El cable que sostiene el mundo: España, guardiana de la soberanía digital europea

El lecho marino como frontera estratégica: España y la defensa del cableado submarino en la era de la guerra híbrida

El 99 % del tráfico intercontinental de datos (y con él, 10 billones de dólares en transacciones diarias) circula por un entramado de cables de fibra óptica tendido sobre el fondo de los océanos. Esta infraestructura, invisible para la opinión pública, se ha convertido en objetivo prioritario de la confrontación geopolítica contemporánea. España, por su posición geográfica, ocupa un lugar central en este nuevo tablero.

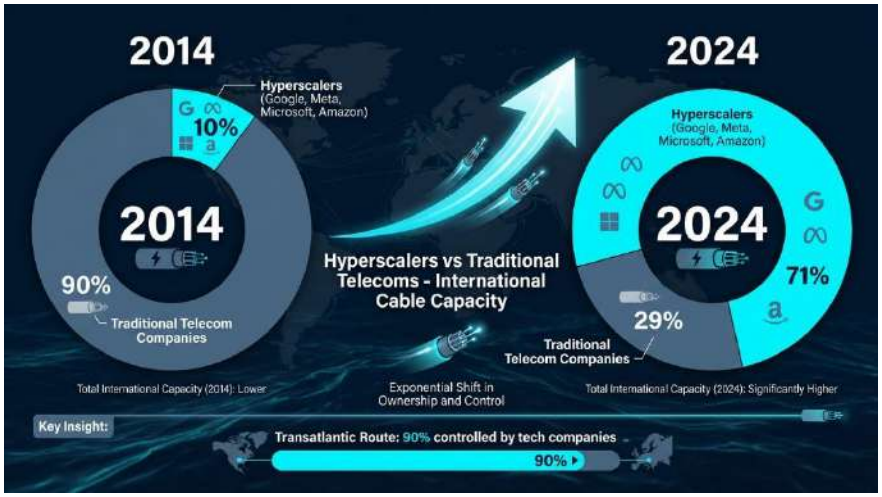
Por Juan M. Llenderrozas

1. Introducción contextual

Existe una ilusión colectiva, alimentada por el propio lenguaje que empleamos para describir la era digital, según la cual nuestros datos habitan "en la nube". Nada más lejos de la topografía real de internet: prácticamente la totalidad del tráfico intercontinental (llamadas, transacciones bancarias, comunicaciones diplomáticas, órdenes militares) discurre por algo más de 1,2 millones de kilómetros de cable tendido sobre el lecho oceánico. Se trata de una tecnología con 175 años de historia, cuyo principio físico apenas ha variado desde los primeros cables telegráficos transatlánticos del siglo XIX, pero cuya relevancia estratégica se ha multiplicado hasta convertirla en columna vertebral de la economía mundial.

El dato resulta desconcertante por su desproporción: el diámetro de esta infraestructura crítica (protegida por una envoltura de polietileno, una armadura de acero y un tubo de cobre que conduce hasta 15.000 voltios para alimentar los repetidores) apenas supera el de una manguera de jardín. En su núcleo, fibras ópticas del grosor de un cabello humano transmiten hasta 480 terabits por segundo. Sobre ese hilo extraordinariamente frágil se sostiene, en sentido literal, el sistema nervioso de la civilización digital.

La progresiva privatización de esta red añade una capa adicional de complejidad, y este dato sí conviene tratarlo como hecho verificado, respaldado por estadísticas de mercado de los últimos ejercicios: en 2014, las grandes tecnológicas (los llamados *hyperscalers*: Google, Meta, Microsoft, Amazon) controlaban apenas el 10 % de la capacidad internacional de cableado. Diez años después, en 2024, esa cifra ha escalado hasta el 71 %, y en la ruta transatlántica, la más relevante del planeta, estas compañías poseen ya el 90 % de la capacidad instalada entre Estados Unidos y Europa[i]. La infraestructura se ha privatizado casi por completo, pero sus implicaciones siguen siendo cuestión de soberanía nacional. Cuando un actor estatal hostil contempla el mapa de vulnerabilidades occidentales, el cable submarino aparece hoy junto al satélite y la red eléctrica como uno de los tres pilares de la infraestructura crítica global; esta última afirmación, conviene precisarlo, constituye una valoración analítica compartida por buena parte de la comunidad de inteligencia occidental, no un axioma establecido por norma alguna.



