Geostrategos

Informe de Riesgo Geopolítico
Infraestructura Submarina Global de Comunicaciones | 30 de julio 2025
Unidad de Análisis Prospectivo

1. Contexto General

La red global de cables submarinos de fibra óptica es la columna vertebral de la economía digital: transporta más del 99 % del tráfico internacional de datos —incluyendo servicios financieros, comunicaciones gubernamentales, investigación científica y operaciones militares— a través de más de 550 sistemas que recorren 1,4 millones de kilómetros bajo el mar.

En un entorno de creciente rivalidad estratégica, esta infraestructura ha dejado de ser un activo técnico invisible para convertirse en un objetivo deliberado de presión geopolítica, sabotaje encubierto y operaciones híbridas. Entre 2023 y el primer semestre de 2025, se han registrado múltiples incidentes en Europa, Asia y África, vinculados a actores estatales, no estatales, y amenazas emergentes en zonas sin regulación efectiva.

Este informe combina dos enfoques complementarios: un Análisis de Vulnerabilidad–Amenaza–Impacto, que evalúa los factores estructurales del riesgo y sus implicaciones sectoriales y geográficas; y un Análisis de Actores y Motivaciones, que identifica a los principales stakeholders, sus intereses estratégicos y patrones de acción.

El propósito es ofrecer a juntas directivas, gobiernos y organismos multilaterales una visión integrada del riesgo, útil para decisiones estratégicas en contextos inciertos, dinámicos y de alta exposición digital.

2. Vulnerabilidad

Naturaleza estructural de la infraestructura

- Extensión física y exposición geográfica: más de 550 sistemas activos cubren 1.4 millones de kilómetros, tendidos sobre plataformas oceánicas, zonas económicas exclusivas y aguas territoriales. Esta infraestructura carece de blindaje físico, especialmente en tramos costeros o de poca profundidad, siendo accesible desde embarcaciones civiles o submarinos no tripulados.
- Concentración de puntos de amarre: zonas como Alejandría (Egipto), Marsella (Francia), Taiwán, Sudáfrica, Singapur y la costa este de EE.UU. concentran nodos de interconexión. Un ataque exitoso en una sola de estas ubicaciones podría generar disrupciones continentales.

- Falta de redundancia en regiones periféricas: África Occidental, el Mar Rojo, algunas islas del Pacífico y América Latina presentan menor diversificación de rutas. En estos contextos, un solo corte puede derivar en aislamiento digital temporal o sostenido.
- Limitada capacidad de monitoreo y respuesta: existen apenas 80 buques de reparación en el mundo, con alta demanda y tiempos de respuesta que oscilan entre 7 y 30 días. En paralelo, los mecanismos de detección temprana de daños o interferencias en cables son fragmentarios y dependen en gran medida de alertas manuales o pérdidas de conectividad.
- Marco jurídico internacional obsoleto: la Convención Internacional para la Protección de Cables Submarinos (1884) carece de fuerza normativa frente a sabotajes deliberados. El derecho internacional marítimo no ofrece respuestas claras ante agresiones encubiertas que se realicen en zonas fuera de jurisdicción nacional.

Evaluación de vulnerabilidad por región

Región	Nivel de Vulnerabilidad	Factores críticos
Mar Báltico	Alta	Proximidad con Rusia; rutas poco profundas; infraestructura dual (gasoductos y datos); congestión geoestratégica
Estrecho de Taiwán	Alta	Baja redundancia; presión geopolítica directa de China; tráfico civil-pesquero denso
Mar Rojo	Alta	Presencia de actores armados (Hutíes); cables densamente tendidos en zona estrecha; ausencia de vigilancia efectiva
Mediterráneo Oriental	Media-Alta	Convergencia de múltiples cables en zonas costeras egipcias; precedentes históricos de sabotaje
Atlántico Norte / Ártico	Media	Actividad rusa de cartografía y patrullaje submarino; redundancia parcial pero creciente vigilancia militar
Sudeste asiático / África Occidental	Alta	Baja resiliencia ante cortes; escasa capacidad local de reparación; rutas emergentes bajo amenaza natural o humana

