



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Análisis de la seguridad de los cables submarinos de
telecomunicaciones frente a amenazas*

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Luis Alda de la Cruz

DIRECTORES: Rubén Nocelo López

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Análisis de la seguridad de los cables submarinos de
telecomunicaciones frente a amenazas*

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_{de}Vigo

RESUMEN

Este Trabajo Fin de Máster analiza la seguridad de los cables submarinos de telecomunicaciones, esenciales para la conectividad global y responsables del 95 % de las comunicaciones internacionales de datos. Se contextualiza su importancia estratégica, destacando su papel en la economía, la seguridad nacional y los servicios digitales, así como su vulnerabilidad frente a amenazas humanas, especialmente sabotajes intencionados.

El trabajo revisa el estado del arte, desde la evolución histórica de los cables hasta su relevancia en conflictos geopolíticos, evaluando medidas actuales de protección física y tecnologías innovadoras como la Detección Acústica Distribuida (DAS), que convierte los cables en sensores para la monitorización en tiempo real. Se describen casos de amenazas recientes, como cortes deliberados de cables submarinos, y acciones sospechosas de buques en zonas estratégicas, subrayando la necesidad de mejorar las estrategias de protección.

Se propone una metodología que combina análisis bibliográfico y prácticas en Red Eléctrica de España, enfocada en evaluar riesgos, identificar vulnerabilidades y explorar soluciones tecnológicas aplicables. Los resultados muestran que el uso de tecnologías como DAS, apoyado por un marco normativo adecuado y cooperación internacional, refuerza significativamente la seguridad de estas infraestructuras críticas.

Las conclusiones destacan la urgencia de desarrollar tecnologías avanzadas y protocolos internacionales para mitigar amenazas actuales y futuras, proponiendo líneas de investigación en inteligencia artificial y monitorización predictiva que permitan una protección más eficiente de los cables submarinos.

PALABRAS CLAVE

Infraestructuras críticas, cables submarinos, amenazas, monitorización, tecnología DAS.

AGRADECIMIENTOS

En primer lugar, a mi director, Rubén, por su constante apoyo y orientación durante todo este proceso. Su compromiso y conocimiento han sido esenciales para llevar a buen término este proyecto.

A todas las personas de Red Eléctrica de España, Aragón Photonics y UPTECH Sensing, que dedicaron parte de su tiempo a mi formación, especialmente a Santos, que gracias a su inestimable y desinteresada ayuda me proporcionó la información necesaria para darle sentido a este trabajo.

A mi amigo, compañero y doctor, Luis, por su apoyo, conocimiento y experiencia, que han sido un aporte significativo en el desarrollo de mi trabajo.

Por supuesto, a mi hermano y a mis padres, por haberme dado la educación y los valores en los que me he guiado durante todo este tiempo para ser la persona que soy.

A mi hijos, Manuela, Olivia, Luis y Alonso, por ser el motor de mi vida y el motivo para seguir siempre mirando hacia adelante.

Y por último, y más importante, a mi esposa, Beatriz, porque un día cortaste tus alas para darle fuerza a las mías. Después de esto... será tu turno.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	5
1 Introducción y objetivos	6
1.1 Contextualización.....	6
1.2 Motivación	7
1.3 Objetivos	7
1.3.1 Hipótesis principal	8
1.3.2 Justificación de la hipótesis	8
1.4 Estructura de la memoria	8
2 Estado del arte	10
2.1 Evolución de los cables submarinos	10
2.2 Seguridad actual de los cables submarinos y sus vulnerabilidades	10
2.3 Amenazas a los cables submarinos	12
2.4 Innovación tecnológica en la seguridad de cables submarinos.....	14
2.5 Contexto regulatorio	16
3 Desarrollo del TFM	18
3.1 Introducción	18
3.2 Estructura	19
3.3 Metodología	20
3.4 Importancia de los cables submarinos.	21
3.4.1 Cables submarinos	24
3.4.2 Protección física de los cables submarinos.....	27
3.5 Amenazas a la Seguridad de Cables Submarinos	31
3.5.1 Amenazas humanas accidentales	31
3.5.2 Amenazas humanas intencionadas	31
3.5.3 Ejemplos recientes de posibles sabotajes	34
3.5.4 Actores con capacidades para realizar sabotajes	36
3.6 Medidas de protección y prevención frente a amenazas.....	38
3.6.1 Medidas de protección convencionales actuales	38
3.6.2 Desafíos y limitaciones actuales	39
3.6.3 Tecnologías de monitorización.....	40
3.7 Medidas de seguridad tecnológicas de cables submarinos. Tecnología DAS	41
3.7.1 Sensores basados en fibra óptica	42

3.7.2 Fundamentos físicos	43
3.7.3 Sensado por retrodifusión	45
3.7.4 Partes de una solución DAS	45
4 Resultados	54
4.1 Evaluación y análisis del sistema DAS	54
4.1.1 Limitaciones de la tecnología DAS	54
4.1.2 Soluciones para aumentar la limitación de distancia de la tecnología DAS.....	55
4.2 Validación de la hipótesis	56
4.3 Medidas para mejorar las seguridad de los cables submarinos.....	56
5 Conclusiones y líneas futuras	60
5.1 Conclusiones	60
5.2 Líneas futuras	61
6 Bibliografía.....	63
Anexo I: Asignaturas del máster relacionadas con el trabajo	68
Anexo II: Listado de Acrónimos	69

ÍNDICE DE FIGURAS

Figura 1-1. Diagrama esquemático de cables submarinos utilizados como sensores para recibir señales acústicas generadas por los barcos mediante tecnología DAS [4].	6
Figura 1-2. Estudios científicos sobre los sensores de fibra óptica para monitorizar el medioambiente [5].	7
Figura 2-1. Buque ruso especializado en operaciones submarinas “Yantar” [14].	13
Figura 2-2. Derrota del buque mercante chino Yi Pen 3 en la zona de rotura de los cables submarinos [8].	13
Figura 2-3. Imagen del interrogador PHASE CP-COTDR “HDAS” [20].	16
Figura 3-1. Amenazas a los cables submarinos (fotomontaje de elaboración propia).	21
Figura 3-2. Foto de inauguración del Centro Marítimo de la OTAN para la Seguridad de Infraestructuras Críticas Submarinas [23].	23
Figura 3-3. Mapa de los cables submarinos de telecomunicaciones a nivel mundial [25].	24
Figura 3-4. Ejemplo de un sistema de telecomunicaciones mediante cable submarino [27].	25
Figura 3-5. Ilustración de un cable de fibra óptica [10].	25
Figura 3-6. Ilustración de un cable submarino eléctrico [30].	26
Figura 3-7. Ilustración de un cable submarino de energía y comunicaciones [29].	27
Figura 3-8. Enterramiento <i>plough</i> o arado de enterramiento [29].	28
Figura 3-9. Sistema para realizar enterramiento <i>jeting</i> [29].	28
Figura 3-10. Equipo para efectuar enterramiento <i>trencher</i> [29].	29
Figura 3-11. Vertido de roca para proteger externamente el cable submarino [29].	30
Figura 3-12. Colchón de cemento para proteger el cable submarino [29].	30
Figura 3-13. Porcentaje de cortes o roturas de cables relacionadas por diferentes causas desde 1959 hasta 2021 [33].	31
Figura 3-14. Mapa ilustrativo de los puntos de corte de los cables submarinos en Taiwán [40].	34
Figura 3-15. Mapa ilustrativo del cable submarino C-Lion 1. En color rojo se muestra el tramo del cable donde se produjo el incidente [41].	35
Figura 3-16. Petrolero Eagle S y helicóptero de la Guardia Fronteriza de Finlandia [44].	36
Figura 3-17. Minisubmarinos preparados para su carga en el buque ruso Yantar [7].	37
Figura 3-18. Capacidades del Servicio de Vigilancia Marítima de Copernicus [49].	39
Figura 3-19. Ejemplo de un vehículo submarino autónomo (UUV) [50].	39
Figura 3-20. Ilustración sobre las diferentes opciones de utilización de los sensores basados en fibra óptica [51].	42
Figura 3-21. Ilustración de los fotones a través de la fibra óptica [52].	43
Figura 3-22. Ilustración del fenómeno de retrodifusión [52].	43
Figura 3-23. Ilustración sobre la dispersión Brillouin [52].	44
Figura 3-24. Ilustración sobre la dispersión Raman [52].	44

Figura 3-25. Esquema de las frecuencias en intensidades en los tres tipos de dispersión en fibras ópticas [16].....	44
Figura 3-26. Partes de una solución DAS [52].....	46
Figura 3-27. Diferentes modelos de interrogadores DAS (elaboración propia con imágenes de [20], [55], [56], [57]).	46
Figura 3-28. Esquema de un OTDR básico (imagen adaptada de [17]).....	47
Figura 3-29. Señal registrada por un sistema C-OTDR antes y después de sufrir una perturbación [17].....	47
Figura 3-30. Ejemplo de análisis de eventos en una solución DAS [52].	49
Figura 3-31. Ejemplos de diferentes señales ante diferentes tipos de eventos (imagen adaptada de [17]).....	50
Figura 3-32. Arrastre de cadena sobre un cable submarino [54].....	51
Figura 3-33. Señal producida por el corte de una radial [54].....	51
Figura 3-34. Detección de un barco mediante el sistema DAS [5].	52
Figura 3-35. Captura de datos del equipo DAS en el momento del cruce del barco por encima del cable submarino de Red Eléctrica de España [54].....	52
Figura 3-36. Ejemplo de un sistema de gestión de incidencias de un enlace de cable submarino [19].....	53
Figura 4-1. Ilustración conceptual de un sistema de vigilancia de Infraestructuras Críticas Submarinas que combina la tecnología DAS, boyas, imágenes y datos satelitales para prevenir actos de sabotaje [60].....	58

ÍNDICE DE TABLAS

Tabla 3-1. Parámetros básicos de interrogadores DAS (elaboración propia adaptada de [16]).....	48
--	----

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contextualización

Los cables submarinos de telecomunicaciones son elementos fundamentales de la infraestructura global, responsables de aproximadamente el 95 por ciento de las comunicaciones internacionales de datos [1]. Estos cables conectan continentes y países, facilitando el intercambio de información en tiempo real y soportando servicios esenciales para la economía, la seguridad nacional y la vida cotidiana, como internet, los sistemas financieros, las comunicaciones gubernamentales y los servicios en la nube. A pesar de su importancia crítica, su vulnerabilidad ha sido históricamente subestimada, ya que están sujetos a una variedad de amenazas naturales y humanas [2].

Las amenazas humanas, como los actos de sabotaje y la manipulación intencionada, han crecido en importancia en un contexto geopolítico de crecientes tensiones internacionales. Los ataques dirigidos a estas infraestructuras pueden tener consecuencias severas en términos de conectividad y seguridad, impactando directamente a economías y poblaciones enteras. Además, la dependencia de estos cables por parte de instituciones gubernamentales y empresas privadas ha aumentado, elevando la necesidad de sistemas avanzados de protección y monitorización [3]. Ante esta realidad, las tecnologías de monitorización, como la Detección Acústica Distribuida (DAS por sus siglas en inglés), están emergiendo como soluciones prometedoras para detectar e intervenir en potenciales sabotajes.

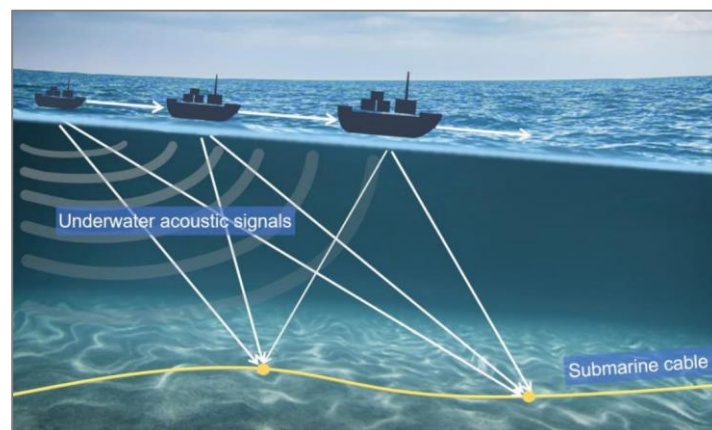


Figura 1-1. Diagrama esquemático de cables submarinos utilizados como sensores para recibir señales acústicas generadas por los barcos mediante tecnología DAS [4].

El gráfico de la Figura 1-2 ilustra el crecimiento en los últimos años de los estudios científicos que utilizan sensores de fibra óptica para monitorizar el medioambiente marino. Destaca el aumento casi exponencial desde el 2015 hasta el presente año, donde seguirá creciendo.

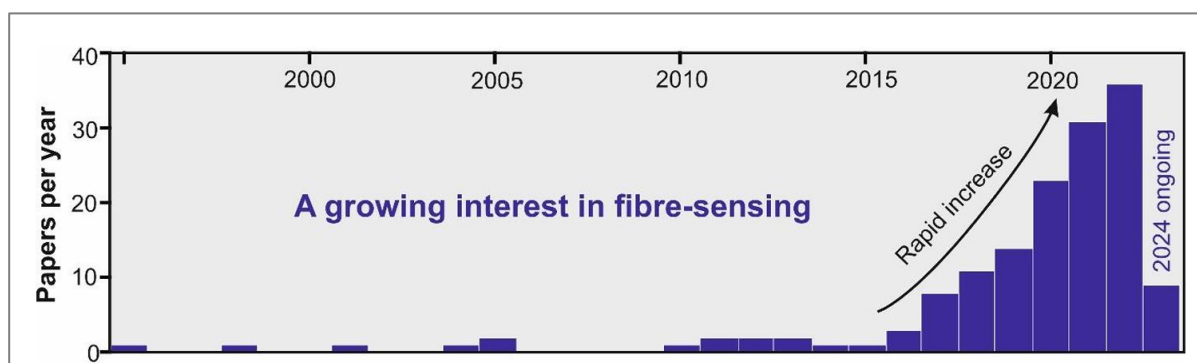


Figura 1-2. Estudios científicos sobre los sensores de fibra óptica para monitorizar el medioambiente [5].

1.2 Motivación

Durante el periodo de prácticas del autor en Red Eléctrica de España, una de las empresas líderes en el sector de infraestructura crítica para el transporte de energía, tuvo la oportunidad de adquirir experiencia práctica en el uso de tecnologías avanzadas para la monitorización de sistemas. Uno de los enfoques principales fue la implementación de la tecnología DAS para la monitorización de fibra óptica en cables submarinos.

La creciente frecuencia de noticias relacionadas con la posibilidad de sabotajes de cables submarinos debido a la tensión geopolítica actual, motivan la necesidad de nuevas soluciones para su protección. Las metodologías tradicionales de monitorización y protección, aunque efectivas hasta cierto punto, no han sido suficientes para garantizar una protección activa y en tiempo real frente a amenazas humanas.

Aquí es donde la tecnología DAS presenta una innovación significativa: al convertir los propios cables en sensores distribuidos, permite una detección continua y en tiempo real de vibraciones y actividades cercanas, que pueden indicar actividades potencialmente peligrosas, como el corte o manipulación de cables. Este enfoque no solo facilita una detección rápida de amenazas, sino también la posibilidad de una intervención temprana, minimizando así los daños y las interrupciones en la comunicación.

Este trabajo se plantea como una respuesta a la necesidad urgente de explorar tecnologías avanzadas para mejorar la seguridad de los cables submarinos. Se trata de abordar una problemática de relevancia global y ofrecer soluciones prácticas y tecnológicas que puedan aplicarse para reducir riesgos en una infraestructura crítica.

1.3 Objetivos

Este trabajo propone analizar y validar el uso de la tecnología DAS en la protección de cables submarinos frente a sabotajes. Para ello, se plantea una hipótesis que será validada o no en función del resultado del análisis planteado.

1.3.1 Hipótesis principal

Los sabotajes a los cables submarinos de telecomunicaciones representan una amenaza directa para la seguridad de Europa, dado su rol esencial como infraestructura crítica. La implementación de la tecnología DAS, gracias a su capacidad para monitorizar y detectar actividades sospechosas en tiempo real, constituye una herramienta clave para prevenir estos sabotajes y fortalecer la resiliencia de los cables submarinos frente a amenazas intencionadas.

1.3.2 Justificación de la hipótesis

Los cables submarinos son la columna vertebral de la conectividad global, responsables de la transmisión de más del 95 por ciento de los datos internacionales [1]. Estas infraestructuras críticas permiten el funcionamiento de servicios esenciales, como las comunicaciones gubernamentales, las transacciones financieras internacionales y la economía digital. En Europa, la dependencia de estos cables es particularmente muy alta, ya que sustentan la operatividad de sectores estratégicos y conectan al continente con el resto del mundo. Dado su carácter indispensable, cualquier interrupción, ya sea accidental o intencionada, podría generar un impacto significativo en la seguridad, la estabilidad económica y la vida diaria de millones de personas [6].

En este contexto, los sabotajes se presentan como una amenaza crítica. Recientes incidentes han evidenciado que actores estatales y no estatales poseen las capacidades necesarias para ejecutar sabotajes dirigidos a los cables submarinos [7]. Estas acciones no solo pueden interrumpir servicios esenciales, sino que también tienen el potencial de desencadenar crisis económicas y conflictos diplomáticos de gran alcance. El ejemplo reciente del corte del cable C-Lion1 en el mar Báltico, ha demostrado la vulnerabilidad de estas infraestructuras y la magnitud de las consecuencias derivadas de un sabotaje deliberado [8].

En este escenario, la implementación de tecnologías avanzadas de monitorización se vuelve una prioridad. La tecnología DAS se destaca como una solución innovadora y eficaz, capaz de transformar los propios cables de fibra óptica en sensores distribuidos que permiten detectar vibraciones y movimientos asociados con actividades sospechosas en tiempo real [9]. Su capacidad para identificar eventos anómalos de forma continua, incluso en entornos submarinos hostiles, lo convierte en una herramienta clave para la prevención proactiva de sabotajes. A diferencia de las medidas tradicionales, que suelen ser reactivas y de cobertura limitada, el DAS ofrece una solución más avanzada y adaptable a las necesidades actuales de seguridad.

En definitiva, la justificación de esta hipótesis radica en la necesidad urgente de proteger las infraestructuras críticas submarinas europeas frente a amenazas intencionadas, utilizando tecnologías disruptivas como el DAS. Este enfoque no solo fortalece la resiliencia de los cables submarinos, sino que también responde a las demandas de seguridad nacional y estabilidad económica en un mundo cada vez más interconectado y expuesto a riesgos derivados de conflictos geopolíticos.