2. Análisis

El espectro de amenazas que afecta a esta red se organiza en dos ejes que conviene distinguir: la naturaleza física o cibernética de la amenaza, y su origen accidental o intencionado. La siguiente tabla resume el panorama descrito en la fuente analizada:

Origen /naturaleza	Física	Cibernética
Accidental	Anclas de buques comerciales arrastradas; redes de pesca de arrastre de fondo; minería submarina; eventos sísmicos y erupciones volcánicas (causa mayoritaria de cortes globales, según el propio informe)	Fallos de configuración de red; vulnerabilidades en la cadena de suministro de componentes
Intencionada	Sabotaje directo; *seabed warfare*; ataques mediante drones submarinos (AUV)	Intrusiones en redes de gestión y telemetría; dependencia de chips y hardware no europeo; hackeo a través de estaciones de amarre terrestres

En el terreno físico accidental, la causa mayoritaria de cortes globales sigue siendo mundana: anclas arrastradas y redes de pesca de arrastre de fondo. En el terreno físico intencionado emerge, en cambio, un concepto que ha ganado protagonismo en los círculos de inteligencia occidentales en los últimos años: el *seabed warfare*, o guerra del lecho marino.

Esta modalidad de conflicto se desarrolla en una zona gris deliberadamente ambigua. Buques oceanográficos y de inteligencia despliegan vehículos autónomos sumergibles (*AUV*) equipados con sonar de barrido lateral y brazos mecánicos capaces de seccionar cables blindados a más de 4.000 metros de profundidad. El objetivo no es únicamente el daño material, sino la negación plausible: diluir la frontera entre un accidente fortuito y un acto de sabotaje deliberado, de manera que resulte extraordinariamente difícil atribuir responsabilidad y activar una respuesta política o militar proporcional.

Sobre este punto conviene aplicar el rigor en el análisis que la propia naturaleza de la información exige. El buque de inteligencia ruso Yantar ha sido detectado en repetidas ocasiones operando con patrones anómalos en zonas próximas a infraestructuras submarinas críticas de interés para los aliados. Se trata de un hecho verificado por seguimiento *AIS* y por publicaciones de fuentes gubernamentales de varios países bálticos. Distinto es afirmar que dichos movimientos correspondan a una operación deliberada de sabotaje: esa atribución continúa pendiente de confirmación oficial por parte de los servicios de inteligencia implicados, y su tratamiento como doctrina consolidada de *seabed warfare* debe entenderse como valoración analítica, respaldada por indicios convergentes, pero no por prueba pericial pública concluyente.

A esta vulnerabilidad física se suma la cibernética. La dependencia de chips y componentes de hardware no europeos, las vulnerabilidades en la cadena de suministro y la posibilidad de intrusión en las redes de gestión y telemetría (o directamente en las estaciones de amarre terrestres, donde el cable emerge del mar) configuran un frente adicional que exige capacidades muy distintas a las tradicionalmente navales. El punto más frágil de todo el sistema, paradójicamente, no está en las profundidades oceánicas sino cerca de la costa: la cámara de amarre, esa bóveda de hormigón bajo la arena de la playa donde el cable realiza la transición del mar a tierra, constituye un punto de acceso físico relativamente sencillo y, por ello, una de las prioridades de protección menos visibles públicamente.

El marco jurídico que debería proteger todo este entramado resulta, sin matices posibles, anacrónico; este extremo sí es hecho verificable con solo consultar el texto vigente. El instrumento internacional de referencia, el Convenio para la Protección de los Cables Submarinos, fue redactado y firmado en 1884, en un contexto tecnológico y geopolítico que nada tiene que ver con el actual. En aguas internacionales, la protección jurídica de los cables se apoya en normas dispersas y de eficacia limitada frente a las amenazas híbridas contemporáneas. Más que un vacío legal absoluto, existe una brecha entre los instrumentos jurídicos disponibles, muchos de ellos concebidos para un entorno tecnológico anterior, y la complejidad operativa de la atribución, la disuasión y la respuesta ante sabotajes encubiertos. Europa, ante esta realidad, no puede seguir apoyándose en una disuasión

puramente legal: se impone una transición hacia la vigilancia tecnológica activa y la presencia física permanente en el mar. Esta última recomendación, cabe señalarlo, constituye una postura estratégica defendida por varios institutos de estudios de seguridad europeos, no un consenso jurídico formalmente adoptado por la Unión.

3. Implicaciones y riesgos estratégicos

Para las fuerzas de seguridad, los servicios de inteligencia y las autoridades encargadas de la gestión de las fronteras, el desplazamiento del cableado submarino al centro de la agenda de seguridad plantea retos de tres naturalezas distintas: operativa, legal y ética.

