¿Puede imponer el Estado su autoridad en defensa del interés nacional en estas circunstancias?

Resulta absolutamente legítima y oportuna la preocupación mostrada por la OTAN con respecto a las acciones maliciosas que puedan llevar a cabo tanto China como Rusia sobre la red de cables submarinos. Pero no podemos olvidar que las amenazas a la seguridad nacional de los Estados europeos, y no solo de ellos, proceden también de otros actores, incluidos nuestros aliados más próximos.

Desde las revelaciones ofrecidas por Edward Snowden en 2013, algunas de las cuales contenían información explícita sobre la intervención de cables submarinos[96], no podemos llevarnos a engaño sobre la magnitud y alcance del espionaje estadounidense con respecto a sus propios socios y aliados. Estados Unidos es el mayor actor en la red de cables. La mayor parte de los datos que transitan por ella pasan por su territorio en algún momento antes de llegar a su destino final, pudiendo ser monitoreados, interceptados o extraídos en cualquier parte de la ruta. En Europa, el conocimiento de estos hechos provocó una reacción inmediata por parte de la Comisión, que llegó a amenazar con suspender los acuerdos de transferencia de datos[97].

La práctica seguida por los Estados Unidos, el espionaje sistemático y a gran escala de sus socios de la OTAN, cuenta con múltiples antecedentes sólidamente documentados[98].

---

[95] MOREL, C. *Les câbles sous-marins. Enjeux et perspectives au XXIe siècle*. CNRS Editions, París, 2023, p. 66.
[96] CHIRGWIN, R. «Snowden doc leak lists submarine'd cables tapped by spooks», *The Register.* 24 de noviembre de 2014. Disponible en: https://www.theregister.com/2014/11/26/snowden_doc_leak_lists_all_the_compromised_cables/
[97] EMMOTT, R. «Brazil, Europe Plan Undersea Cable to Skirt U.S. Spying». Reuters, 24 de febrero de 2014. Disponible en: https://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224
[98] PIODI, F. y MOMBELLI, I. *The ECHELON Affair. The EP and the global interception system 1998-2002*. European Parliamentary Reserch Service, 2014. Disponible en: https://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf
MILLER, G. «The Intelligence Coup of the Century», *The Washington Post.* 11 de febrero de 2020. Disponible en: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

La guerra de Ucrania ha cambiado radicalmente el tono y la percepción europea sobre estos hechos, pero las tensiones que han provocado en la relación euroatlántica aún se evidenciaban al inicio de la actual presidencia de Joe Biden[99]. No puede darse por hecho que estas viejas prácticas de espionaje hayan desaparecido, ni mucho menos. Con toda probabilidad, los temores que manifiestan las autoridades estadounidenses hacia la posible interferencia de China en las redes de cable se deban a que disponen de un conocimiento experto sobre las posibilidades de espionaje que ofrecen las nuevas tecnologías[100] para extraer información de inteligencia de semejante cantidad de datos[101]. Pretender confiar en la ejemplaridad del comportamiento internacional de Estados Unidos[102] y en la autorregulación de la red no parece ser la mejor opción que puedan contemplar los Estados europeos.

Conclusiones y recomendaciones

La llegada de los nuevos sistemas de cables submarinos de última generación a la península ibérica ha trasformado —podría decirse, revolucionado— la posición internacional de España y Portugal en la red global de telecomunicaciones. Existe la posibilidad real de que nos convirtamos en un nodo relevante en los flujos que transitan entre África, América, Europa y Oriente Medio. Esta transformación va a tener un impacto económico y tecnológico de primera magnitud sobre nuestra estructura productiva, un cambio de alcance estratégico que afecta no solo a nuestro territorio, sino también al entorno de interacción más frecuente con el que nos conecta la red. Esta nueva situación obliga a España a adoptar las medidas necesarias para garantizar la integridad de la infraestructura y la seguridad de la información que transita por ella, a través de acciones

[99] CERULUS, L. y BURCHARD, H. v. d. «Snowden's back: Spying scandal clouds EU-US ties ahead of Biden visit», *Politico.* 31 de mayo de 2021. Disponible en: https://www.politico.eu/article/edward-snowden-is-back-spying-scandal-disrupts-eu-us-ties-ahead-of-joe-biden-europe-visit/
[100] WALTON, C. «China Will Use Huawei to Spy Because So Would You», *Foreign Policy*. 14 de julio de 2020. Disponible en: https://foreignpolicy.com/2020/07/14/britain-boris-johnson-china-will-use-huawei-to-spy-because-so-would-you/
[101] Se ha especulado con la imposibilidad de gestionar el enorme volumen de datos obtenidos para lograr información de inteligencia, pero parece que es factible (MACASKILL, E. *et al.* «GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications», *The Guardian.* 21 de junio de 2013. Disponible en: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa).
[102] FARRELL, H. y FINNEMORE, M. «The End of Hypocrisy: American Foreign Policy in the Age of Leaks», *Foreign Affairs.* Noviembre-diciembre de 2013. Disponible en: https://www.foreignaffairs.com/articles/united-states/2013-10-15/end-hypocrisy

que pueda llevar a cabo de forma autónoma, pero promoviendo también una estrecha cooperación con sus socios y aliados. España no parte de cero en la tarea, pero deberán adoptarse nuevas actuaciones, que habrán de implementarse en distintos niveles.