1.4 Estructura de la memoria

El presente trabajo está organizado en seis capítulos, diseñados para abordar de manera exhaustiva los objetivos, el estado del arte, la metodología y los resultados relacionados con la seguridad de los cables submarinos de telecomunicaciones frente a amenazas.

En primer lugar, se presenta la introducción, donde se contextualiza la importancia de los cables submarinos como infraestructuras críticas. Se destaca su papel esencial en la conectividad global y su

vulnerabilidad frente a amenazas humanas y naturales. En esta sección también se incluye la motivación del trabajo, los objetivos principales y la hipótesis que se busca validar a lo largo del estudio.

A continuación, se aborda el estado del arte, que realiza un análisis detallado de los estudios previos relevantes en este ámbito. Se examina la evolución histórica de los cables submarinos, sus vulnerabilidades, las principales amenazas a las que se enfrentan, y se lleva a cabo una revisión de las tecnologías emergentes que podrían ofrecer soluciones a estos problemas, con especial énfasis en la tecnología DAS.

La metodología utilizada en este trabajo se describe en el siguiente capítulo. Aquí se detalla el enfoque adoptado para el desarrollo del análisis, que incluye la revisión bibliográfica, el análisis de amenazas y vulnerabilidades, y la integración de casos prácticos basados en experiencias profesionales. Este enfoque combina elementos teóricos y prácticos para construir un marco robusto que permita validar la hipótesis planteada.

El desarrollo del trabajo comprende un análisis profundo de la seguridad física y tecnológica de los cables submarinos. Se evaluarán las amenazas intencionadas, como los sabotajes, y se explorarán medidas preventivas y soluciones tecnológicas avanzadas. En este apartado se pone un énfasis especial en el uso de sistemas DAS para la monitorización en tiempo real y se incluyen propuestas de mejora basadas en tecnologías emergentes.

Los resultados y la discusión se presentan posteriormente, analizando los hallazgos obtenidos durante el desarrollo del trabajo. Se evalúa la eficacia de las soluciones tecnológicas propuestas, se identifican sus limitaciones y se discuten las áreas de mejora. Este análisis permite comprender la viabilidad práctica de las medidas adoptadas y su impacto en la seguridad de los cables submarinos.

Finalmente, el trabajo concluye con un capítulo dedicado a las conclusiones y líneas futuras. Aquí se resumen los principales hallazgos y contribuciones del estudio, destacando su relevancia en el campo de la seguridad de cables submarinos. Además, se proponen líneas futuras de investigación y desarrollo para abordar los desafíos restantes y ampliar el impacto de las soluciones tecnológicas identificadas.

2 ESTADO DEL ARTE

Dentro de este capítulo se enumeran y comentan estudios previos realizados que motivan el desarrollo del presente trabajo. En primer lugar se describe la evolución de los cables submarinos en las últimas décadas para poner en contexto el trabajo. Posteriormente se destacan diferentes análisis sobre la seguridad actual de los cables submarinos y sus vulnerabilidades, estudios sobre las amenazas a las que se enfrentan dichos cables y artículos científicos y tecnológicos sobre la aplicación de tecnologías innovadoras enfocadas a prevenir accidentes o en el caso concreto de la Defensa, evitar acciones de sabotajes.

2.1 Evolución de los cables submarinos

Los cables submarinos de telecomunicaciones han experimentado una evolución significativa desde sus inicios en el siglo XIX hasta la actualidad. Inicialmente, los cables telegráficos submarinos utilizaban conductores de cobre. Estos primeros cables permitían la transmisión de señales telegráficas a largas distancias, aunque con limitaciones en la capacidad y velocidad de transmisión [10].

El primer cable submarino internacional fue instalado en 1850, conectando Gran Bretaña con Francia a través del estrecho de Dover. Aunque este cable fue accidentalmente dañado poco después de su instalación, marcó el inicio de una era en las comunicaciones globales. Posteriormente, en 1858, se tendió el primer cable transatlántico entre Irlanda y Terranova, superando desafíos técnicos como profundidades de hasta 4.000 metros [11].

España también ha jugado un papel en el desarrollo de estas infraestructuras. En 1860, se tendieron cables que conectaban la península con las Islas Baleares y aseguraban comunicaciones interinsulares, fortaleciendo la conectividad regional [11].

2.2 Seguridad actual de los cables submarinos y sus vulnerabilidades

El artículo titulado "La vulnerabilidad de las infraestructuras críticas submarinas. Capacidades y cometidos derivados de la necesidad de su protección" [3], aborda la creciente importancia estratégica de las infraestructuras submarinas y la necesidad de protegerlas. Destaca que las infraestructuras submarinas, como cables de comunicación y tuberías de energía, son esenciales para el funcionamiento de las sociedades modernas, pero también son vulnerables a amenazas como sabotajes, accidentes y desastres naturales.

El autor analiza las capacidades necesarias para proteger estas infraestructuras, incluyendo la vigilancia, la detección de amenazas y la respuesta rápida ante incidentes. Además, subraya la importancia de la cooperación internacional y la coordinación entre diferentes entidades para garantizar la seguridad de estas infraestructuras críticas.

También, en [12], se analiza la importancia estratégica de los fondos marinos en el contexto de la seguridad y defensa nacional. Destaca que los fondos marinos son áreas de creciente interés debido a su riqueza en recursos naturales y su papel en las comunicaciones globales, especialmente a través de cables submarinos que soportan la mayor parte del tráfico internacional de datos. Así mismo, subraya la complejidad de estos entornos, que presentan desafíos técnicos y operativos para su exploración y vigilancia. Además, enfatiza la necesidad de desarrollar capacidades específicas para proteger estas infraestructuras críticas de posibles amenazas, incluyendo acciones de sabotaje o interferencias por parte de actores estatales y no estatales.

Por otra parte, el análisis efectuado en [13], analiza la vulnerabilidad de los cables submarinos de telecomunicaciones y su importancia para la seguridad nacional y la soberanía digital. Destaca que estos cables son infraestructuras críticas que soportan la mayor parte del tráfico de datos a nivel mundial, lo que los convierte en objetivos potenciales de sabotaje y otras amenazas. El artículo examina los organismos y marcos regulatorios involucrados en la gobernanza de los cables submarinos, identificando lagunas en su protección. Se presta especial atención a la actuación de actores clave como la Unión Europea.

El papel crucial que desempeñan los cables submarinos, especialmente bajo la amenaza de conflictos entre grandes potencias, se describe en [1]. Los autores destacan que estos cables transportan más del 95 % de los datos internacionales, siendo fundamentales para las infraestructuras de información y comunicación a nivel global. Sin embargo, su relevancia los convierte en objetivos potenciales en conflictos geopolíticos, especialmente entre Estados Unidos, China y Rusia. El informe subraya la necesidad de proteger estas infraestructuras críticas mediante estrategias que incluyen la colaboración internacional, el desarrollo de tecnologías de vigilancia y la implementación de políticas de seguridad cibernética robustas. Además, se enfatiza la importancia de la resiliencia de la red para mitigar posibles interrupciones causadas por acciones hostiles o desastres naturales.

El artículo "La Importancia Geoestratégica de los Cables Submarinos" de [2], destaca el papel fundamental de estos cables en la infraestructura global de comunicaciones. Cubriendo vastas extensiones oceánicas, estas líneas subacuáticas transportan la mayor parte del tráfico internacional de datos, incluyendo comunicaciones digitales y operaciones financieras críticas. Su impacto en la conectividad mundial supera con creces al de las alternativas satelitales, convirtiéndolos en elementos imprescindibles para el funcionamiento del mundo moderno.

También subraya el rol preeminente de China en el desarrollo y control de las redes de cables submarinos. Empresas chinas han liderado proyectos de instalación y mantenimiento en diversos puntos estratégicos del planeta, consolidando su influencia en la red global de telecomunicaciones. Esta posición privilegiada permite a China no solo gestionar el flujo de datos a nivel global, sino también aumentar su capacidad de monitoreo y control, lo que tiene implicaciones significativas en términos de seguridad internacional.

A medida que tecnologías como la inteligencia artificial y el Internet de las cosas generan una demanda sin precedentes de conectividad rápida y confiable, los cables submarinos están siendo modernizados y ampliados para satisfacer estas necesidades. La incorporación de tecnologías

avanzadas no solo mejora la eficiencia y velocidad de transmisión de datos, sino que también refuerza la resiliencia de los cables frente a amenazas externas. Estas mejoras son fundamentales para garantizar su continuidad operativa en un mundo cada vez más interconectado.

En síntesis, los cables submarinos constituyen una infraestructura esencial que sostiene la economía global y las comunicaciones internacionales. Su relevancia estratégica requiere un esfuerzo coordinado a nivel global para garantizar su protección frente a riesgos actuales y futuros. La colaboración entre países y el desarrollo de nuevas tecnologías desempeñarán un papel crucial para salvaguardar estas infraestructuras críticas en los años venideros.

2.3 Amenazas a los cables submarinos

En este punto se enumeran los estudios y análisis de amenazas procedentes de acciones humanas con el objetivo de causar daños a los cables submarinos de forma intencionada, como son los sabotajes. Los daños producidos por acciones humanas accidentales no son objeto de este trabajo aunque se describen en un punto para complementar la información.

Uno de los artículos destacados en este ámbito es el escrito por Luis V. Pérez Gil y titulado “Operaciones submarinas rusas encubiertas: las capacidades de la 29ª División de submarinos de la Flota del Norte” [7]. El autor ofrece un análisis detallado sobre las capacidades y actividades de esta unidad de élite de la Armada rusa.

La 29ª División de submarinos de la Flota del Norte se especializa en operaciones encubiertas y de inteligencia en aguas profundas. Está equipada con submarinos nucleares de última generación, diseñados para misiones de reconocimiento, sabotaje y despliegue de dispositivos en el fondo marino. Estas capacidades permiten a Rusia llevar a cabo operaciones clandestinas, incluyendo la manipulación de infraestructuras submarinas críticas, como cables de comunicación y tuberías de energía.

El artículo destaca la importancia estratégica de estas capacidades en el contexto de la competencia geopolítica actual. Las operaciones submarinas encubiertas proporcionan a Rusia una herramienta poderosa para proyectar influencia y llevar a cabo acciones que pueden desestabilizar a potenciales adversarios sin recurrir a enfrentamientos directos. Además, la capacidad de interferir con infraestructuras submarinas críticas representa una amenaza significativa para las comunicaciones y el flujo de energía a nivel global.

Pérez Gil también analiza las implicaciones para la seguridad internacional y la necesidad de que otras naciones fortalezcan sus capacidades de defensa submarina. La sofisticación de las operaciones de la 29ª División plantea desafíos significativos para la detección y neutralización de estas actividades, lo que requiere inversiones en tecnología avanzada y la formación de personal especializado en guerra submarina.

En relación con el artículo anterior, en [14], se aborda la actividad del buque ruso Yantar, especializado en operaciones submarinas, cerca de cables transatlánticos de internet frente a la costa de Irlanda en 2021. Este buque, conocido por sus capacidades para operar en el lecho marino, ha generado preocupación debido a su potencial para realizar actividades de espionaje o sabotaje en infraestructuras críticas. La presencia del Yantar en esta zona estratégica pone de relieve los riesgos para la seguridad de las comunicaciones globales y el creciente interés geopolítico en los cables submarinos.



Figura 2-1. Buque ruso especializado en operaciones submarinas “Yantar” [14].

Como ejemplos de posibles sabotajes, en [8] se analiza los cortes de cables submarinos en el mar Báltico y las implicaciones legales de la interdicción de buques sospechosos. El autor detalla cómo, en noviembre de 2024, se produjeron cortes en los cables submarinos de telecomunicaciones C-Lion1, que conectan Finlandia y Alemania, y en otro cable entre Suecia y Lituania. Estos incidentes ocurrieron en la zona económica exclusiva de Suecia y generaron sospechas de sabotaje, especialmente hacia el buque mercante chino Yi Peng 3, que estaba en la zona en ese momento.



Figura 2-2. Derrota del buque mercante chino Yi Pen 3 en la zona de rotura de los cables submarinos [8].

El autor del artículo examina las respuestas de los Estados costeros, como Suecia y Dinamarca, que consideraron la posibilidad de abordar e inspeccionar el Yi Peng 3 para investigar su posible implicación en los cortes de los cables. Discute las bases legales para tales acciones, incluyendo el consentimiento del Estado del pabellón, China, y las disposiciones del Derecho internacional marítimo que podrían permitir la interdicción en casos de sospecha de actividades ilícitas.

Además, el artículo contextualiza estos eventos dentro de una percepción rusa de estar en conflicto con la OTAN, sugiriendo que tales actos podrían formar parte de tácticas de guerra híbrida dirigidas a infraestructuras críticas. Lott subraya la dificultad de proteger los cables submarinos contra cortes intencionales y la importancia de la cooperación internacional para abordar estas amenazas.

Otro ejemplo en el que el sabotaje tomó más fuerza para ser real, fue el que se informa en [15], sobre la interrupción de los servicios de internet en las islas Matsu, un archipiélago taiwanés cercano a China continental, debido al corte de dos cables submarinos en marzo de 2023.

Según la Comisión Nacional de Comunicaciones de Taiwán, sospechó que dos barcos chinos habrían sido responsables de los daños: un barco pesquero habría cortado el primer cable a unos 50 kilómetros de la costa, y seis días después, un carguero chino habría dañado el segundo. Aunque el gobierno taiwanés no acusó directamente a Pekín de un acto deliberado, estos incidentes generaron preocupación sobre la seguridad nacional y la vulnerabilidad de las infraestructuras críticas.

La pérdida de conectividad afectó significativamente la vida diaria de los 14.000 residentes de Matsu, dificultando actividades como pagos de facturas, citas médicas y operaciones comerciales. La isla tuvo que depender de transmisiones de microondas como solución temporal, lo que resultó en conexiones inestables y lentas.

Expertos en defensa sugirieron que estos cortes podrían ser parte de las tácticas de intimidación de China contra Taiwán, en el contexto de las crecientes tensiones en la región. En respuesta, las autoridades taiwanesas tomaron medidas para reforzar la protección de sus infraestructuras submarinas y mejorar las tecnologías de respaldo para garantizar la estabilidad de las comunicaciones en situaciones de emergencia.

2.4 Innovación tecnológica en la seguridad de cables submarinos

Una vez que se han comentado los estudios y análisis sobre la seguridad de los cables submarinos, sus vulnerabilidades y amenazas a las que se enfrentan, en este punto se detallan aquellos que se refieren a la tecnología DAS como parte de una solución al problema planteado sobre la seguridad física.

Los autores en [16], realizan un análisis detallado del uso de los sensores acústicos distribuidos por fibra óptica en el ámbito de la ingeniería civil. Estos sistemas permiten una monitorización continua, eficiente y en tiempo real de estructuras críticas como puentes, túneles, edificios y presas, detectando vibraciones y deformaciones que podrían comprometer la integridad estructural.

Sin embargo, el artículo también aborda los desafíos asociados con esta tecnología. Entre los principales problemas se encuentran la sensibilidad y precisión limitadas en ciertos entornos, la complejidad de manejar grandes volúmenes de datos generados y la necesidad de adaptar estos sistemas a infraestructuras ya existentes. Además, los costes iniciales y la falta de estándares generalizados para su implementación representan barreras adicionales para su adopción masiva.

A pesar de estas limitaciones, los autores concluyen que el DAS tiene un potencial transformador para la ingeniería civil. Recomiendan enfocarse en investigaciones futuras que optimicen la tecnología, mejoren su integración con otras herramientas de monitoreo y reduzcan los costes, facilitando así su uso generalizado.

En el contexto de las empresas eléctricas, esta tecnología ofrece oportunidades significativas para mejorar la detección de intrusiones, monitorear condiciones ambientales y supervisar el estado según se recoge en [17]. El artículo detalla diversas aplicaciones de la tecnología DAS en el sector eléctrico, incluyendo la detección temprana de fallos en cables subterráneos y submarinos, la vigilancia de perímetros en subestaciones y la monitorización de líneas de transmisión. Los autores también abordan los desafíos asociados con la implementación de DAS, como la necesidad de calibración precisa y la

gestión de grandes volúmenes de datos generados. A pesar de estos retos, concluyen que la tecnología DAS representa una oportunidad valiosa para las empresas eléctricas que buscan optimizar sus operaciones.

Otro estudio destacado es el realizado en [18], donde proponen una arquitectura basada en la nube que facilita la transmisión, el almacenamiento y el análisis en tiempo real de datos provenientes de sistemas DAS. Esta solución aborda los retos asociados con el ancho de banda, la capacidad de almacenamiento y la necesidad de procesamiento eficiente para aplicaciones industriales críticas. Los autores implementan y evalúan diferentes estrategias para garantizar la integridad de los datos y optimizar la respuesta en tiempo real.

Entre los hallazgos clave, el artículo destaca cómo los servicios en la nube no solo ofrecen flexibilidad y escalabilidad, sino que también permiten integrar algoritmos avanzados de procesamiento de señales y análisis de datos. Esto mejora significativamente la precisión y velocidad en la detección de eventos críticos, como actividades sísmicas o intrusiones.

En conclusión, el trabajo demuestra que las soluciones basadas en la nube pueden transformar la manera en que los sistemas DAS gestionan y procesan datos, allanando el camino para aplicaciones más eficientes, económicas y versátiles en el monitoreo de activos y seguridad. La investigación subraya el potencial de estas tecnologías para satisfacer las crecientes demandas del sector industrial y de infraestructura crítica.

Como casos de estudio, cabe destacar el realizado por Aragón Photonics para Red Eléctrica de España [19], donde se examinan las estrategias para proteger cables submarinos destinados a la transmisión de energía eléctrica, que enfrentan constantes riesgos por actividades humanas y naturales, como el garreo de anclas, el arrastre de redes y la instalación de otros cables. Estos incidentes, ya sean accidentales o intencionales, generan interrupciones en el servicio eléctrico, costes elevados de reparación y problemas significativos para los usuarios. La solución propuesta utiliza la tecnología de DAS, que permite detectar vibraciones y clasificar eventos en tiempo real, con un enfoque en prevenir daños y localizar posibles responsables en caso de incidentes.