3. Amenaza

Actores identificados

- **Rusia**: implicada directa o indirectamente en múltiples incidentes en el Mar Báltico y el Atlántico Norte. Utiliza embarcaciones civiles, flota pesquera y buques "científicos" para cartografiar cables y realizar operaciones clandestinas (ej. casos *Yi Peng 3*, *Eagle S*, *Yantar*). El patrón más utilizado es el de "ancla arrastrada" sobre rutas sensibles.
- **China**: asocia tácticas de presión "zona gris" contra Taiwán con sabotajes quirúrgicos a sus cables. Buques como *Shunxin 39* o *Hongtai 58* operan con transpondedores modificados y maniobras evasivas. También se reportan desarrollos tecnológicos orientados al corte selectivo.
- **Actores criminales o terroristas:** Históricamente presentes en episodios puntuales (caso Egipto 2013). Aunque hoy no hay evidencia de operaciones sistemáticas, la accesibilidad de estos tramos y la falta de vigilancia aumentan el riesgo latente.

Modos operativos detectados

Técnica	Frecuencia	Explicación
Ancla arrastrada (real o fingida)	Alta	Cubre gran parte de los casos en Báltico y Taiwán
Redes pesqueras industriales	Media	Utilizadas como pretexto para enredos accidentales
Transpondedores falsos / apagados	Media–Alta	Permiten encubrimiento, cambio de identidad, evasión de trazabilidad
Buceo costero (sabotaje manual)	Baja	Ej. Egipto 2013; potencial para escenarios urbanos
Ataques indirectos por guerra marítima	Baja–Media	Casos de yemeníes y África Occidental en 2024

Nivel de amenaza

Región	Nivel de Amenaza	Principal actor sospechado
Mar Báltico	Muy Alto	Rusia
Estrecho de Taiwán	Alto	China
Mediterráneo Oriental	Medio	Actores no estatales / criminales
Atlántico Norte	Medio–Alto	Rusia

4. Impacto

Tipos de impacto por sector

Sector	Impacto potencial (ejemplos)
Gobiernos y defensa	Interrupción en comunicaciones diplomáticas y de seguridad; pérdida de redundancia en tiempos de crisis
Finanzas y mercados	Latencia o caída de redes de pago transfronterizo; pérdida de sincronización bursátil en operaciones millonarias
Empresas y telecomunicaciones	Caídas de conectividad internacional; necesidad de redirección costosa de tráfico; daño reputacional
Infraestructura crítica	Interrupción de servicios como aviación civil, control marítimo, cadenas de suministro digital
Ciudadanía y servicios digitales	Afectación de conectividad en millones de usuarios; interrupción educativa, médica y laboral remota

5. Análisis de Actores Estratégicos

Rusia

Rusia dispone de capacidades navales especializadas para operar en el dominio submarino, incluyendo submarinos de inteligencia, buques como el Yantar y una red de embarcaciones pesqueras y comerciales con tripulación entrenada para misiones encubiertas. Su historial incluye actos de sabotaje relevantes, como el ataque al gasoducto Nord Stream y cortes en cables del Mar Báltico. En los últimos años, ha estado implicada indirectamente en varios incidentes confirmados en esa región —notablemente los casos Yi Peng 3, Eagle S y Silver Dania— mediante el uso

deliberado de la técnica del "ancla arrastrada", diseñada para simular accidentes y mantener negación plausible. Esta conducta responde a una estrategia orientada a explotar la asimetría informacional, desestabilizar sin provocar una confrontación directa y erosionar la cohesión europea a través de una forma de guerra híbrida submarina.