En el plano interno deberán aplicarse las recomendaciones ofrecidas por el Plan de Acción de la UE aprobado en octubre de 2023[103], completando y actualizando los análisis de riesgo de todos los operadores del sector del cable, con el objeto de aumentar la resiliencia de las infraestructuras terrestres y marítimas, y adoptando una planificación de contingencia específica para el caso de interrupciones graves del servicio. Un paso necesario, y urgente, es reconocer oficialmente los sistemas de cables submarinos como «infraestructura crítica».

Cabe destacar que, en España, la capacidad de los sistemas para seguir funcionando tras un incidente es muy elevada en la actualidad, gracias a la redundancia de cables en las principales rutas y la gestión realizada por los operadores. Pero debería evaluarse la conveniencia de fortalecer algunos aspectos vulnerables, como el reforzamiento de la conexión entre Melilla y la Península, posiblemente a través de un cable de doble uso, eléctrico y de fibra óptica. O la posibilidad de disponer de un buque, de titularidad pública, adaptado para realizar reparaciones de cables sin tener que depender exclusivamente de una oferta privada reducida y muy demandada[104].

Aunque los cables son gestionados y mantenidos por empresas privadas, las autoridades públicas deben asegurarse de que estas compañías cumplen los protocolos de seguridad establecidos para garantizar la integridad de la red. La supervisión pública no debe restringirse a los procedimientos de autorización previos al inicio de su actividad, sino mantenerse en el tiempo, ofreciendo de forma periódica el apoyo necesario para mantener los estándares de seguridad más elevados.

Esta supervisión por parte de las autoridades públicas ha de inscribirse en una visión estratégica global que deberá plasmarse en las próximas versiones de la Estrategia Nacional de Seguridad Marítima y la Estrategia de Seguridad Nacional. Esta visión estratégica debe contemplar al conjunto de los actores que operan en el sector del cable

[103] CONSEJO EUROPEO / CONSEJO DE LA UNIÓN EUROPEA. *Op. cit.*
[104] Estas carencias se pusieron de manifiesto durante la interrupción del servicio provocada por los accidentes en los cables que conectan con Melilla en 2007 y 2010.

submarino e integrar las partes tanto «húmeda» como «seca» de los sistemas, bajo el principio general de seguridad nacional.

En el plano internacional, se deberá seguir profundizando en la colaboración establecida en el marco de la UE y de la OTAN y, en general, en todos los foros multilaterales destinados a tal fin. La relevancia de la red global para la sociedad mundial exige todos los esfuerzos para erigir un marco jurídico internacional que establezca un régimen eficaz de protección a los cables.

En el plano operativo práctico se deberá analizar la conveniencia de profundizar en la colaboración con algunos de nuestros aliados más próximos, específicamente con Portugal. Dada la integración efectiva entre los sistemas de cables que aterrizan en territorio portugués y español, resultaría más eficaz sostener una visión común sobre los medios necesarios para proteger estas infraestructuras. La gran extensión marina bajo jurisdicción de ambos Estados requiere una exigente dedicación para llevar a cabo las tareas de control y vigilancia encomendadas. Esta necesidad compartida ofrece una ocasión para profundizar en la cooperación ya establecida, tanto en términos bilaterales como en el marco de la Alianza Atlántica, poniendo en práctica un «plan regional de vigilancia» en línea con las recomendaciones dadas por la UE.

Finalmente, la estrategia de seguridad nacional relativa a los sistemas de cable submarino debería inscribirse en una acción política más ambiciosa, orientada a definir una política de Estado para afrontar los desafíos que entrañan las tecnologías emergentes y disruptivas y la digitalización[105]: una política tecnológica y digital con proyección exterior que permita integrar la dimensión geopolítica y de seguridad con las políticas públicas, dando como resultado una línea de acción exterior de contenido tecnológico y alcance estratégico.

España, junto con sus aliados y socios europeos, debe seguir dando los pasos necesarios para garantizar que la protección de esta infraestructura crítica sea proporcional a su extraordinaria importancia para la seguridad nacional y la prosperidad de su economía.

[105] JORGE RICART, R. «Hacia una nueva línea de acción exterior tecnológica en España y Europa». Real Instituto Elcano, ARI 16/2021. Disponible en: https://www.realinstitutoelcano.org/analisis/hacia-una-nueva-linea-de-accion-exterior-tecnologica-en-espana-y-europa/

*Rafael García Pérez**
Profesor titular de Relaciones Internacionales (Universidad Pablo de Olavide, Sevilla)
Profesor del Instituto Universitario General Gutiérrez Mellado (UNED)
rgarcia@upo.es