El desafío principal consistía en evitar daños a los cables submarinos y, en caso de ocurrir, identificar con precisión a los responsables. Esto requeriría la capacidad de detectar la proximidad de embarcaciones a las áreas de riesgo con suficiente antelación para alertarlas. Además, el sistema debía ser capaz de operar de manera confiable en entornos submarinos complejos, donde los daños pueden ocurrir rápidamente y ser difíciles de rastrear. Bajo estas premisas, se confió en la supervisión de dos enlaces submarinos interinsulares, uno de 17 kilómetros y otro de 57 kilómetros, con el objetivo de implementar una solución avanzada y adaptable.

La solución implementada consistió en el uso del interrogador PHASE CP-COTDR “HDAS” fabricado por Aragón Photonics Labs, que tiene un alcance de hasta 70 km y la capacidad de operar en canales duales. Este sistema utiliza fibras ópticas monomodo G652-D, que ya estaban instaladas y eran propiedad del operador, integrando la tecnología DAS con herramientas de monitoreo avanzado. Una base de datos robusta de patrones acústicos, desarrollada en proyectos de investigación previos, permitió al sistema clasificar agresiones específicas como el garreo de anclas o el arrastre de redes. El software del sistema se adaptó para incluir información de sistemas de identificación automática (AIS), lo que permitió asociar alarmas acústicas con movimientos de embarcaciones cercanas.



Figura 2-3. Imagen del interrogador PHASE CP-COTDR “HDAS” [20].

El sistema se diseñó con altos estándares de ciberseguridad para proteger las comunicaciones y garantizar la integridad de los datos transmitidos. Su implementación ha permitido al operador supervisar en tiempo real dos enlaces submarinos, cubriendo un total de 80 kilómetros, con planos de expansión a un tercer enlace. Los resultados iniciales muestran una operación exitosa, con la capacidad de detectar y prevenir daños antes de que ocurran, así como de identificar con precisión los responsables en caso de incidentes.

Entre los beneficios destacados del sistema se encuentran el bajo costo de capital (CAPEX) debido a la reutilización de la infraestructura de fibra óptica existente, el bajo costo operativo (OPEX) gracias a los mínimos requerimientos de mantenimiento, y la alta disponibilidad del sistema por la confiabilidad de la fibra óptica como sensor. Además, la solución permite compartir la fibra óptica tanto para el monitoreo acústico como para las telecomunicaciones, optimizando recursos y reduciendo costos adicionales.

En resumen, este caso de estudio demuestra cómo la tecnología DAS puede integrarse de manera efectiva para proteger infraestructuras submarinas críticas. La solución no solo mejora la detección y prevención de daños, sino que también ofrece un modelo de gestión eficiente y escalable para el monitoreo de cables submarinos, aportando mayor seguridad y reduciendo costes operativos en el sector energético.

2.5 Contexto regulatorio

En cuanto a documentación regulatoria, se destaca la Recomendación (UE) 2024/779 de la Comisión Europea, publicada el 26 de febrero de 2024, que establece directrices para garantizar la seguridad y resiliencia de las infraestructuras de cables submarinos en la Unión Europea [21]. Reconociendo que la mayoría del tráfico internacional de datos se transmite a través de estas infraestructuras, el documento destaca su importancia estratégica para la soberanía digital europea.

La Recomendación identifica amenazas clave, como sabotajes, ataques físicos y vulnerabilidades cibernéticas. Para enfrentarlas, insta a los Estados miembros a evaluar riesgos, implementar medidas de seguridad, y reforzar la cooperación internacional en la protección de estos cables.

Un punto central del documento es el énfasis en la innovación tecnológica para fortalecer la resiliencia. Entre las medidas propuestas se incluyen sistemas de monitorización avanzada que detecten anomalías en tiempo real, tecnologías de ciberseguridad para proteger las comunicaciones y redundancia inteligente mediante rutas alternativas y capacidad de recuperación automática. También se fomenta la investigación y desarrollo en cables submarinos de próxima generación, incorporando características como auto-reparación y sensores remotos.

A nivel nacional, la Estrategia Nacional de Seguridad Marítima 2024 [22], subraya la importancia estratégica de los cables submarinos como infraestructuras críticas para la conectividad global. Estas

infraestructuras desempeñan un papel clave en las conexiones eléctricas y digitales con los archipiélagos y otros continentes, lo que las convierte en elementos esenciales para la seguridad y el desarrollo económico de España. Sin embargo, también se destacan como objetivos vulnerables ante múltiples amenazas, incluidos los atentados terroristas, sabotajes y ciberataques. Ejemplos recientes de sabotajes en otras regiones refuerzan la preocupación por la posibilidad de interrupciones en los servicios que dependen de estos cables, lo que tendría repercusiones severas para la seguridad nacional y la estabilidad económica.

En respuesta a estas amenazas, la Estrategia Nacional plantea una serie de medidas para proteger los cables submarinos. Entre ellas se incluyen la integración de estas infraestructuras en análisis de riesgos, el fortalecimiento de los sistemas de vigilancia y la colaboración público-privada. Además, se destaca la necesidad de cooperación internacional para garantizar su seguridad, especialmente en un contexto de amenazas híbridas que incluyen sabotajes intencionados, explotación no autorizada de recursos naturales y ciberataques dirigidos a las redes de comunicación. Estas acciones se enmarcan en un esfuerzo más amplio para proteger las infraestructuras críticas del país, reconociendo la relevancia de los cables submarinos no solo para España, sino también para la estabilidad de la economía y las comunicaciones globales.

3 DESARROLLO DEL TFM

3.1 Introducción

Este trabajo tiene como objetivo analizar la situación actual de la seguridad física de los cables submarinos, con un enfoque particular en aquellos destinados a las telecomunicaciones. Estos cables son fundamentales para la transmisión de datos a larga distancia, sustentando la conectividad global y facilitando el intercambio de información entre naciones. Su importancia trasciende el ámbito tecnológico, pues representan un pilar esencial para el funcionamiento de sistemas financieros, comunicaciones gubernamentales y servicios digitales que sostienen las economías modernas. Por esta razón, se consideran infraestructuras críticas, cuya protección es prioritaria para garantizar tanto la estabilidad económica como la seguridad nacional de los países que dependen de ellas.

La investigación presentada se centra en identificar y evaluar los riesgos, amenazas y vulnerabilidades a las que se enfrentan estos cables submarinos, poniendo un énfasis particular en los daños provocados por sabotajes deliberados. Estos actos de sabotaje no solo representan una amenaza a la continuidad de los servicios, sino que también tienen el potencial de desestabilizar relaciones diplomáticas y causar daños económicos significativos. A través de este análisis, se busca entender las dinámicas que hacen que estas infraestructuras sean objetivos atractivos para actores malintencionados, así como explorar las medidas de seguridad física necesarias para protegerlas de manera efectiva. Este enfoque no solo aborda los desafíos inmediatos, sino que también considera las implicaciones a largo plazo de no garantizar una protección adecuada.

Un aspecto destacado en este contexto es la dificultad para identificar de manera clara y precisa a los responsables de los incidentes que han sido catalogados como posibles sabotajes a cables submarinos. La naturaleza remota de estas infraestructuras y la falta de herramientas avanzadas de monitorización en muchas áreas dificultan el rastreo y la atribución de responsabilidades. Esta falta de claridad complica las respuestas diplomáticas y legales, dejando a menudo a las naciones afectadas en una posición de vulnerabilidad. Sin embargo, se plantea que la incorporación de soluciones avanzadas basadas en tecnologías de la información y las comunicaciones (TIC), podría ofrecer un medio para abordar este desafío. Estas tecnologías no solo pueden mejorar la capacidad de detección de incidentes en tiempo real, sino también facilitar la recolección de evidencia que permita identificar a los perpetradores y prevenir futuros ataques.

En última instancia, este trabajo busca contribuir al desarrollo de estrategias más robustas para la protección de los cables submarinos, destacando la necesidad de una colaboración internacional y el empleo de tecnologías innovadoras. El análisis realizado subraya la importancia de avanzar en la implementación de soluciones TIC en estas infraestructuras críticas, reconociendo su potencial para transformar la manera en que se gestionan los riesgos y se garantiza la seguridad física de los cables submarinos de telecomunicaciones. Con una comprensión más profunda de los desafíos actuales y las oportunidades tecnológicas, se espera sentar las bases para futuras investigaciones y desarrollos en este campo crucial.

3.2 Estructura

Este trabajo de investigación ha sido estructurado en cuatro secciones principales, cada una destinada a abordar un aspecto clave relacionado con la seguridad de los cables submarinos, especialmente los que son considerados infraestructuras críticas para los Estados. En la primera sección, se analiza la importancia estratégica de estos cables desde la perspectiva de la seguridad nacional e internacional. Los cables submarinos no solo son fundamentales para la conectividad global, sino que también sustentan servicios esenciales como las comunicaciones gubernamentales, el sistema financiero y las transacciones comerciales internacionales. Su papel como columna vertebral de la transmisión de datos los convierte en un componente esencial para la estabilidad económica y social de las naciones. Este análisis inicial destaca cómo su protección es una prioridad creciente en un contexto global marcado por tensiones geopolíticas y una dependencia cada vez mayor de las redes digitales.

En la segunda sección, el enfoque se centra en las medidas de seguridad actualmente implementadas para garantizar la integridad de los cables submarinos. Estas incluyen tanto estrategias físicas como tecnológicas destinadas a prevenir daños accidentales y sabotajes. Se analizan las restricciones operativas, como las áreas de exclusión alrededor de los cables en zonas sensibles, las patrullas marítimas y el uso de tecnologías de monitoreo en tiempo real, como los drones submarinos y los sensores básicos. Sin embargo, también se destacan las limitaciones de estas medidas, que a menudo son insuficientes para abordar amenazas sofisticadas y de gran alcance. Esta sección proporciona un panorama detallado de las prácticas actuales, identificando tanto sus fortalezas como las áreas en las que es necesario avanzar para mejorar la protección de estas infraestructuras críticas.

La tercera sección está dedicada a las amenazas a las que están expuestos los cables submarinos, con un enfoque particular en los riesgos asociados con actos de sabotaje. Aquí se detallan los métodos empleados para atacar estos cables, que van desde cortes físicos realizados por embarcaciones hasta interferencias electrónicas avanzadas. Además, se analizan los actores con capacidad para llevar a cabo estos sabotajes, incluyendo tanto actores estatales como no estatales, y se discuten las motivaciones que pueden impulsarlos, como intereses políticos, económicos o estratégicos. Esta parte del trabajo subraya cómo los sabotajes no solo afectan la conectividad de un país, sino que también pueden generar repercusiones a nivel regional y global, exacerbando tensiones diplomáticas y causando pérdidas económicas significativas.

En este contexto, se plantea la hipótesis de que los sabotajes a cables submarinos de telecomunicaciones representan una amenaza crítica para la seguridad y la economía de los Estados, pero que el uso de tecnologías avanzadas de monitoreo, como el DAS, puede contribuir significativamente a prevenir estas amenazas al permitir una detección temprana y una respuesta

eficaz. Esta hipótesis guía el análisis a lo largo del trabajo y establece la base para evaluar las limitaciones actuales y las posibles soluciones tecnológicas para proteger estas infraestructuras críticas.

Por último, dado que el máster está centrado en las TIC para la Defensa, la cuarta sección plantea una serie de propuestas innovadoras basadas en estas tecnologías para mejorar la seguridad de los cables submarinos. Estas propuestas incluyen el uso de sistemas avanzados de monitorización como el DAS para detectar actividades sospechosas en tiempo real, así como la integración de inteligencia artificial para el análisis predictivo de amenazas. También se exploran soluciones híbridas que combinan tecnologías emergentes con estrategias tradicionales de seguridad, destacando cómo estas innovaciones pueden prevenir riesgos de manera más eficaz y garantizar la resiliencia de estas infraestructuras críticas frente a amenazas modernas. Esta última sección ofrece una visión prospectiva, subrayando la importancia de la investigación y el desarrollo continuo en este campo para enfrentar los desafíos actuales y futuros.

3.3 Metodología

La metodología seguida en este trabajo se estructura en cuatro partes diferenciadas, cada una diseñada para abordar los distintos aspectos clave del análisis sobre la seguridad de los cables submarinos. En las dos primeras partes, la metodología empleada consistió en un análisis exhaustivo de la literatura académica relacionada con la importancia estratégica de los cables submarinos y las medidas utilizadas actualmente para garantizar su seguridad. Esta revisión permitió construir un marco teórico sólido que sirvió como base para identificar las fortalezas y limitaciones de las estrategias existentes, tanto en términos de políticas de protección como de tecnologías implementadas. La literatura revisada incluyó informes gubernamentales, estudios académicos y documentos técnicos que proporcionaron una visión integral sobre la relevancia de estas infraestructuras críticas y los enfoques actuales para protegerlas.

En la tercera parte, y teniendo en cuenta los hallazgos de las dos secciones anteriores, se adoptó una metodología orientada al análisis de las amenazas existentes, con un énfasis particular en los riesgos asociados con sabotajes. Este enfoque permitió identificar y categorizar las principales amenazas, los actores con capacidad para llevarlas a cabo y las vulnerabilidades específicas que hacen de los cables submarinos objetivos atractivos para estos ataques. La metodología empleada incluyó el estudio de casos históricos de sabotajes, así como la evaluación de informes técnicos y documentos estratégicos que describen las capacidades de actores estatales y no estatales. Este análisis permitió entender cómo las amenazas evolucionan en función del contexto geopolítico y tecnológico, destacando la necesidad de desarrollar soluciones innovadoras para contrarrestarlas.

Por último, el trabajo adopta una perspectiva más práctica en su sección final, basada en las prácticas realizadas por el autor en Red Eléctrica de España, una empresa clave en el sector energético español. Durante esta experiencia profesional, el autor tuvo la oportunidad de participar en la implementación de tecnologías avanzadas para la monitorización de cables submarinos. Este enfoque práctico permitió analizar de primera mano cómo se integran tecnologías innovadoras, como sensores y sistemas de comunicación en tiempo real, para supervisar el estado de estas infraestructuras críticas. Las prácticas realizadas ofrecieron un valioso aprendizaje sobre los desafíos técnicos y operativos asociados con la implementación de soluciones de monitorización, así como sobre los beneficios tangibles que estas tecnologías pueden aportar a la seguridad de los cables submarinos.

En esta última parte, no solo se presenta un marco teórico detallado, sino que también se ofrece un análisis práctico basado en la experiencia directa adquirida en el campo profesional. Esta combinación de teoría y práctica enriquece significativamente el estudio, ya que permite evaluar la aplicabilidad real de las tecnologías avanzadas en escenarios concretos. Además, se destacan las oportunidades de mejora y las lecciones aprendidas durante el proceso, proporcionando una base sólida para futuras investigaciones y desarrollos en el ámbito de la protección de infraestructuras críticas submarinas. Esta integración de enfoques teóricos y prácticos refuerza la validez de los resultados y subraya la importancia de las soluciones innovadoras para enfrentar los retos actuales en la seguridad de los cables submarinos.

3.4 Importancia de los cables submarinos.

En los últimos años, la seguridad de los cables submarinos ha adquirido una relevancia cada vez mayor, convirtiéndose en un tema recurrente en el ámbito de las infraestructuras críticas y la seguridad internacional. Esta creciente preocupación responde al papel fundamental que desempeñan estos cables en la conectividad global y la economía digital, así como a las amenazas emergentes que ponen en riesgo su funcionamiento. Organizaciones internacionales y gobiernos están comenzando a dar pasos significativos para abordar estas amenazas y garantizar la protección de estas infraestructuras esenciales. La Unión Europea, reconociendo la importancia estratégica de los cables submarinos, emitió en febrero de 2024 un documento titulado "Recomendación sobre Infraestructuras de Cables Submarinos Seguras y Resilientes", un marco que establece medidas concretas para reforzar la seguridad y resiliencia de estas infraestructuras en todo el territorio europeo [21].

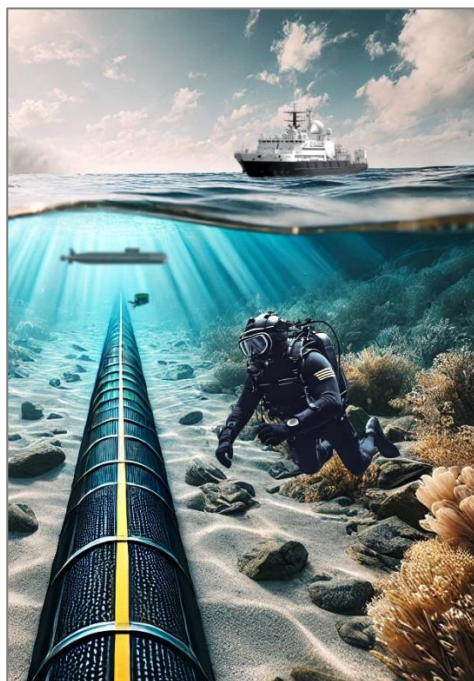


Figura 3-1. Amenazas a los cables submarinos (fotomontaje de elaboración propia).

El documento emitido por la Unión Europea subraya que los cables submarinos son esenciales para la conectividad global y la seguridad digital de la región, ya que gestionan la mayor parte del tráfico de datos internacionales. Sin embargo, también señala que estos cables son vulnerables a una serie de riesgos, incluidos sabotajes, ataques físicos, ciberataques y cortes de energía. Estas amenazas, de materializarse, podrían tener graves repercusiones económicas y de seguridad para los Estados

miembros de la Unión Europea. Reconociendo estas vulnerabilidades, la recomendación destaca la necesidad de un enfoque coordinado entre los países europeos para proteger estas infraestructuras, mejorar su seguridad y garantizar su funcionamiento frente a amenazas, en particular aquellas que puedan provenir de actores externos, ya sean estatales o no estatales.

La recomendación no solo identifica los riesgos, sino que también establece un enfoque integral que abarca tanto la seguridad física como la ciberseguridad de los cables submarinos. Este enfoque refleja la importancia estratégica de estas infraestructuras para la soberanía digital de Europa, así como para la estabilidad económica y la capacidad de defensa tecnológica del continente. Además, enfatiza la importancia de la inversión pública y privada para fortalecer estas infraestructuras vitales, fomentando la resiliencia frente a amenazas modernas y promoviendo la independencia tecnológica. Uno de los aspectos más destacados del documento es su insistencia en la necesidad de una coordinación internacional sólida como base para enfrentar amenazas que trascienden fronteras, especialmente en un contexto geopolítico en el que actores con intenciones hostiles podrían atacar estas infraestructuras críticas.