China

China cuenta con una marina de guerra con proyección regional y creciente presencia global, apoyada por una flota de embarcaciones civiles y científicas de doble uso, así como por una industria nacional de cableado submarino liderada por Huawei Marine. En los últimos años, ha protagonizado cortes deliberados a cables que conectan a Taiwán, particularmente entre 2023 y 2025, utilizando buques con maniobras evasivas y tecnologías diseñadas específicamente para la sección de cables en profundidad. Estas acciones encajan en una estrategia de coerción gradual, orientada a debilitar la resiliencia digital de Taiwán sin recurrir a la fuerza militar directa, como antesala posible de un escenario de bloqueo o invasión.

Estados Unidos

Estados Unidos posee una armada con proyección global, capacidades avanzadas de detección satelital, alianzas estratégicas en ciberseguridad y marcos regulatorios para controlar inversiones extranjeras sensibles. En respuesta al aumento de incidentes, ha intensificado la investigación sobre actos de sabotaje atribuidos a Rusia y China, ha impuesto sanciones a proveedores de infraestructura digital como Huawei y ZTE, y ha promovido el desarrollo de sistemas alternativos de conectividad global, como Starlink y Project Kuiper. Su motivación principal es preservar el dominio sobre infraestructuras críticas de comunicación, mitigando vulnerabilidades en cables clave que sostienen tanto su seguridad nacional como el funcionamiento de su economía digital.

Unión Europea y OTAN (flanco europeo)

La Unión Europea enfrenta una alta dependencia de la infraestructura de cables submarinos para su interconectividad interna, aunque con capacidades técnicas desiguales entre sus miembros. En el último período, han impulsado investigaciones conjuntas sobre incidentes en el Mar Báltico, activado el Mando Cibernético de la OTAN, reforzado patrullajes combinados en zonas sensibles y lanzado el plan "Cable Security" para mejorar la vigilancia y resiliencia de estas redes. Su accionar busca proteger intereses regionales, disuadir nuevas agresiones sin escalar el conflicto y asegurar la continuidad digital en escenarios de crisis.

Taiwán

Taiwán presenta una alta dependencia de la conectividad digital y capacidades limitadas de defensa submarina, aunque ha avanzado en la adquisición de radares, patrulleras y en la

cooperación con empresas privadas para proteger su infraestructura crítica. En los últimos años, ha denunciado internacionalmente los cortes deliberados a sus cables, intensificado las inspecciones costeras y reforzado la vigilancia en puertos estratégicos. Estas acciones responden a la necesidad de preservar su conectividad en caso de una escalada con China y evitar un aislamiento digital que comprometa su seguridad y gobernabilidad.

6. Dinámicas de interacción

Rusia y China comparten métodos encubiertos —como el uso de embarcaciones civiles, transpondedores manipulados y sabotaje físico—, pero con objetivos distintos: Moscú busca desestabilizar psicológica y políticamente a Europa mediante una "guerra submarina silenciosa", mientras que Beijing emplea tácticas coercitivas selectivas para debilitar la resiliencia de Taiwán sin escalar a un conflicto abierto. En contraste, Estados Unidos y sus aliados en la Unión Europea y la OTAN adoptan posturas esencialmente defensivas, centradas en vigilancia, sanciones, patrullajes y fortalecimiento normativo, aunque limitadas por marcos legales fragmentados y respuestas reactivas. Taiwán, por su parte, refuerza capacidades costeras y eleva su perfil internacional ante el riesgo de aislamiento digital. Este equilibrio inestable se ve agravado por la inercia estructural del sector privado —clave para la resiliencia técnica pero carente de herramientas de defensa activa— y por la posibilidad de daños colaterales provocados por actores no estatales o incidentes no atribuidos en zonas de conflicto.