En el plano operativo, la vigilancia de miles de kilómetros de costa y de la Zona Económica Exclusiva exige capacidades de detección temprana que hasta hace pocos años eran patrimonio casi exclusivo de las grandes potencias navales: sonar de barrido, vehículos submarinos autónomos, sensores acústicos distribuidos. La incorporación de sensores integrados en la nueva generación de cables *SMART* (capaces de detectar presión, temperatura y actividad sísmica) y el desarrollo del *Distributed Acoustic Sensing* (*DAS*), que convierte la propia fibra óptica en un micrófono submarino a escala continental capaz de identificar la firma acústica de un buque no autorizado antes de que se produzca el corte, representan un salto cualitativo cuya eficacia real en despliegue masivo todavía debe validarse operativamente; se trata, por tanto, de una capacidad tecnológica demostrada en pruebas piloto, pero cuya generalización sigue siendo, a día de hoy, más proyecto que realidad extendida.

En el plano legal, la falta de un régimen jurídico unificado que abarque tanto la parte húmeda como la parte seca del ecosistema de cables (desde el tramo oceánico hasta el centro de datos que gestiona el tráfico) genera fisuras normativas que dificultan tanto la prevención como la persecución de responsabilidades. La Directiva NIS 2 de la Unión Europea representa el intento más ambicioso de cerrar esa brecha, al exigir estándares obligatorios de ciberresiliencia a los operadores tecnológicos y respaldar esa exigencia con la protección del Estado.

Su aplicación efectiva, sin embargo, depende de la capacidad de cada Estado miembro para articular una verdadera alianza público-privada entre quienes poseen físicamente la infraestructura y quienes son propietarios de los datos que por ella circulan (los hyperscalers y operadores de telecomunicaciones). El grado real de cumplimiento de esta directiva por parte de las tecnológicas es todavía, en el momento de escribir estas líneas, información pendiente de verificación pública sistemática.

En el plano ético y de gobernanza, la creciente concentración de la propiedad de esta infraestructura crítica en manos de un reducido número de corporaciones privadas, mayoritariamente estadounidenses, plantea una tensión de fondo entre soberanía nacional y propiedad privada que ningún marco regulatorio ha resuelto satisfactoriamente. Proteger una infraestructura de la que el Estado no es propietario, pero de cuya integridad depende su funcionamiento económico y su capacidad de comunicación soberana, constituye un

dilema de gobernanza que trasciende lo puramente técnico y que previsiblemente marcará la agenda legislativa europea de la próxima legislatura.

4. Perspectiva europea y española

España ha experimentado, en los últimos años, una transformación notable en su posición dentro del mapa digital global: de un papel periférico ha pasado a convertirse en la primera línea de la conectividad intercontinental. Proyectos de cableado de gran escala como Sistemas como Marea y Grace Hopper, con su punto de amarre en Bilbao, junto con los proyectos mediterráneos y africanos que conectan o prevén conectar la península con el norte de África, el Mediterráneo y el Atlántico, consolidan a España como nodo relevante de la conectividad digital euroatlántica, atraídos por una posición geoestratégica que ofrece rutas de alta capacidad hacia América y hacia África, reduciendo la dependencia histórica de los nodos del norte de Europa. Este dato, referido a proyectos ya operativos o en construcción avanzada, puede considerarse hecho verificado.

Esta ventaja competitiva conlleva, sin embargo, una responsabilidad ineludible. La península se perfila además como alternativa segura al corredor del mar Rojo, por donde transita una parte muy significativa del tráfico digital entre Europa y Asia que utiliza cables que atraviesan el mar Rojo a través del estrecho de Bab el-Mandeb, lo que convierte ese corredor en un punto de concentración de riesgo geopolítico y operativo

La inestabilidad de esa región y los ataques a buques mercantes registrados en los últimos ejercicios han provocado cortes críticos cuya reparación resulta casi imposible debido a la inseguridad armada de la zona. Frente a ese cuello de botella, la robusta conexión euromediterránea que atraviesa España ofrece a la Unión Europea un puente diversificado que blinda su soberanía digital y permite sortear los bloqueos de Oriente Medio; su consolidación como alternativa estructural al Rojo, no obstante, depende de inversiones adicionales todavía en fase de planificación, por lo que corresponde calificarla de proyección estratégica más que de hecho consumado.