A pesar de su enfoque integral, el éxito de las medidas propuestas en el documento dependerá en gran medida de la capacidad de los Estados miembros para implementarlas de manera efectiva. La cooperación interna y la colaboración internacional son pilares fundamentales para garantizar que estas medidas sean aplicadas con éxito y puedan adaptarse rápidamente a un panorama de amenazas en constante evolución. Además, la agilidad en la adopción de nuevas tecnologías y la implementación de medidas frente a amenazas emergentes serán claves para lograr los objetivos establecidos en la recomendación. Esto es particularmente relevante en un entorno global en el que los ataques a infraestructuras críticas están adquiriendo formas más sofisticadas, combinando amenazas físicas y cibernéticas.

En lo que respecta a las TIC, el documento citado incluye un punto destacado, el número 15, en el que insta a "debatir las posibilidades de adopción y despliegue de soluciones innovadoras para detectar y prevenir las amenazas a las infraestructuras de cables submarinos". Esta llamada a la innovación tecnológica reconoce el papel esencial de las TIC en la protección y monitorización de estas infraestructuras críticas. Siguiendo esta línea, el presente trabajo incluye un capítulo específico en el que se proponen soluciones tecnológicas innovadoras destinadas a abordar las amenazas identificadas. Estas propuestas buscan no solo responder a las necesidades actuales, sino también anticiparse a futuras vulnerabilidades mediante el uso de tecnologías avanzadas que refuercen la seguridad y resiliencia de los cables submarinos en un entorno global cada vez más complejo y desafiante.

La OTAN ha tomado recientemente un paso significativo hacia la protección de infraestructuras críticas submarinas mediante la creación del Centro Marítimo para la Seguridad de las Infraestructuras Críticas Submarinas [23]. Este centro tiene como misión garantizar la seguridad de miles de kilómetros de tuberías y cables submarinos que son fundamentales para el suministro energético, las comunicaciones globales y la actividad económica. Estas infraestructuras, debido a su ubicación remota y al entorno en el que operan, son especialmente vulnerables a ataques dirigidos a interrumpir sus funciones, con el potencial de causar consecuencias devastadoras a nivel internacional. La iniciativa de la OTAN busca no solo proteger estos recursos esenciales, sino también reforzar la capacidad de los Estados miembros para prevenir y responder a amenazas que afecten directamente a su seguridad y estabilidad.

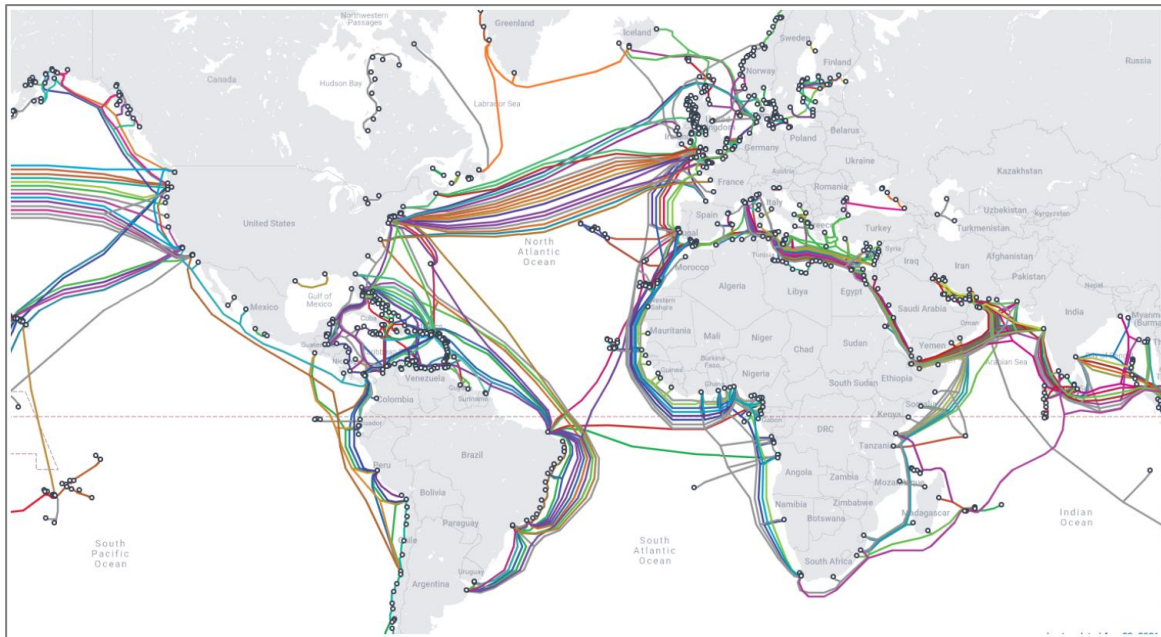


Figura 3-2. Foto de inauguración del Centro Marítimo de la OTAN para la Seguridad de Infraestructuras Críticas Submarinas [23].

En el marco de este esfuerzo, se destaca en diversos análisis la implementación de sensores submarinos que tendrán la capacidad de monitorizar actividades sospechosas y atribuir responsabilidades a actores malintencionados. Esta capacidad de atribución es clave en un entorno geopolítico en el que los sabotajes y las actividades encubiertas están en aumento, y donde la falta de claridad sobre los responsables puede complicar las respuestas diplomáticas y operativas. Sin embargo, el uso del futuro como forma verbal en la descripción de estas capacidades pone de manifiesto que, a día de hoy, todavía existe un largo camino por recorrer en lo que respecta a la seguridad efectiva de los cables submarinos. Aunque se han dado pasos significativos en términos de concienciación y planificación, la implementación de medidas tangibles que logren proteger estas infraestructuras críticas sigue siendo un desafío en evolución.

A nivel nacional, el compromiso con la protección de estas infraestructuras críticas también se ha evidenciado en foros estratégicos como el XIV simposio transregional del poder naval, celebrado en octubre de 2024 en Venecia, Italia [24]. Durante este evento, el Almirante Jefe de Estado Mayor de la Armada (AJEMA) presentó una ponencia centrada en los retos actuales relacionados con la seguridad de las infraestructuras submarinas críticas, incluyendo los cables submarinos. En su intervención, el AJEMA subrayó la necesidad de incorporar nuevas tecnologías como una herramienta esencial para mejorar la eficiencia y la eficacia de las medidas destinadas a proteger estas infraestructuras. Estas tecnologías emergentes, aunque aún en fases de desarrollo, se consideran fundamentales para enfrentar los retos que presentan los avances en capacidades ofensivas de actores estatales y no estatales.

Tanto a nivel nacional como internacional, se observa un consenso creciente sobre la importancia de las tecnologías emergentes y disruptivas en la protección de infraestructuras críticas submarinas. Sin embargo, estas tecnologías aún son vistas como una solución futura, lo que pone de manifiesto la necesidad de actuar con prontitud para acelerar su desarrollo e implementación. En este sentido, la cooperación civil-militar, junto con un respaldo político firme, es considerada indispensable para abordar los retos actuales y futuros. La integración de sensores avanzados, herramientas de monitorización en tiempo real y sistemas de análisis predictivo permitirá fortalecer las capacidades defensivas y garantizar la resiliencia de estas infraestructuras en un entorno geopolítico marcado por amenazas complejas y en constante evolución. Estas iniciativas deben ser acompañadas por políticas coherentes y una coordinación internacional efectiva, aspectos que resultan cruciales para traducir estas visiones estratégicas en resultados concretos y sostenibles.



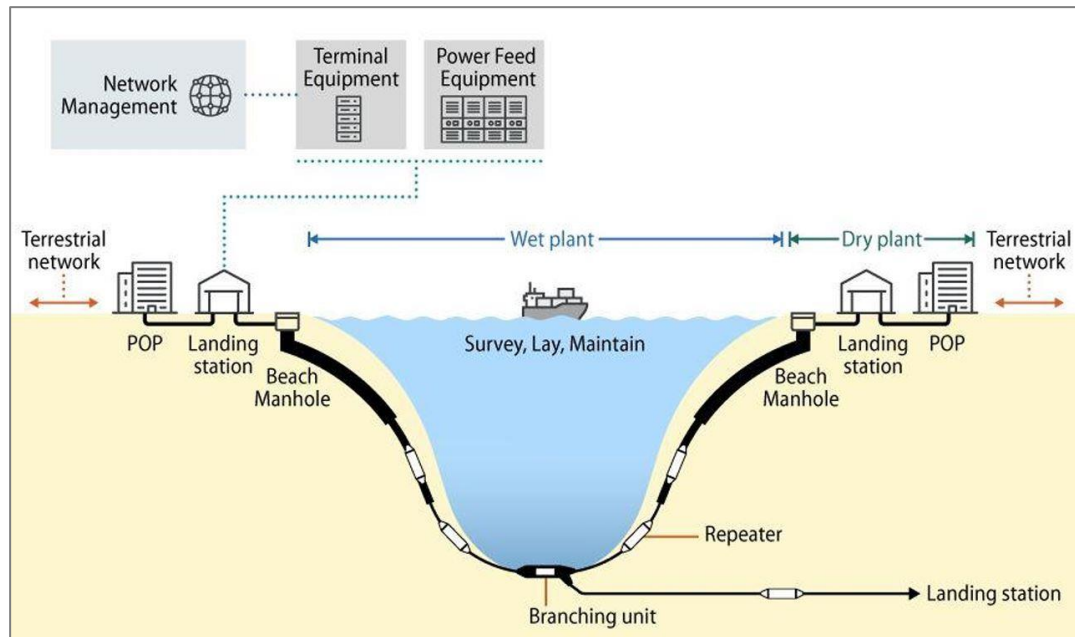


Figura 3-4. Ejemplo de un sistema de telecomunicaciones mediante cable submarino [27].

Un aspecto clave de los cables submarinos es su capacidad para soportar grandes volúmenes de datos simultáneamente, utilizando tecnologías de transmisión óptica de última generación. Los cables de fibra óptica, que son los más comunes hoy en día, tienen una capacidad mucho mayor en comparación con los cables de cobre antiguos [28].

3.4.1.1 Cables submarinos de fibra óptica

Los cables de fibra óptica tienen una capacidad de transmisión de datos superior a los cables de cobre. Pueden manejar enormes volúmenes de datos a velocidades extremadamente altas, con la capacidad de transmitir señales en múltiples longitudes de onda de luz, lo que se conoce como multiplexación por división de longitud de onda (WDM). Están diseñados para resistir la presión y las condiciones adversas del fondo marino, como la corrosión y las tensiones mecánicas.

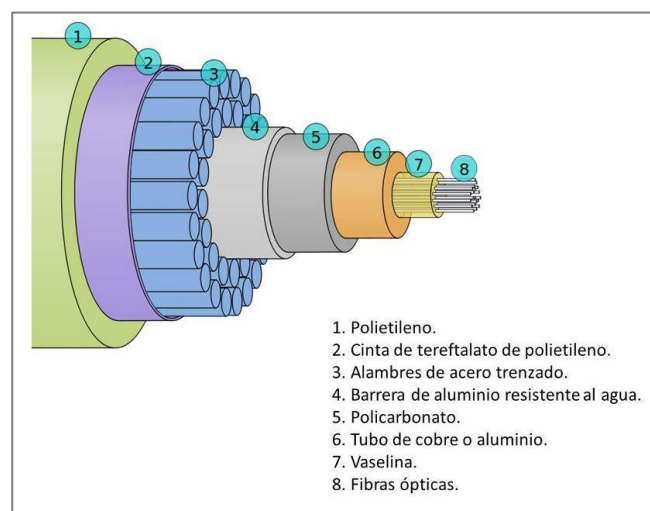


Figura 3-5. Ilustración de un cable de fibra óptica [10].

Son el tipo más común de cable submarino utilizado en las telecomunicaciones modernas, que abarcan desde el acceso a Internet hasta la telefonía internacional y las redes empresariales globales.

Estos cables interconectan continentes y son la columna vertebral de la conectividad global para servicios como el comercio electrónico, las operaciones financieras en tiempo real, los servicios en la nube y la transmisión de datos masivos.

3.4.1.2 Cables submarinos de energía

Estos cables están diseñados para transmitir electricidad de alta potencia entre continentes o islas, a través de canales submarinos. Pueden ser de cobre o aluminio, con un aislamiento robusto para evitar pérdidas de energía y resistir el ambiente marino [29]. Transmiten energía a altas tensiones y corrientes, por lo general en sistemas de corriente continua (DC), lo que permite largas distancias sin pérdidas significativas de energía.



Figura 3-6. Ilustración de un cable submarino eléctrico [30].

Estos cables se utilizan para conectar redes eléctricas entre continentes o entre países separados por el mar, como los cables entre el Reino Unido y Francia, o entre España y Marruecos [30]. Además, estos cables permiten la transferencia de energía entre regiones que carecen de suficientes recursos energéticos locales, facilitando la eficiencia en el uso de las energías renovables y la estabilidad de las redes eléctricas. Su importancia estratégica es considerable porque aseguran la diversificación de las fuentes de energía y la resiliencia de las redes eléctricas, un aspecto clave en la política energética internacional.

3.4.1.3 Cables submarinos multipropósito (comunicaciones y energía)

Estos cables combinan fibras ópticas para transmisión de datos con conductores eléctricos para transmitir energía. Este diseño permite proporcionar tanto servicios de telecomunicaciones como energía en una sola infraestructura. A menudo, se utilizan en proyectos de infraestructura donde tanto la transmisión de energía como las telecomunicaciones son necesarias. Son especialmente valiosos en proyectos industriales complejos, ya que proporcionan una solución integral que optimiza los costes de construcción y mantenimiento de la infraestructura energética y de telecomunicaciones.

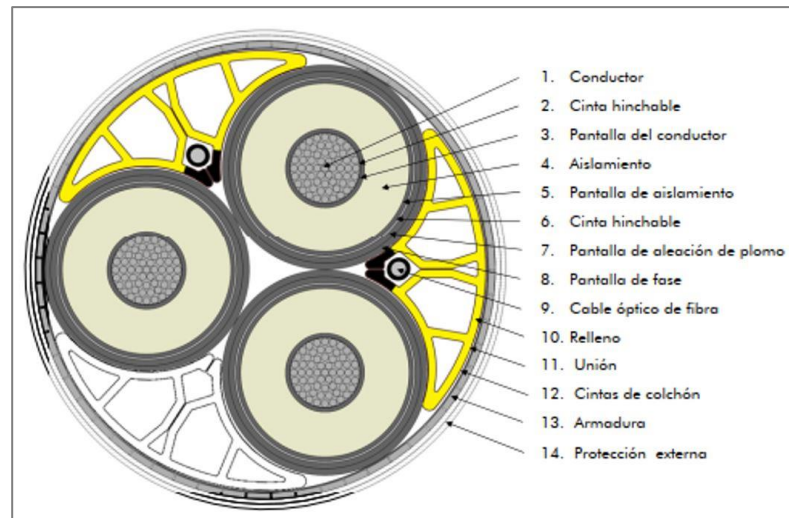


Figura 3-7. Ilustración de un cable submarino de energía y comunicaciones [29].

3.4.2 Protección física de los cables submarinos

Los métodos de protección de los cables submarinos son técnicas diseñadas para garantizar la integridad y el funcionamiento de estas infraestructuras críticas frente a amenazas naturales y humanas. Dado que estos cables son fundamentales para las telecomunicaciones globales, es esencial implementar estrategias eficaces para prevenir daños y garantizar su operatividad a largo plazo [31].

3.4.2.1 Método preferente de protección: Enterramiento

El enterramiento es uno de los métodos más comunes y efectivos para proteger los cables submarinos. Consiste en excavar zanjas en el lecho marino y enterrar los cables a profundidades de uno a tres metros. Este método es particularmente útil en zonas costeras o áreas con alta actividad marítima, donde los cables están expuestos a riesgos como la pesca de arrastre o las anclas de los barcos [29]. A continuación, se analiza más en detalle los distintos tipos de modos de protección de cables basados en técnicas de enterramiento.

3.4.2.1.1 Enterramiento “plough”

Un enterramiento *plough* o arado de enterramiento es una herramienta utilizada en la instalación de cables submarinos y tuberías, especialmente en el lecho marino. Este equipo se utiliza para enterrar el cable o tubería en el fondo marino, protegiéndolo de posibles daños por anclas de barcos, fauna marina y otras amenazas.



Figura 3-8. Enterramiento *plough* o arado de enterramiento [29].

El arado tiene una forma que le permite cavar en el lecho marino mientras se tira de él por un barco. Tiene una parte frontal afilada que corta el sedimento, creando un canal donde se puede colocar el cable o tubería. A medida que el arado avanza, desplaza el sedimento hacia un lado y permite que el cable se introduzca en el canal creado. Después de que el cable se coloca, el sedimento se vuelve a asentar sobre él, cubriéndolo y proporcionando protección. Este método es rápido y eficiente, ya que permite el enterramiento de cables y tuberías a profundidades significativas en un solo paso, en comparación con otros métodos que pueden requerir múltiples etapas.

Se utiliza en proyectos de instalación de cables de telecomunicaciones, interconexiones eléctricas submarinas, y en la industria del petróleo y gas para el enterramiento de tuberías. Al enterrar los cables o tuberías, se reduce el riesgo de daños mecánicos y se aumenta su vida útil.

3.4.2.1.2 Enterramiento “*jeting*”

El enterramiento *jeting* utiliza un equipo que inyecta agua a alta presión para crear un canal donde se pueda colocar el cable o la tubería.



Figura 3-9. Sistema para realizar enterramiento *jeting* [29].

El sistema *jeting* utiliza boquillas que expulsan agua a alta presión. Esta presión ayuda a crear un surco en el sedimento, permitiendo que el cable o la tubería se introduzcan en el lecho marino. El equipo de *jeting* suele estar montado en un barco o en una plataforma y puede ser operado de forma remota. Las boquillas se colocan en la parte inferior y son dirigidas hacia el fondo marino. Este método es muy eficiente en sedimentos blandos, ya que puede enterrar el cable o la tubería a profundidades significativas rápidamente.

3.4.2.1.3 Enterramiento “trencher”

El enterramiento *trencher* es una técnica utilizada para enterrar cables y tuberías en el lecho marino. Este dispositivo excava un canal en el fondo marino donde se puede colocar el cable o la tubería, proporcionando así una protección efectiva contra daños.