7. Tipos de Stakeholders según responsabilidad y poder

Tipo de stakeholder	Ejemplos clave	Nivel de poder	Nivel de responsabilidad	Observación estratégica
Actores disruptivos	Rusia, China	Alto	Bajo	Capacidad ofensiva, uso de negación plausible, operación asimétrica
Actores protectores	EE.UU., OTAN, UE	Alto	Alto	Reaccionan bajo marcos legales; necesitan escalar capacidades disuasivas
Actores expuestos	Taiwán, África, Egipto	Bajo – Medio	Medio	Altamente dependientes, vulnerables ante agresores mayores

Actores facilitadores	Navieras civiles, operadores cable	Medio	Bajo – Medio	Posibles vehículos de interferencia; algunos cooperan con Estados
Actores técnicos–privados	Big Tech, ISPs	Alto	Medio	Clave en redundancia técnica, pero sin rol político directo
Actores normativos	ONU, UIT	Bajo	Bajo	Limitada influencia real; instrumentos jurídicos desfasados

El ecosistema de riesgo en torno a los cables submarinos está compuesto por actores con niveles asimétricos de poder y responsabilidad. Rusia y China operan como actores disruptivos con alta capacidad ofensiva y baja rendición de cuentas, mientras que Estados Unidos, la OTAN y la UE actúan como protectores con poder comparable pero limitados por marcos legales. Taiwán y países del Sur Global figuran como actores expuestos, vulnerables ante amenazas mayores. Empresas navieras y operadores de cable pueden facilitar acciones encubiertas, intencionadas o no, y las grandes tecnológicas desempeñan un papel clave en la resiliencia, aunque sin influencia geopolítica directa. Por último, organismos normativos como la ONU o la UIT mantienen bajo poder e impacto, dada la obsolescencia de los marcos regulatorios vigentes.

8. Conclusión y Escenarios Prospectivos

La infraestructura global de cables submarinos se ha convertido en un objetivo táctico en la competencia estratégica entre potencias. Actores como Rusia y China ya operan mediante métodos encubiertos —como el corte de cables con anclas arrastradas o la interferencia en zonas críticas— sin asumir responsabilidad directa. La respuesta occidental sigue siendo fragmentaria, jurídica y tecnológicamente lenta frente a un adversario que actúa en la "zona gris".

A la luz del comportamiento reciente y las capacidades involucradas, se proyectan los siguientes escenarios para el periodo julio 2025 – junio 2026:

Escenario	Descripción	Probabilidad	Consecuencias

1. Continuidad del patrón de sabotaje selectivo	Se repiten cortes "accidentales" en zonas sensibles (Báltico, Taiwán, Mar Rojo) usando buques civiles con apoyo estatal	Alta	Daños recurrentes a cables clave; disrupciones regionales controladas; respuesta diplomática limitada
2. Incidente de escalada no atribuida	Un corte simultáneo en múltiples cables genera interrupción masiva sin atribución clara	Media	Crisis de conectividad entre regiones (p.ej. África–Europa); presión sobre foros multilaterales
3. Ataque deliberado encubierto en América Latina o África Occidental	Se extiende la zona de operaciones hacia regiones con baja vigilancia o respuesta	Media	Desconexión parcial de países vulnerables; evidencia de globalización del conflicto híbrido
4. Refuerzo de protección estratégica por parte de alianzas democráticas	Implementación de sistemas de monitoreo, acuerdos OTAN-EU y cooperación con big tech	Media–Baja	Mejora en detección temprana; disuasión parcial; aumento de tensiones interestatales

Geostrategos prevé que el entorno operativo seguirá caracterizado por ataques de bajo umbral, difícil atribución y alta efectividad disruptiva. La infraestructura de cables submarinos debe dejar de ser vista como un activo técnico y asumirse como un activo geopolítico crítico en disputa. Si los Estados, alianzas y actores privados no adoptan una estrategia integral de protección, la red global de cables submarinos —de la cual depende la conectividad digital mundial— será cada vez más vulnerable a interferencias hostiles, con consecuencias crecientemente difíciles de contener.