El dispositivo institucional español para hacer frente a estos riesgos se apoya en tres pilares. El Sistema Integrado de Vigilancia Exterior (SIVE) de la Guardia Civil, concebido inicialmente para la vigilancia marítima y el control fronterizo, reúne capacidades que podrían contribuir de forma significativa a la protección de infraestructuras críticas submarinas. La integración de radares de superficie, cámaras optrónicas de largo alcance y sistemas AIS permite detectar e investigar patrones de navegación anómalos en áreas sensibles, incluidos los corredores de cable próximos a costa. Mi experiencia profesional me ha permitido constatar las altas capacidades del SIVE para vigilar amplios sectores del litoral y contribuir a la protección de instalaciones y tendidos de cable submarino próximos a costa. Resultaría conveniente completar su despliegue hasta alcanzar la totalidad del litoral peninsular e insular y, al mismo tiempo, adaptar sus procedimientos, criterios de alerta e integración de datos para incorporar de manera expresa la protección de estas infraestructuras críticas a su misión de vigilancia marítima.

La Armada, por su parte, asume bajo el mandato de la Estrategia Nacional de Seguridad Marítima (resumida en el principio de "proteger España en y desde la mar") la vigilancia de la extensa Zona Económica Exclusiva española, desarrollando capacidades de intervención subacuática mediante vehículos submarinos autónomos y vehículos submarinos autónomos y operados remotamente (*AUV* y *ROV*, respectivamente), así como otros medios especializados de inspección e intervención subacuática. Esta labor se integra, además, en el marco de la Alianza Atlántica a través de la coordinación con la Célula de Coordinación de Infraestructuras Submarinas Críticas de la OTAN (*Critical Undersea Infrastructure Coordination Cell* - *CUICC*), organismo creado como respuesta institucional a la escalada de incidentes en aguas europeas.

El tercer pilar, de naturaleza normativa, exige sellar las fisuras legales entre la tierra y el mar mediante la clasificación jurídica unificada del ecosistema de cables como infraestructura crítica, tarea en la que la transposición de la Directiva NIS 2 constituye el instrumento más inmediato disponible para las autoridades españolas y europeas. La Directiva NIS 2 ofrece

un marco relevante para reforzar la gestión de riesgos, la seguridad de la cadena de suministro, la notificación de incidentes y la responsabilidad de la alta dirección en sectores críticos. No obstante, su aplicación a los distintos elementos del ecosistema de cableado submarino deberá concretarse mediante la normativa nacional, la designación de entidades esenciales o importantes y los mecanismos de coordinación público-privada que se establezcan.

5. Conclusión y prospectiva

El fondo del mar ha dejado de ser un espacio vacío e inexplorado para convertirse en el auténtico sistema nervioso de la economía y la seguridad globales. La paradoja resulta llamativa: la infraestructura más determinante para la vida digital contemporánea sigue protegida por un tratado internacional de 1884 y por un hilo de fibra óptica del grosor de un cabello. Esta desproporción entre relevancia estratégica y fragilidad material seguirá siendo, con toda probabilidad, uno de los ejes centrales de la conflictividad híbrida de la próxima década, aunque conviene subrayar que esta proyección constituye un ejercicio prospectivo y no una certeza verificable con la información hoy disponible.

Tres tendencias marcarán, previsiblemente, la evolución de este dominio en los próximos años. Primero, la consolidación del *seabed warfare* como modalidad reconocida de confrontación en zona gris, con una probable multiplicación de incidentes atribuibles bajo negación plausible, especialmente en el Báltico, el Mediterráneo oriental y el mar Rojo. Segundo, la generalización de los cables SMART y la tecnología *DAS* como estándar de facto en los nuevos despliegues, desplazando el paradigma de la vigilancia reactiva hacia la detección temprana. Tercero, una presión regulatoria creciente (impulsada por la Directiva NIS 2 y por marcos equivalentes en desarrollo dentro de la OTAN) para unificar el tratamiento jurídico de la infraestructura crítica submarina, superando por fin la fragmentación heredada del siglo XIX.

España, por geografía y por la escala de sus despliegues recientes, no puede permitirse un papel secundario en esta transición; sostiene el tridente que protege los nodos más vitales de la era digital: capacidad de vigilancia, presencia naval activa y una posición geoestratégica que ningún otro país europeo puede replicar con facilidad. La resiliencia frente a estas amenazas no se construye sobre la ilusión de la invulnerabilidad, sino sobre tres capacidades complementarias que conviene consolidar sin demora: redundancia de rutas para que ningún corte aislado comprometa el servicio, vigilancia activa y permanente sobre los corredores críticos, y una capacidad soberana de reparación que permita restablecer el tráfico en plazos razonablemente cortos. Quien logre ese equilibrio entre disuasión tecnológica y capacidad de recuperación contará, en la práctica, con una ventaja estratégica difícil de igualar en el nuevo dominio del lecho marino.

[i] https://resources.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list-new