Figura 3-10. Equipo para efectuar enterramiento *trencher* [29].

Los *trenchers* son equipos especializados que pueden ser de diferentes tipos, como de rueda, de cadena o de cuchilla y adaptarse a diferentes tipos de sedimentos, desde arenas suaves hasta materiales más duros. Estos dispositivos están diseñados para excavar y mover sedimentos del fondo marino, creando un surco para enterrar el cable o la tubería. A medida que el equipo avanza, el cable o la tubería se colocan en el canal recién excavado y en algunos casos, también puede ayudar a rellenar el canal después de la instalación. Los *trenchers* pueden excavar a diversas profundidades, lo que permite enterrar los cables o tuberías a niveles adecuados para protegerlos de los daños.

3.4.2.2 Métodos alternativos de protección externa

Los métodos alternativos de protección externa son soluciones válidas para la protección de cables submarinos allá donde las técnicas de enterramiento no son viables, como lechos marinos rocosos o zonas con alta actividad geológica [32]. Entre ellos cabe citar las técnicas de vertidos de roca y los colchones de cemento, los cuales se analizan a continuación.

3.4.2.2.1 Vertido de roca

Consiste en la colocación de rocas o bloques de material en el fondo marino para crear una barrera que proteja los cables o estructuras de daños mecánicos y ambientales. Este método es especialmente útil en áreas donde hay riesgos de erosión, impacto de anclas de barcos o actividad marina intensa.

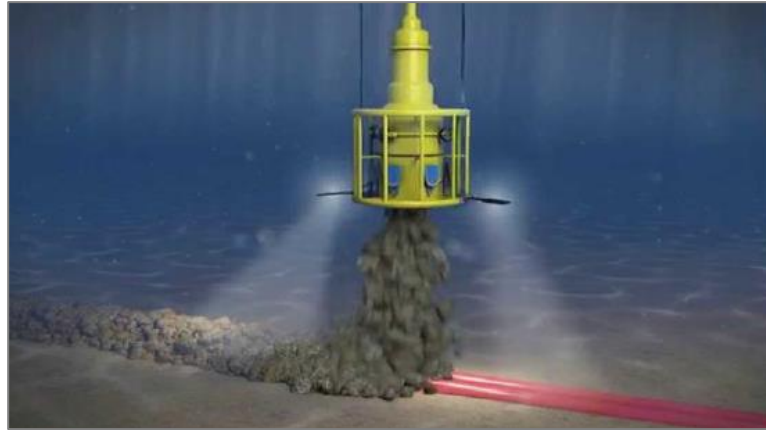


Figura 3-11. Vertido de roca para proteger externamente el cable submarino [29].

Se emplean rocas, bloques de cemento o material similar que se vierten o se colocan en el fondo marino. Las piedras pueden variar en tamaño y forma, y se eligen en función de la profundidad del agua y las condiciones del fondo marino. Las rocas proporcionan una protección sólida y duradera, capaces de resistir las condiciones adversas del entorno marino. Al actuar como una barrera, la protección por vertido de roca reduce el riesgo de daños a cables y estructuras por anclas de barcos, fauna marina y movimientos del lecho marino. Este método ayuda a estabilizar el lecho marino alrededor de los cables y tuberías, evitando la erosión y el desplazamiento del sedimento.

En cuanto a inconvenientes, el coste de transporte de las rocas y su colocación puede ser alto, especialmente si se utilizan rocas grandes o pesadas. Con el tiempo, las rocas pueden ser desplazadas por corrientes marinas, lo que puede reducir su efectividad como barrera protectora. También puede ser necesario realizar mantenimientos periódicos para reponer o ajustar las rocas. Además, la instalación puede verse afectada por condiciones meteorológicas adversas, como fuertes corrientes u oleaje, lo que puede complicar el vertido de rocas. Así mismo, en áreas remotas o difíciles de acceder, la logística de transporte y colocación de rocas puede ser un desafío.

3.4.2.2 Colchones de cemento

Los colchones de cemento son estructuras que se colocan sobre el lecho marino, proporcionando una protección adicional a los cables submarinos. El peso del colchón ayuda a mantener el cable en su lugar, evitando movimientos que puedan causar tensiones.



Figura 3-12. Colchón de cemento para proteger el cable submarino [29].

Los colchones absorben y distribuyen el impacto de objetos móviles en el agua, como barcos o tormentas, minimizando el riesgo de daño. Dichos colchones se despliegan cuidadosamente sobre el

cable ya instalado y se utilizan técnicas de anclaje para asegurar que se mantengan en su lugar, especialmente en áreas con corrientes fuertes.

Como ventaja, los colchones de cemento son resistentes a la corrosión y a los elementos, garantizando una larga vida útil. Pueden diseñarse en diferentes tamaños y formas, adaptándose a diversas condiciones del fondo marino. Su uso reduce significativamente el riesgo de daño por pesca de arrastre, anclajes de barcos y otros impactos. Como desventaja, la fabricación e instalación de colchones de cemento puede ser costosa, lo que requiere una evaluación cuidadosa de su viabilidad económica.

3.5 Amenazas a la seguridad de los cables submarinos

En este capítulo se describirán aquellas amenazas en las que el ser humano se ve involucrado, ya sea de forma accidental o de forma intencionada. Si bien es cierto que las amenazas naturales pueden provocar daños de una intensidad similar a los provocados por el ser humano, no se analizarán al no ser objeto de este trabajo.

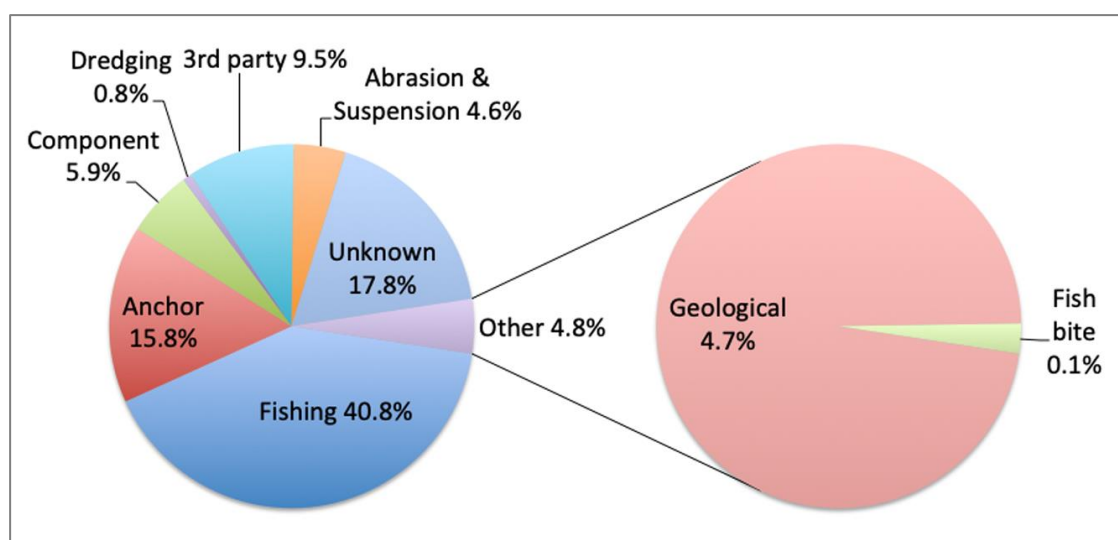


Figura 3-13. Porcentaje de cortes o roturas de cables relacionadas por diferentes causas desde 1959 hasta 2021 [33]

3.5.1 Amenazas humanas accidentales

Los cables submarinos son vulnerables a daños no intencionados, principalmente causados por anclas de barcos, equipos de pesca, y fenómenos naturales como terremotos o deslizamientos de tierra. Cada año se cortan entre 100 y 150 cables, mayormente por actividades humanas accidentales [34].

Por citar algún ejemplo, en mayo de 2024, frente a la costa de Sudáfrica, el arrastre del ancla de un buque dañó dos cables submarinos, afectando significativamente la conectividad a Internet en África Oriental [35].

3.5.2 Amenazas humanas intencionadas

Las amenazas humanas intencionadas a los cables submarinos se refieren a acciones deliberadas que buscan dañar, interrumpir o explotar estas infraestructuras críticas. Estas amenazas incluyen actos de sabotaje, espionaje y otras actividades maliciosas que pueden comprometer la integridad de las comunicaciones globales.

3.5.2.1 *Sabotajes y actos de vandalismo*

Los sabotajes a cables submarinos constituyen una amenaza creciente, especialmente en el actual contexto de tensiones geopolíticas. Estas infraestructuras, que sostienen la mayor parte de las comunicaciones globales, son vulnerables a ataques por parte de países con capacidades técnicas y militares avanzadas [1], [7]. Para algunas naciones, los actos de sabotaje pueden ser herramientas estratégicas para ejercer presión sobre sus adversarios o formar parte de estrategias más amplias en escenarios de conflicto. Este tipo de ataques, que a menudo son encubiertos, resaltan la fragilidad de estas infraestructuras críticas y la necesidad de fortalecer sus sistemas de protección para evitar consecuencias devastadoras [9].

Los motivos detrás de estos sabotajes suelen estar ligados a intereses políticos, económicos o estratégicos. En un mundo cada vez más interconectado, los cables submarinos son esenciales para garantizar el flujo de datos que sustenta actividades fundamentales como las transacciones financieras, las comunicaciones gubernamentales y el comercio internacional [2]. Debido a su importancia, estas infraestructuras se convierten en objetivos clave para aquellos actores que buscan desestabilizar a sus oponentes. Los métodos empleados para sabotear cables submarinos son diversos: pueden incluir cortes físicos, realizados mediante embarcaciones pesqueras o navales, así como interferencias electrónicas capaces de alterar las señales transmitidas a través de las fibras ópticas [13]. Estas tácticas, aunque diferentes, comparten un objetivo común: interrumpir la conectividad y generar caos en las naciones afectadas.

Las consecuencias de un sabotaje a estas infraestructuras no se limitan al país directamente atacado; su impacto puede ser global. A nivel local, el daño a un cable submarino puede paralizar servicios esenciales como la banca, la atención médica o las comunicaciones, desencadenando crisis nacionales de gran magnitud [14]. Por ejemplo, la interrupción de un cable que conecta un país en desarrollo con mercados internacionales podría dificultar las operaciones empresariales, derivar en pérdidas económicas significativas y erosionar la confianza de los inversores. Este tipo de eventos tiene el potencial de afectar la estabilidad económica de regiones enteras, especialmente aquellas con menor capacidad para diversificar su conectividad [1].

A nivel global, los sabotajes generan efectos aún más amplios debido a la naturaleza interconectada de las infraestructuras de comunicación. Los cables submarinos constituyen la columna vertebral de la transferencia de datos entre continentes, y su interrupción puede congestionar las redes alternativas, provocando un efecto dominó que afecta a múltiples países. Esto no solo retrasa la transferencia de datos y las operaciones comerciales, sino que también genera incertidumbre y desconfianza en los mercados globales [9].

El impacto del sabotaje también se extiende a las relaciones diplomáticas entre naciones. Cuando un país es percibido como responsable de un sabotaje, pueden surgir represalias económicas, sanciones internacionales e incluso escaladas militares [7]. Este tipo de desconfianza deteriora la cooperación en temas críticos como la seguridad, el comercio y la sostenibilidad ambiental. Por ejemplo, un ataque a un cable submarino atribuido a una nación rival podría intensificar las tensiones diplomáticas, contribuyendo a la polarización y a la formación de bloques de países que se ven mutuamente como amenazas. A largo plazo, estos incidentes alimentan un clima de desconfianza global que dificulta la colaboración en asuntos de interés común [15].

Desde una perspectiva de seguridad nacional, los sabotajes a cables submarinos obligan a los gobiernos a reevaluar sus estrategias de defensa y a destinar mayores recursos a la protección de infraestructuras críticas. Esto incluye la implementación de medidas más estrictas, como la monitorización constante mediante tecnologías avanzadas y la presencia naval en áreas vulnerables [24]. Sin embargo, estas acciones también tienen consecuencias estratégicas, ya que la militarización de ciertas rutas marítimas puede exacerbar las tensiones en regiones conflictivas. Este proceso no solo aumenta el riesgo de enfrentamientos directos, sino que también fomenta una carrera armamentista en tecnología de monitorización y defensa, elevando aún más la complejidad del panorama geopolítico actual [7].

El sabotaje a cables submarinos puede responder a diversas motivaciones que abarcan intereses políticos, estratégicos y económicos. Comprender estas motivaciones no solo es crucial para prevenir los ataques, sino también para diseñar estrategias efectivas que mitiguen su impacto. Estas amenazas pueden provenir tanto de actores estatales como no estatales, lo que incrementa su complejidad. Además, los sabotajes suelen centrarse en vulnerabilidades tanto físicas como cibernéticas, explotando los puntos débiles de una infraestructura que resulta esencial para la conectividad global [13]. La diversidad de los motivos y las capacidades de los posibles perpetradores subraya la necesidad de una comprensión profunda y un enfoque integral para abordar estos riesgos.

En el ámbito político, los sabotajes a cables submarinos suelen ser utilizados como herramientas para ejercer presión en el marco de tensiones geopolíticas. Los estados pueden recurrir a estas tácticas para interrumpir las comunicaciones de un adversario, debilitando así su capacidad de respuesta y obteniendo una ventaja táctica en un conflicto. Este tipo de ataques puede ser particularmente efectivo en contextos de inestabilidad política, donde las interrupciones en las comunicaciones socavan la confianza pública en los líderes del gobierno y generan caos. Asimismo, los sabotajes pueden servir como un medio para que un país demuestre su poder o dominio en una región específica, enviando un mensaje estratégico a sus rivales sobre su capacidad de influir en la dinámica regional. Un ejemplo de ello son las declaraciones de funcionarios rusos, en el contexto de la guerra en Ucrania, que insinuaron que el país podría atacar cables de comunicación submarinos como represalia por sanciones internacionales, lo que ilustra el uso del sabotaje como herramienta política [36].

Los intereses económicos también juegan un papel destacado en los sabotajes a cables submarinos. Al interrumpir las comunicaciones de competidores, actores estatales o grupos organizados pueden intentar obtener ventajas significativas en mercados clave. Esto es particularmente relevante en sectores como la banca, las finanzas y el comercio, donde la rapidez en las comunicaciones es crucial para garantizar operaciones eficientes [37]. La congestión de las redes causada por un sabotaje puede generar retrasos, aumentar los costos para las empresas dependientes de estas comunicaciones y, en última instancia, desestabilizar economías enteras. Además, la percepción de que un país es vulnerable a estos ataques puede desincentivar la inversión extranjera, afectando negativamente la economía local. Los sabotajes de este tipo no solo causarían pérdidas directas, sino que también erosionan la confianza en la infraestructura crítica de una región [38].

En algunos casos, el sabotaje de cables submarinos forma parte de estrategias más amplias en conflictos prolongados. Al interrumpir la conectividad, un atacante puede limitar el flujo de información hacia y desde un país, debilitando su capacidad para responder de manera efectiva a situaciones de crisis. En conflictos donde la información es un recurso estratégico, la interrupción de comunicaciones puede representar un golpe crítico a las capacidades operativas de un adversario. Esta

vulnerabilidad se agrava aún más cuando se considera la dependencia de ciertos países, como China, para la reparación de cables dañados [1]. En escenarios de hostilidad, China podría limitar o retrasar dichas reparaciones, dejando a los países afectados sin servicio durante largos periodos. Además, estos sabotajes físicos pueden complementarse con ciberataques, creando un entorno caótico que amplifica la efectividad de las operaciones hostiles.

Otra preocupación creciente es el papel de actores estatales, particularmente China, en la construcción y mantenimiento de cables submarinos. Existe el riesgo de que estas naciones utilicen su posición estratégica para espiar o monitorizar los datos que fluyen a través de los cables que construyen o mantienen [39]. Esta capacidad no solo plantea riesgos de interceptación de datos en tiempos de paz, sino que también podría facilitar interrupciones a gran escala en periodos de conflicto, incluyendo el corte total de acceso a internet para países enteros. Estas posibilidades resaltan la complejidad del sabotaje a cables submarinos, que combina vulnerabilidades físicas y cibernéticas, y subrayan la necesidad de medidas preventivas y colaborativas que aborden estas amenazas de manera integral.

3.5.3 Ejemplos recientes de posibles sabotajes

Entre los ejemplos recientes de daños sufridos por los cables submarinos debido posiblemente a sabotajes, cabe mencionar el incidente en 2023 donde Taiwán acusó a dos barcos chinos de cortar los cables submarinos que proporcionaban internet a las islas Matsu, afectando a unos 14.000 residentes. El primer incidente ocurrió el 2 de febrero, cuando un pesquero chino cortó uno de los cables a unos 50 kilómetros de la costa. Seis días después, el 8 de febrero, un carguero chino dañó el segundo cable. Estos cortes dejaron a las islas Matsu sin conexión estable a internet durante semanas, obligando a los residentes a depender de transmisiones limitadas a través de microondas de radio como respaldo. La interrupción del servicio complicó actividades cotidianas como pagar facturas, concertar citas médicas y gestionar negocios locales. Aunque el gobierno taiwanés no acusó directamente a Pekín de una acción deliberada, algunos expertos sugieren que estos actos podrían formar parte de una estrategia de acoso por parte de China hacia Taiwán [12].



Figura 3-14. Mapa ilustrativo de los puntos de corte de los cables submarinos en Taiwán [40].

Otro incidente reciente destacado fue el corte del cable C-Lion1 en el mar Báltico, ocurrido el 17 de noviembre de 2024 [8]. Este incidente involucró al buque chino Yi Peng 3, sospechoso de haber cortado los cables en un posible acto de sabotaje. Tras semanas de negociaciones diplomáticas, el gobierno chino permitió que investigadores europeos abordaran el barco para recopilar pruebas. Aunque se investigó si el capitán del buque había sido sobornado por inteligencia rusa, se descartó la implicación directa de China en el caso. El incidente subraya la vulnerabilidad de las infraestructuras submarinas críticas en el Báltico y la creciente amenaza de tácticas de guerra híbrida que involucran a actores estatales y no estatales.

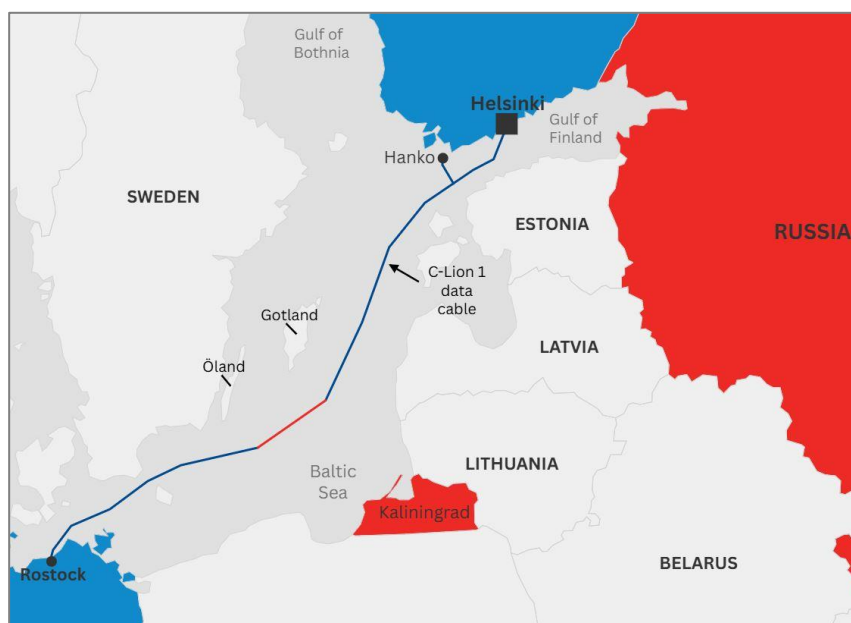


Figura 3-15. Mapa ilustrativo del cable submarino C-Lion 1. En color rojo se muestra el tramo del cable donde se produjo el incidente [41].

El último caso de posible sabotaje que ha sido informado durante la redacción de la presente memoria, fue el ocurrido el 25 de diciembre de 2024 en el mar Báltico, donde el cable submarino Estlink 2, que transporta electricidad de Finlandia a Estonia, se desconectó repentinamente de la red [42]. El buque que realizó el presunto sabotaje es el petrolero Eagle S, que según las autoridades finlandesas, el barco pudo navegar decenas de millas arrastrando el ancla por el fondo marino llegando a perderlo. El buque fue apresado y derivado hasta el fondeadero de Svartbeck, cerca del puerto petrolero de Kilpilahti, en Porvoo, donde las autoridades finlandesas se encontraban realizando una investigación penal [43].

Posiblemente, este sea el primer caso donde se hayan tomado acciones penales relacionadas con actos de sabotaje a infraestructuras submarinas.



Figura 3-16. Petrolero Eagle S y helicóptero de la Guardia Fronteriza de Finlandia [44].

3.5.4 Actores con capacidades para realizar sabotajes

La Dirección Principal de Investigación de Aguas Profundas (GUGI) del Ministerio de Defensa ruso es una agencia responsable de la investigación y el desarrollo en el ámbito de la tecnología submarina y las operaciones en aguas profundas. Su labor incluye el estudio de sistemas de defensa submarina, la exploración de recursos en el lecho marino y el desarrollo de nuevas tecnologías para submarinos y otros vehículos sumergibles [45].

Además de lo anterior, tiene encomendadas las actividades submarinas encubiertas, incluida la identificación y levantamiento de mapas e interferencia de los cables submarinos de comunicaciones.

Tal y como detalla el doctor Pérez Gil en [7], la 29ª División de Submarinos de la Marina rusa, una de las más avanzadas en operaciones de aguas profundas, y que opera bajo las órdenes de la GUGI, representa una amenaza importante para las infraestructuras críticas submarinas, especialmente los cables de telecomunicaciones que sostienen buena parte del tráfico global de información. Estas capacidades se han intensificado como parte de la estrategia de guerra híbrida de Rusia, especialmente tras la guerra en Ucrania.

Los cables submarinos, que conectan continentes y permiten el flujo de datos y comunicaciones a nivel mundial, son objetivos estratégicos para la 29ª División de Submarinos. La GUGI asigna a sus submarinos la tarea de identificar, mapear e incluso intervenir en estos cables.

La 29ª División cuenta con submarinos capaces de alcanzar grandes profundidades, como el *Losharik*, diseñado para operar hasta 6.000 metros bajo el nivel del mar [46]. Estos submarinos no solo pueden transportar equipos para operaciones de interferencia en infraestructuras, sino que también están dotados de sofisticados sensores y sistemas de comunicaciones para coordinar operaciones de inteligencia. Estas capacidades permiten a la Marina rusa alcanzar, manipular y potencialmente destruir infraestructuras submarinas críticas sin ser detectados.

Para realizar estas operaciones, Rusia emplea mini submarinos no tripulados y vehículos de operación remota (ROV), lanzados desde grandes submarinos nodriza o desde buques especializados. Estos buques, como el *Yantar* y el *Zvezdochka*, están equipados con plataformas de soporte para ROV y otros dispositivos de intervención, capaces de alcanzar y manipular infraestructura submarina en misiones a largas distancias de sus bases.



Figura 3-17. Minisubmarinos preparados para su carga en el buque ruso Yantar [7].

La Marina rusa ha desplegado estos buques en las cercanías de cables submarinos de telecomunicaciones internacionales, como los que se encuentran al oeste de la costa irlandesa [14]. Estas operaciones se realizan con frecuencia en misiones de reconocimiento y, en algunos casos, de interferencia, siendo especialmente difíciles de rastrear ya que los buques apagan sus Sistemas de Identificación Automática (AIS).

La Marina rusa también utiliza buques civiles de la Academia de Ciencias de Rusia y la Sociedad Geográfica Rusa como cobertura para estas misiones. Estos barcos, a pesar de tener un propósito declarado de investigación científica, cuentan con equipamiento sofisticado que les permite realizar tareas similares a las de la 29ª División. Este encubrimiento proporciona una manera de mantener presencia en regiones estratégicas bajo una apariencia civil, dificultando la identificación de sus actividades reales por las fuerzas de inteligencia de otros países.

La 29ª División y la GUGI siguen ampliando su capacidad de operaciones encubiertas mediante el desarrollo de nuevos buques y submarinos especializados. En construcción se encuentran unidades como el *Vicealmirante Burilichev*, una versión avanzada del buque *Yantar*, que servirá como plataforma para nuevos vehículos submarinos autónomos (UUV), y el batiscafo *Sergey Bavin*, capaz de sumergirse hasta 11.000 metros. La modernización de estas unidades les permitirá extender su rango de operación y mejorar su capacidad de maniobra en regiones alejadas, especialmente en el Ártico y el Atlántico.

La capacidad de la 29ª División de Submarinos de operar en zonas profundas le otorga una ventaja considerable para ejecutar misiones encubiertas y potencialmente agresivas contra infraestructuras submarinas de Occidente. Las operaciones de vigilancia e interferencia en los cables submarinos permiten a Rusia obtener información valiosa, realizar ataques cibernéticos indirectos e incluso destruir infraestructuras críticas en caso de conflicto. Este tipo de acciones no solo pueden afectar la capacidad de comunicación y coordinación de las naciones occidentales, sino que también minan la confianza en la seguridad de las infraestructuras globales.

Además, el uso de buques civiles y la presencia constante de buques de la GUGI en aguas internacionales indican que Rusia tiene un plan a largo plazo para monitorizar y, si es necesario, atacar estos recursos estratégicos. Con el desarrollo de nuevas tecnologías y vehículos no tripulados, la Marina rusa puede realizar estas misiones de forma encubierta y sin señales claras de su autoría, incrementando la complejidad de la defensa para la OTAN y otros países aliados.

La presencia de unidades como el *Yantar* y los avances en los submarinos nucleares de clase *Jabárovsk* sugieren que la Marina rusa se está preparando para un entorno donde el control y la manipulación de los fondos marinos serán estratégicamente cruciales, tanto en tiempos de paz como de conflicto.

3.6 Medidas de protección y prevención frente a amenazas

3.6.1 Medidas de protección convencionales actuales

El Convenio de Protección de Cables Submarinos de 1884 representa uno de los primeros esfuerzos internacionales por proteger estas infraestructuras esenciales [13]. A pesar de su relevancia histórica, este tratado no ha sido actualizado con regularidad para reflejar las amenazas contemporáneas, como los sabotajes intencionados, las tensiones geopolíticas o los ataques cibernéticos. Por otro lado, la regulación de los cables submarinos depende principalmente de las leyes de cada país dentro de su zona económica exclusiva (ZEE), donde las autoridades tienen jurisdicción para garantizar la seguridad de estas infraestructuras. Sin embargo, fuera de estas áreas, en aguas internacionales, la protección es mucho más limitada, lo que deja grandes tramos de cable expuestos a riesgos, sin una autoridad clara o recursos suficientes para salvaguardarlos de manera efectiva [13].

En ciertas zonas sensibles se han establecido áreas de exclusión alrededor de los cables submarinos, con restricciones específicas que prohíben actividades como la pesca y la navegación de embarcaciones no autorizadas. Estas medidas buscan minimizar el riesgo de daños accidentales o intencionados, creando barreras para proteger estas infraestructuras críticas. Sin embargo, dichas restricciones enfrentan importantes desafíos en su implementación y cumplimiento. A menudo, estas normas son violadas, ya sea por desconocimiento o de manera deliberada, y la falta de recursos para monitorear constantemente estas áreas dificulta hacerlas cumplir de manera efectiva. Estas limitaciones resaltan la necesidad de reforzar las estrategias de protección, especialmente en áreas donde los cables son más vulnerables.

Las patrullas marítimas y la vigilancia satelital se utilizan en puntos críticos con el fin de prevenir daños a infraestructuras críticas [47]. Estas herramientas son útiles para identificar y mitigar amenazas en áreas específicas, especialmente aquellas de alta sensibilidad estratégica. El Centro de Satélites de la Unión Europea (SatCen) desempeña un papel esencial en el análisis de actividades militares y despliegues de fuerzas, contribuyendo significativamente a la política exterior y de seguridad común de la UE. El SatCen proporciona información geoespacial precisa y oportuna, esencial para la toma de decisiones en situaciones críticas [48].

Así mismo, el Servicio de Vigilancia Marítima de Copernicus (CMS por sus siglas en inglés), implementado por la Agencia Europea de Seguridad Marítima (EMSA por sus siglas en inglés), proporciona productos de observación de la Tierra, como imágenes satelitales y productos derivados, para mejorar la comprensión y el monitoreo de las actividades en el mar. Este servicio apoya diversas funciones operativas, incluyendo seguridad marítima, protección, aduanas, aplicación de la ley, monitoreo de la contaminación marina, control de pesca y cooperación internacional [49].

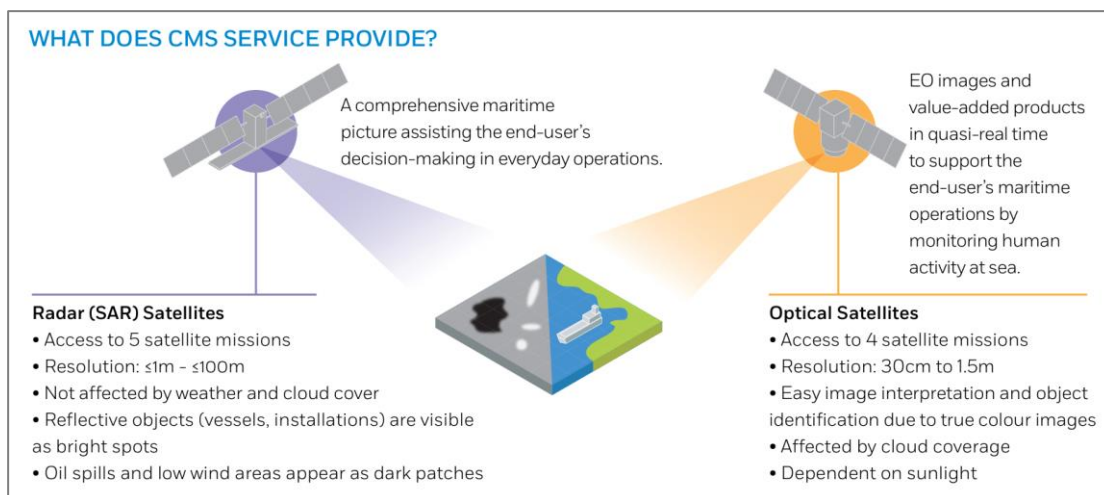


Figura 3-18. Capacidades del Servicio de Vigilancia Marítima de Copernicus [49].

Sin embargo, implementar un sistema de monitoreo continuo y exhaustivo es una tarea que implica elevados costos económicos y técnicos, lo que dificulta su sostenibilidad a largo plazo. La necesidad de cubrir vastas extensiones marinas y de garantizar una vigilancia constante subraya las limitaciones de estas estrategias, que muchas veces no logran ofrecer una cobertura adecuada para proteger toda la longitud de los cables.

Algunos países, como Estados Unidos y Reino Unido, han optado por tecnologías avanzadas para monitorear los cables submarinos en zonas críticas. Entre estas tecnologías se encuentran los UUV y los drones submarinos, que permiten detectar de forma temprana actividades sospechosas alrededor de los cables [50]. Este enfoque proporciona información valiosa que puede ser utilizada para tomar decisiones preventivas en tiempo real y responder a posibles amenazas antes de que ocurran daños significativos. Estas herramientas son particularmente útiles en áreas de alta sensibilidad, donde las actividades humanas o geopolíticas representan un mayor riesgo para la integridad de los cables.



Figura 3-19. Ejemplo de un vehículo submarino autónomo (UUV) [50].

3.6.2 Desafíos y limitaciones actuales

En aguas internacionales, los Estados enfrentan una importante limitación en cuanto a la protección de los cables submarinos, ya que carecen de derechos exclusivos para garantizar su

seguridad. Esto significa que actores externos, ya sean estatales o no estatales, pueden operar en proximidad a estas infraestructuras sin restricciones legales claras, lo que dificulta las tareas de monitoreo y protección [8]. La ausencia de un marco regulador sólido y aplicable en estas áreas deja un vacío crítico que puede ser aprovechado para actividades como el sabotaje, la manipulación o el espionaje. Esta situación pone de relieve la vulnerabilidad inherente de los cables submarinos en aguas internacionales y la necesidad urgente de desarrollar sistemas de protección más efectivos y estrategias de cooperación internacional para abordar este desafío [39].

Sin la implementación de tecnologías avanzadas como el DAS, muchos cables submarinos permanecen sin una monitorización continua y detallada, lo que impide detectar y responder de manera oportuna a eventos como sabotajes, interferencias o daños accidentales. El DAS, al permitir la monitorización en tiempo real, representa una herramienta prometedora para abordar esta carencia, pero su implementación aún es limitada debido a factores económicos y tecnológicos. En la actualidad, gran parte de los cables submarinos en zonas menos estratégicas carecen de cualquier tipo de vigilancia activa, lo que los convierte en objetivos fáciles para quienes deseen interrumpir la conectividad global. Esta falta de monitoreo efectivo subraya la importancia de avanzar en la adopción de tecnologías innovadoras que permitan una protección más integral.

La implementación de tecnologías avanzadas, así como la vigilancia continua de los cables submarinos, conlleva costos significativos que muchos estados no están en condiciones de asumir de manera independiente. En regiones menos estratégicas o económicamente desarrolladas, la falta de recursos suficientes para invertir en medidas de protección modernas agrava aún más la vulnerabilidad de estas infraestructuras críticas. Sin un mecanismo sólido de cooperación internacional y financiamiento adicional, es improbable que estas áreas puedan beneficiarse de las tecnologías necesarias para garantizar la seguridad de los cables. Esto destaca la necesidad de establecer alianzas entre estados, organismos internacionales y actores privados para compartir recursos y responsabilidades en la protección de los cables submarinos, especialmente en contextos donde las limitaciones económicas son un obstáculo importante.

Aunque existen acuerdos y tratados internacionales diseñados para regular y proteger las infraestructuras submarinas, estos no abordan de manera adecuada las amenazas modernas que enfrentan los cables submarinos. Gran parte de estos marcos normativos fueron desarrollados en un contexto donde los riesgos asociados a sabotajes intencionados o ciberataques eran inexistentes o poco significativos. Además, muchos de estos acuerdos carecen de mecanismos efectivos de aplicación, lo que limita su utilidad en situaciones reales de amenaza. Por lo tanto, resulta imprescindible actualizar estas normativas para reflejar los desafíos contemporáneos y garantizar su aplicabilidad práctica. La creación de regulaciones específicas para los cables submarinos, que incluyan disposiciones claras sobre protección, monitoreo y atribución de responsabilidades, es una tarea prioritaria para los Estados en la búsqueda de una mayor seguridad y resiliencia en estas infraestructuras críticas.

3.6.3 Tecnologías de monitorización

La implementación de tecnologías avanzadas de monitorización se ha convertido en una necesidad crucial para garantizar la seguridad de los cables submarinos, particularmente en un contexto global en el que las amenazas como el sabotaje y las interferencias deliberadas están en aumento. Estas tecnologías permiten detectar y responder rápidamente a incidentes que podrían comprometer la integridad de estas infraestructuras críticas, minimizando los daños potenciales y fortaleciendo la resiliencia de las redes de comunicación globales. Una de las herramientas más prometedoras son los

sensores submarinos, diseñados para detectar actividades anómalas en las proximidades de los cables. Estos dispositivos, que incluyen sensores acústicos y de movimiento, son capaces de identificar buques no autorizados o vibraciones inusuales que podrían indicar un intento de corte o manipulación de los cables. Al instalar estos sensores en puntos estratégicos, se crea un sistema de alerta temprana que permite a los operadores intervenir de manera proactiva ante posibles amenazas.

Además de los sensores submarinos, la integración de sistemas de posicionamiento global (GPS) en embarcaciones que operan cerca de los cables submarinos puede ser una solución eficaz para monitorizar el tráfico marítimo en zonas sensibles. Equipar a las embarcaciones pesqueras y comerciales con GPS no solo ayuda a rastrear sus movimientos, sino que también permite detectar desviaciones de rutas seguras que podrían poner en riesgo la infraestructura submarina. Este tipo de monitorización es especialmente útil en áreas de alta densidad de tráfico marítimo, donde las actividades no autorizadas o negligentes representan un peligro significativo para los cables. Con un sistema de posicionamiento global adecuado, las autoridades pueden actuar de manera rápida y eficiente, previniendo incidentes antes de que se conviertan en problemas graves.

Otra herramienta fundamental en la monitorización de cables submarinos es el uso de satélites de vigilancia, que ofrecen una perspectiva amplia y continua de las áreas marítimas críticas [47]. Estos satélites permiten observar patrones de comportamiento en el tráfico marítimo y detectar actividades sospechosas que podrían pasar desapercibidas con sistemas de monitoreo más tradicionales. Su capacidad para cubrir vastas extensiones de océano los convierte en un recurso invaluable para complementar las tecnologías de monitorización terrestre y submarina. Además, los datos obtenidos por los satélites pueden integrarse con otros sistemas, como los sensores submarinos y el GPS, creando una red de vigilancia multifacética que fortalece significativamente las capacidades de respuesta ante incidentes.

En conjunto, estas tecnologías representan un avance importante hacia la protección de los cables submarinos frente a las amenazas modernas. Su implementación, aunque requiere inversiones significativas, es esencial para garantizar la seguridad y continuidad de las comunicaciones globales. La combinación de sensores submarinos, sistemas GPS y satélites de vigilancia proporciona un enfoque integral que aborda tanto las amenazas locales como las de mayor alcance, permitiendo una protección más completa y efectiva de estas infraestructuras críticas. Este enfoque también destaca la importancia de la cooperación internacional y el desarrollo de normativas específicas que respalden la adopción de estas tecnologías, asegurando que los cables submarinos sigan siendo una base segura y confiable para la conectividad global.

3.7 Medidas de seguridad tecnológicas de cables submarinos. Tecnología DAS

La tecnología DAS representa una innovación clave en el ámbito de la monitorización y seguridad de infraestructuras críticas, como los cables submarinos. A través de esta tecnología, se utiliza la fibra óptica no solo como un medio de transmisión de datos, sino también como un sensor distribuido capaz de detectar y registrar eventos acústicos y vibraciones en tiempo real. Esta capacidad convierte a los cables de fibra óptica en herramientas multifuncionales que pueden monitorizar grandes distancias de forma continua, proporcionando información precisa sobre su entorno y las posibles amenazas [18]. DAS ha sido adoptada en múltiples sectores, desde la detección de fugas en oleoductos hasta la vigilancia de fronteras, y en el caso de los cables submarinos, ofrece una solución avanzada para proteger estas infraestructuras frente a daños accidentales y actos intencionados. Antes de

profundizar en su funcionamiento y aplicaciones, es importante entender los principios básicos que sustentan esta tecnología y cómo se integra en sistemas de seguridad modernos.

3.7.1 Sensores basados en fibra óptica

Un sensor basado en fibra óptica es un dispositivo avanzado que emplea fibra óptica para medir diversas magnitudes físicas, como temperatura, presión, deformación y otras variables relevantes [51]. Este tipo de sensor utiliza las propiedades intrínsecas de la luz que viaja a través de la fibra para detectar cambios en el entorno de manera precisa y confiable. Al aprovechar las características únicas de la fibra óptica, estos sensores son capaces de transformar pequeños cambios en el entorno en variaciones medibles de las propiedades de la luz, como la intensidad, la fase, la longitud de onda o la polarización. Estas variaciones, a su vez, pueden ser analizadas para proporcionar datos detallados sobre las condiciones del medio que rodea la fibra. Este principio subyacente convierte a los sensores de fibra óptica en herramientas indispensables para una amplia gama de aplicaciones que requieren una monitorización precisa y fiable [16], [17], [51].

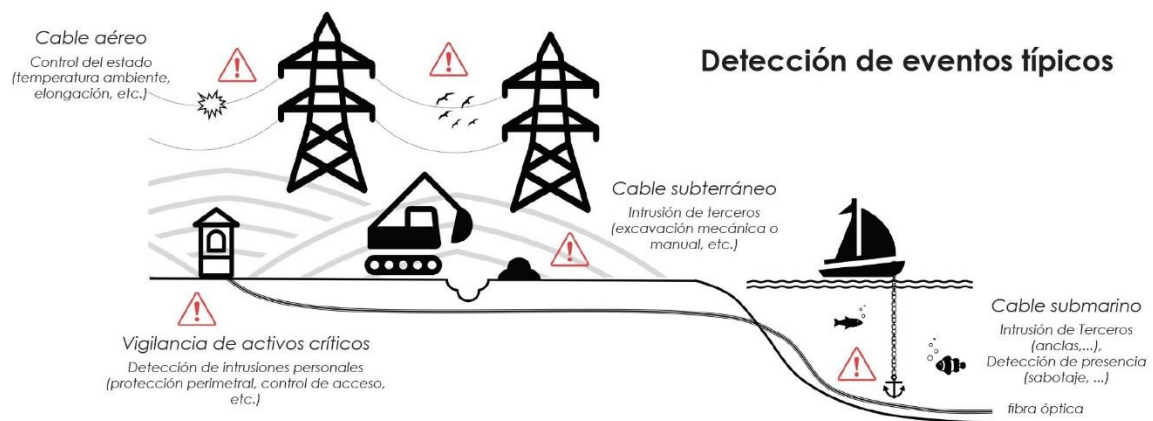


Figura 3-20. Ilustración sobre las diferentes opciones de utilización de los sensores basados en fibra óptica [51].

La tecnología detrás de estos sensores se fundamenta en la sensibilidad de la fibra óptica a los cambios físicos en su entorno inmediato. Por ejemplo, un cambio en la temperatura del entorno puede alterar la longitud de onda de la luz que viaja a través de la fibra, permitiendo medir esta variación con gran precisión. De manera similar, la presión o deformaciones mecánicas pueden influir en las propiedades ópticas de la fibra, proporcionando datos detallados sobre estas magnitudes. Este enfoque no solo garantiza un nivel de sensibilidad excepcional, sino que también permite que los sensores funcionen en entornos hostiles donde otros dispositivos tradicionales podrían fallar. La capacidad de medir con precisión incluso en condiciones adversas hace que los sensores de fibra óptica sean una opción ideal para aplicaciones en las que la fiabilidad es fundamental [16].

Los sensores de fibra óptica son especialmente valorados por su alta sensibilidad, inmunidad a las interferencias electromagnéticas y su capacidad para operar en entornos extremos. Estas características los convierten en una solución versátil y confiable en sectores tan variados como la industria, la medicina, la seguridad y la monitorización de infraestructuras críticas. Por ejemplo, en aplicaciones industriales, estos sensores se utilizan para controlar procesos en tiempo real, garantizando la seguridad y eficiencia de los sistemas. En el ámbito médico, son empleados para monitorizar parámetros fisiológicos con gran precisión y mínima intrusión [17]. En el campo de la seguridad y la infraestructura, los sensores de fibra óptica desempeñan un papel crucial en la

monitorización de puentes, edificios, túneles y cables submarinos, donde su capacidad para detectar deformaciones o vibraciones con alta sensibilidad contribuye a prevenir fallos estructurales o sabotajes [18].

En resumen, los sensores basados en fibra óptica representan una tecnología innovadora y altamente eficiente que aprovecha las propiedades de la luz para ofrecer soluciones avanzadas en monitorización y medición. Su capacidad para funcionar en condiciones extremas, junto con su alta precisión y resistencia a interferencias, los posiciona como una herramienta esencial en una amplia gama de aplicaciones. A medida que la tecnología sigue evolucionando, su papel en sectores clave, como la seguridad de infraestructuras críticas, continuará expandiéndose, proporcionando soluciones cada vez más sofisticadas y efectivas. Este avance refuerza la importancia de los sensores de fibra óptica como una pieza clave en el desarrollo de sistemas modernos de mando y control.

3.7.2 Fundamentos físicos

Los fotones en la fibra óptica tienen una cierta probabilidad de chocar con las moléculas de los materiales que la forman.

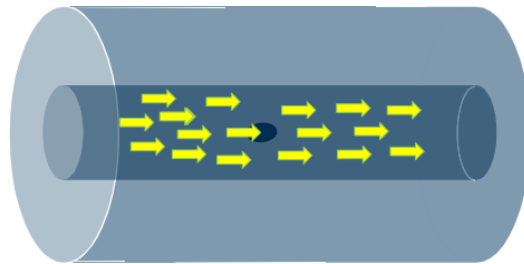


Figura 3-21. Ilustración de los fotones a través de la fibra óptica [52].

Si tras el impacto, la luz es guiada en sentido contrario, decimos que se produce “retrodifusión”.

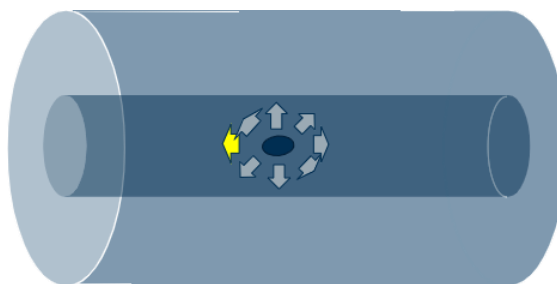


Figura 3-22. Ilustración del fenómeno de retrodifusión [52].

Si la interacción es elástica, se produce el fenómeno Rayleigh donde la luz se dispersa pero no se pierde energía; la luz sigue teniendo la misma longitud de onda en promedio. Si la interacción es inelástica, se produce la dispersión denominada Brillouin, donde la energía de la onda luminosa no se conserva completamente. Parte de esta energía se transfiere a las ondas acústicas, lo que resulta en un cambio en la longitud de onda (frecuencia) de la luz.

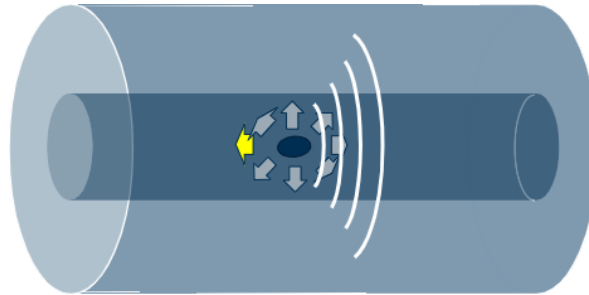


Figura 3-23. Ilustración sobre la dispersión Brillouin [52].

También existe la dispersión Raman que se refiere a un fenómeno en el que la interacción de la luz con los electrones de un material provoca excitaciones que, al volver al estado de reposo, resultan en la emisión de un fotón con una energía diferente.

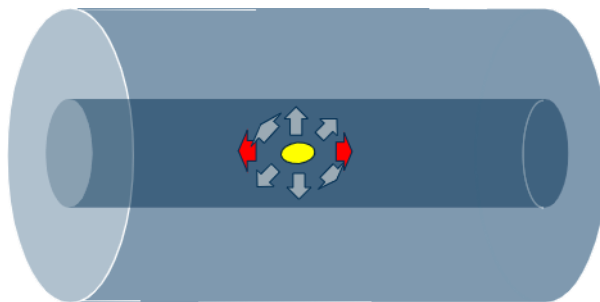


Figura 3-24. Ilustración sobre la dispersión Raman [52].

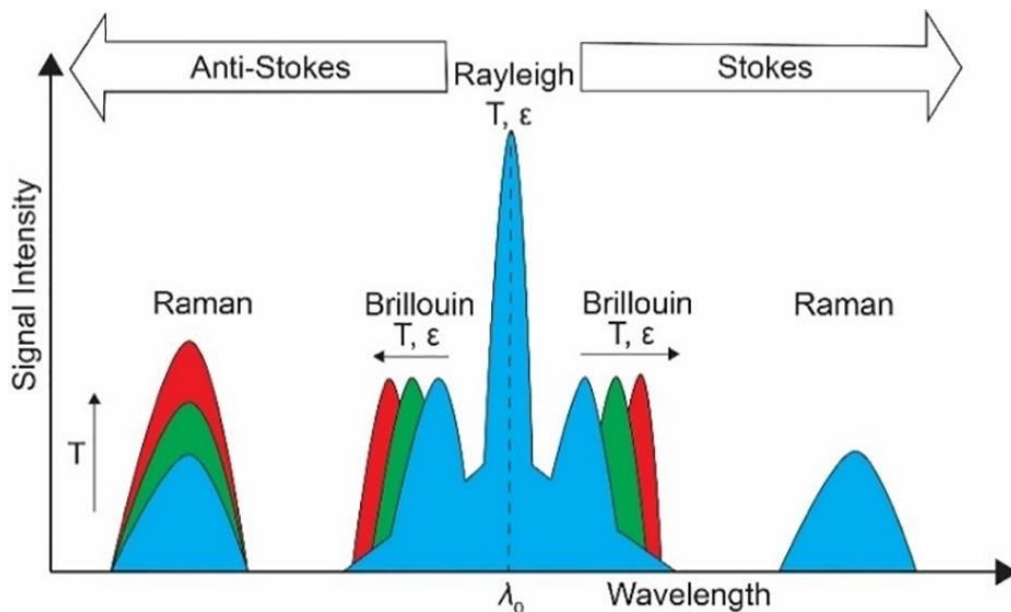


Figura 3-25. Esquema de las frecuencias en intensidades en los tres tipos de dispersión en fibras ópticas [16].

3.7.3 Sensado por retrodifusión

El DAS es una tecnología innovadora que utiliza la dispersión Rayleigh para detectar y medir vibraciones en tiempo real a lo largo de una fibra óptica, transformándola en un sensor distribuido de alta sensibilidad. Este enfoque se basa en la capacidad de las fibras ópticas para responder a cambios en su entorno, lo que permite monitorizar de manera continua y detallada una amplia gama de infraestructuras críticas. El DAS funciona según el mismo principio fundamental que el reflectómetro óptico de dominio temporal (OTDR) [53], y utiliza técnicas como la reflectometría de dominio temporal óptica coherente (C-OTDR), donde un pulso de luz es enviado a través de la fibra óptica, y a medida que la luz viaja por su interior, una pequeña parte de ella se dispersa de forma natural debido al efecto Rayleigh [16]. Este fenómeno de dispersión es altamente sensible a perturbaciones externas, como vibraciones, movimientos, cambios de temperatura o tensiones mecánicas, las cuales alteran la fase de la luz dispersada. Estas variaciones en la fase son capturadas por el sistema DAS, que las analiza para identificar y caracterizar las condiciones del entorno que afectan a la fibra.

La sensibilidad del efecto Rayleigh convierte al DAS en una herramienta excepcionalmente precisa para detectar vibraciones en tiempo real, incluso en entornos hostiles y a lo largo de grandes distancias. Esta tecnología permite monitorizar fibras ópticas con longitudes de hasta 120 kilómetros, proporcionando una cobertura extensiva que es difícil de igualar con otros sistemas de sensores. Una de las capacidades más destacadas del DAS es su capacidad para localizar eventos con una resolución espacial de 0.8 metros, en algunos casos concretos, lo que facilita la identificación de la ubicación exacta de incidentes o actividades sospechosas. Además, el DAS puede clasificar distintos tipos de actividad en función de las características de las señales que detecta, comparándolas con patrones predefinidos. Esto permite identificar no solo la presencia de vibraciones, sino también su origen, como podría ser el movimiento de vehículos, actividades humanas o interferencias mecánicas específicas [16].

Otra ventaja significativa del DAS es su potencial para integrarse con sistemas avanzados de gestión de datos, lo que amplía enormemente sus aplicaciones y efectividad. Cuando se combina con herramientas de análisis contextual, el DAS no solo registra datos brutos de vibraciones, sino que también proporciona información contextualizada que puede ser utilizada para tomar decisiones informadas en tiempo real. Por ejemplo, en la supervisión de infraestructuras críticas como cables submarinos o líneas de energía, el DAS puede detectar actividades anómalas que sugieran posibles daños o amenazas, permitiendo a los operadores actuar de manera proactiva para evitar incidentes mayores [17], [19]. Esta capacidad de supervisión continua y contextualizada convierte al DAS en una tecnología esencial para la gestión de grandes infraestructuras, donde la identificación temprana de problemas es clave para garantizar su seguridad y funcionamiento eficiente.

3.7.4 Partes de una solución DAS

Una solución DAS consta de varios componentes clave que trabajan en conjunto para detectar, procesar y analizar eventos acústicos o vibraciones a lo largo de un cable de fibra óptica.



Figura 3-26. Partes de una solución DAS [52].

3.7.4.1 Interrogador DAS

Un interrogador DAS es el dispositivo que se utiliza para enviar pulsos de luz a través de una fibra óptica y para recibir y analizar la luz que se dispersa de vuelta debido al efecto Rayleigh. Es el componente central en un sistema de monitorización de fibra óptica [54].



Figura 3-27. Diferentes modelos de interrogadores DAS (elaboración propia con imágenes de [20], [55], [56], [57]).

El interrogador emite pulsos de luz a intervalos regulares a lo largo de la fibra óptica. Posteriormente captura la luz que regresa a medida que se dispersa por las vibraciones y perturbaciones en el entorno [17].

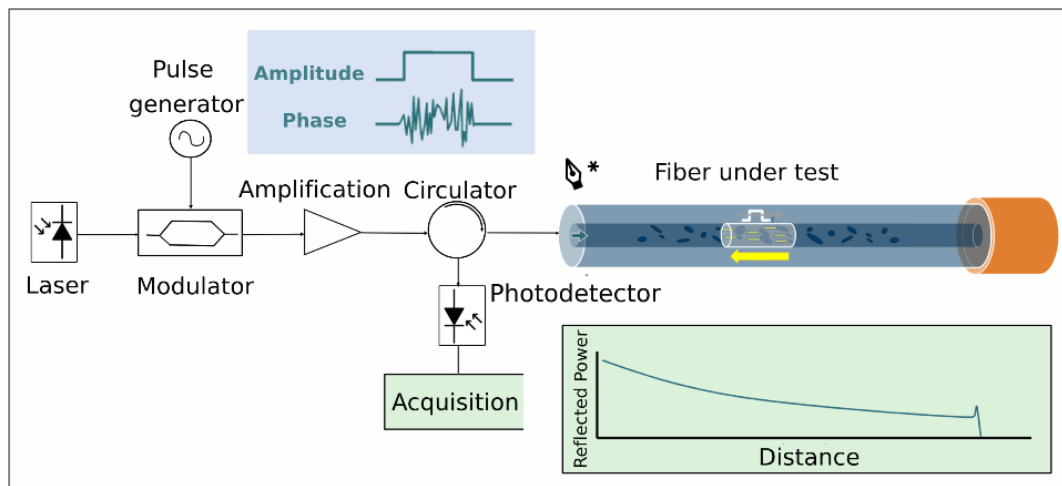


Figura 3-28. Esquema de un OTDR básico (imagen adaptada de [17]).

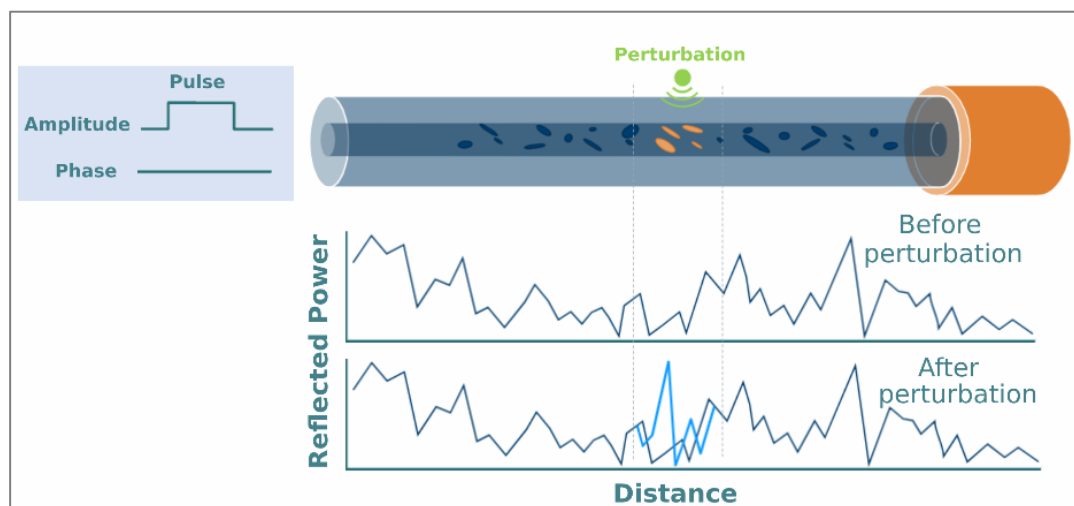


Figura 3-29. Señal registrada por un sistema C-OTDR antes y después de sufrir una perturbación [17].

A continuación se exponen los parámetros básicos de los interrogadores DAS que se comercializan actualmente. En dicha tabla se puede ver el alcance máximo sin repetidores, la resolución espacial mínima y el rango de frecuencias disponible por los diferentes interrogadores. Destacar que el interrogador que permite el mayor alcance máximo de detección sin necesidad de utilizar repetidores es el NBX-S4100 con un alcance de 120 km. Por otra parte, el interrogador DAS Terra15 permite alcanzar una resolución de sólo 80 cm, ideal para aplicaciones que requieren de mayor precisión. Por último, el interrogador FOSINA que dispone de un alcance de detección de 100 km y además puede trabajar con frecuencias de hasta 100 kHz, lo que indica una capacidad avanzada para procesar señales acústicas de alta frecuencia, permitiendo detectar, clasificar y analizar eventos con mayor precisión y resolución.

Parámetros	HDAS (Aragón Photonics)	MS- DAS2000 (Ovlink)	CRI-4400 (Halliburton)	QuantX (OptaSense)	Helio DAS (Fotech)	iDAS- MG (Silixa)	Treble+ (Terra15)	DxS (FOSINA)	NBX-S4100 (NEUBREX TECHNOLOGIES)
Alcance de detección sin repetidores (km)	70	20	50	50	40	50	30	100	120
Resolución espacial mínima (m)	10	2	1	2	1	3	0.8	1.5	1
Rango de frecuencias (kHz)	0.2 - 4	0 - 50	-	-	0.005-20	0.4- 100	0.4-100	100	0.0001-10

Tabla 3-1. Parámetros básicos de interrogadores DAS (elaboración propia adaptada de [16]).

3.7.4.2 Cable sensor

La capacidad de detección de un sensor basado en fibra óptica está intrínsecamente ligada tanto al tipo de cable utilizado como a su ubicación en relación con el objetivo que se desea monitorizar [52]. El diseño del cable, incluyendo el material de recubrimiento y las características específicas de la fibra óptica, juega un papel crucial en la sensibilidad del sensor y en su capacidad para registrar ciertas magnitudes físicas, como vibraciones, tensiones o cambios de temperatura. Por ejemplo, un cable diseñado para alta sensibilidad en entornos dinámicos será más eficaz para detectar vibraciones causadas por movimientos en su proximidad, mientras que otros tipos de cables con propiedades térmicas especializadas pueden ser más adecuados para monitorizar fluctuaciones de temperatura en infraestructuras críticas. Además, la ubicación del cable en relación con el objeto o fenómeno que se quiere detectar es igualmente determinante, ya que su proximidad o alineación puede influir directamente en la precisión y la resolución de las mediciones. Un cable situado en contacto directo con una estructura, como un puente o un gasoducto, tendrá una capacidad diferente de detección en comparación con uno que esté enterrado o sumergido en un entorno marino. Esta interdependencia entre el diseño del cable y su posicionamiento resalta la importancia de planificar cuidadosamente la implementación de sensores en función de las necesidades específicas de monitorización y las características del entorno operativo.

3.7.4.3 Análisis de eventos

Cuando se detecta un evento acústico, como una vibración o un sonido, el sistema interrogador del DAS captura la señal acústica en su forma original, conocida como señal RAW. Esta señal contiene toda la información relevante sobre el evento, incluyendo su amplitud, frecuencia y fase. Sin embargo, debido a la enorme cantidad de datos generados por un sistema DAS, con una capacidad de capturar hasta 100.000 puntos por segundo y kilómetro, resulta impracticable analizar en profundidad todas las señales detectadas. Es por ello que se hace necesario implementar estrategias avanzadas para filtrar y priorizar los datos, permitiendo que solo los eventos más relevantes sean sometidos a un análisis exhaustivo. Este proceso comienza con la identificación de candidatos a eventos significativos, sobre los cuales se aplican técnicas avanzadas como el filtrado predictivo, la umbralización adaptativa y la detección 2D basada en *clustering* [52], [54].

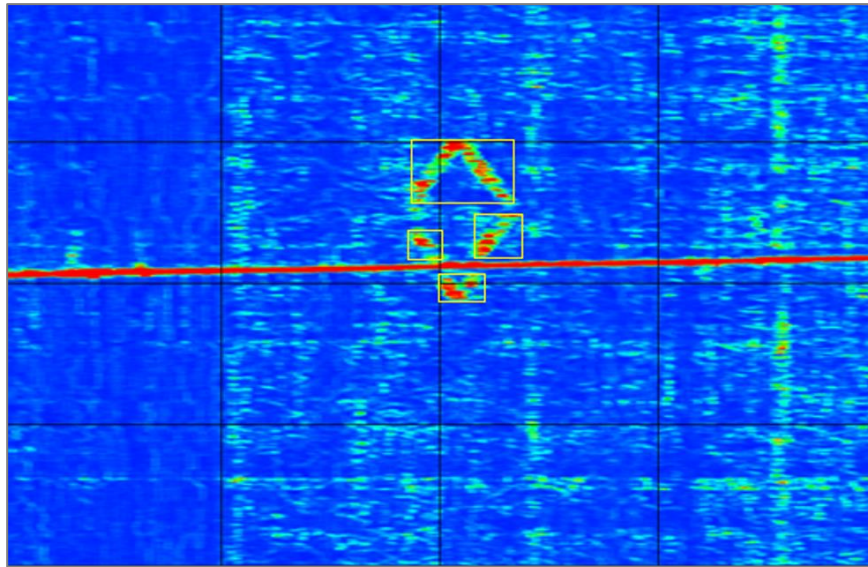


Figura 3-30. Ejemplo de análisis de eventos en una solución DAS [52].

El filtrado predictivo es una de las herramientas clave utilizadas en este contexto. Esta técnica emplea modelos matemáticos y análisis estadísticos para predecir el comportamiento esperado de las señales acústicas, lo que permite diferenciar entre ruido y señales relevantes. Al comparar la señal detectada con un patrón predefinido, el filtrado predictivo ayuda a eliminar ruido ambiental, como el causado por corrientes marinas o actividad aleatoria, y a resaltar eventos significativos que podrían ser indicativos de una anomalía o amenaza potencial. Por ejemplo, si se espera un patrón específico de vibración en una estructura monitoreada, el sistema puede identificar desviaciones de ese patrón que podrían sugerir actividad anómala [17], [18], [52], [54]. Al reducir las interferencias y enfocar el análisis en los eventos más relevantes, esta técnica mejora considerablemente la calidad de los datos procesados y facilita la detección temprana de situaciones críticas.

Además del filtrado predictivo, la aplicación de umbrales adaptativos es otra técnica fundamental en el análisis de datos DAS. Esta metodología permite ajustar dinámicamente los umbrales de detección en función de las condiciones ambientales y del contexto operativo. A diferencia de los umbrales estáticos, que pueden generar falsas alarmas o pasar por alto eventos significativos, los umbrales adaptativos establecen niveles de referencia que se adaptan a las variaciones en tiempo real de los datos acústicos. Por ejemplo, en un entorno con fluctuaciones naturales significativas, como el movimiento constante del agua en cables submarinos, este enfoque permite que solo aquellos eventos que superen un umbral ajustado sean considerados como candidatos relevantes. Esto no solo reduce la cantidad de datos irrelevantes que deben ser procesados, sino que también minimiza el riesgo de generar falsas alarmas, optimizando así la eficiencia del sistema [52], [54].

La detección 2D, basada en algoritmos de *clustering*, complementa estas técnicas al agrupar eventos similares en función de sus características acústicas, como frecuencia, amplitud o duración. Este enfoque utiliza algoritmos de agrupamiento como *k-means* o DBSCAN para organizar los datos en patrones o clústeres, lo que permite identificar comportamientos recurrentes o eventos relacionados que podrían no ser evidentes en un análisis lineal. Por ejemplo, si múltiples vibraciones de baja amplitud ocurren en una misma zona geográfica y en intervalos de tiempo cercanos, la detección 2D puede agrupar estos eventos

como un clúster, sugiriendo una posible actividad coordinada o recurrente. Esta capacidad para identificar patrones en los datos mejora la comprensión de los eventos detectados y proporciona una base sólida para la toma de decisiones informadas [52], [54].

En conjunto, estas técnicas permiten a los sistemas DAS manejar de manera eficiente los enormes volúmenes de datos que generan, enfocándose en eventos significativos mientras se eliminan datos redundantes o irrelevantes. El filtrado predictivo, los umbrales adaptativos y la detección 2D no sólo optimizan la capacidad del sistema para identificar amenazas potenciales, sino que también mejoran la precisión y la confiabilidad del análisis, convirtiendo al DAS en una herramienta esencial para la monitorización y protección de infraestructuras críticas en tiempo real.

3.7.4.4 Clasificación de eventos

La clasificación de eventos en una solución DAS es el proceso mediante el cual los datos recogidos por el sistema, en forma de señales acústicas o vibraciones a lo largo de un cable de fibra óptica, son interpretados y categorizados en función de su origen, naturaleza y características. Este proceso es fundamental para el correcto funcionamiento de los sistemas DAS, ya que estos generan enormes cantidades de datos en tiempo real, que deben ser analizados y procesados para distinguir entre eventos relevantes y ruido de fondo. Los eventos pueden incluir actividades humanas (como excavaciones, corte de cables, manipulación no autorizada o intrusiones), fenómenos naturales (como terremotos, deslizamientos de tierra o corrientes marinas) y otros ruidos ambientales (como el tráfico de embarcaciones o animales marinos). Se utilizan algoritmos de clasificación para detectar y localizar eventos tales como fugas, fallas de cables, actividades de intrusión u otros sonidos anormales [58].

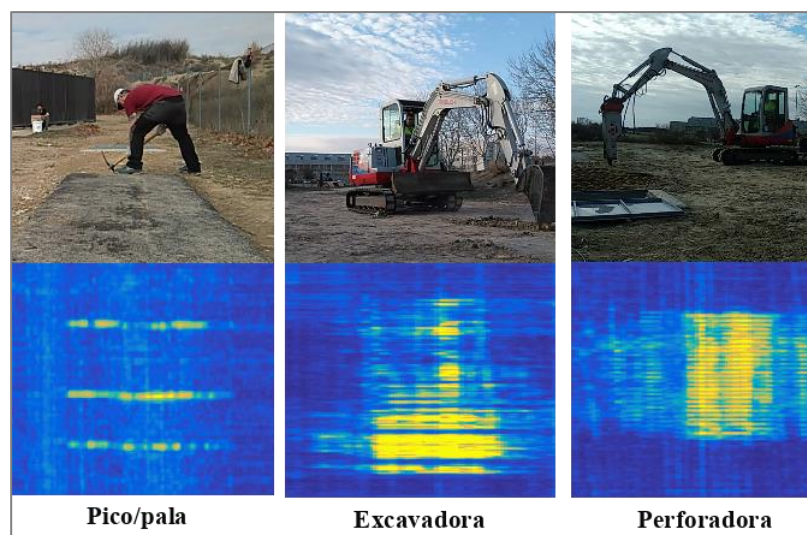


Figura 3-31. Ejemplos de diferentes señales ante diferentes tipos de eventos (imagen adaptada de [17]).

La intensidad de la señal reflejada o transmitida puede variar según la magnitud del estímulo. Por ejemplo, un sonido más fuerte generará una mayor variación en la señal. La respuesta espectral de la fibra puede cambiar según la frecuencia del estímulo. Esto permite identificar diferentes tipos de eventos, como vibraciones o sonidos, dependiendo de su frecuencia. El DAS permite medir fenómenos a lo largo de toda la longitud de la fibra, lo que facilita la localización precisa de los estímulos [17], [52]. Dependiendo de cómo se generan las

vibraciones (por ejemplo, golpes, vibraciones de maquinaria, etc.), la manera en que se propagan a través de la fibra puede variar, afectando las características de la señal.

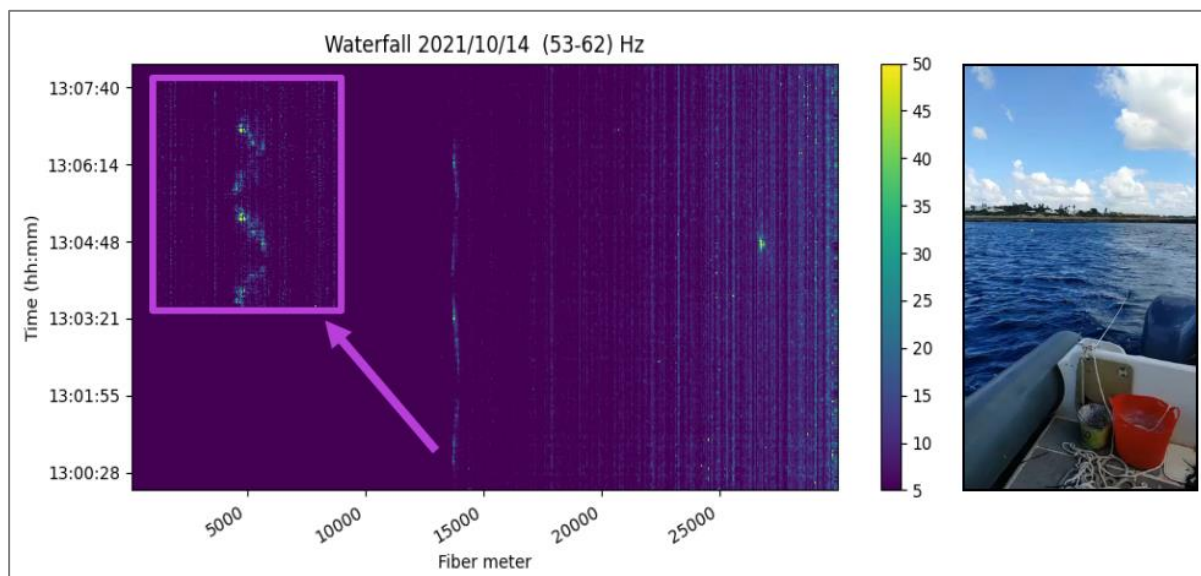


Figura 3-32. Arrastre de cadena sobre un cable submarino [54].

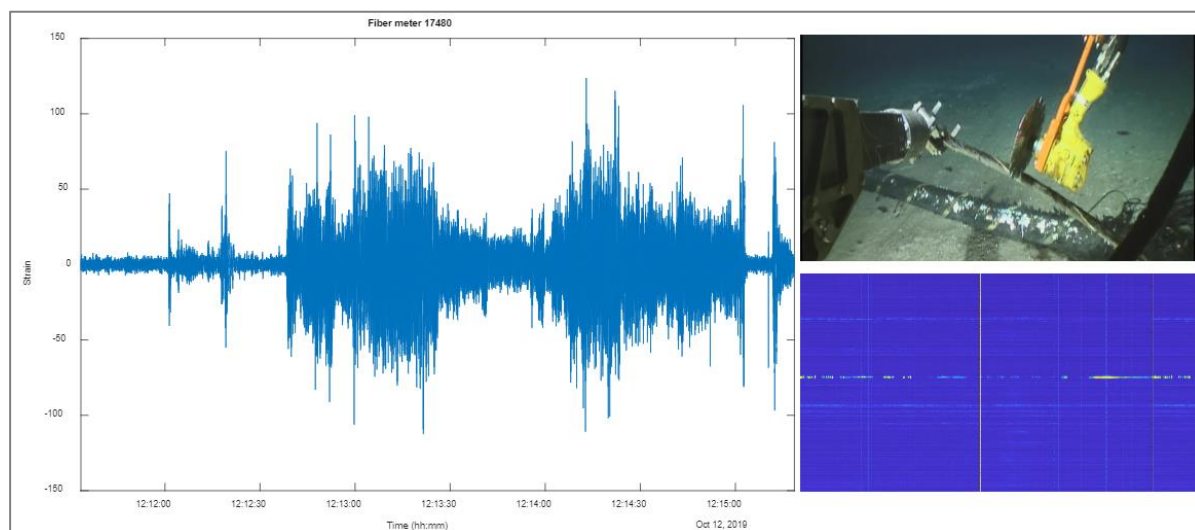


Figura 3-33. Señal producida por el corte de una radial [54].

En la Figura 3-34 se muestra otro ejemplo de detección de un barco a través del sistema DAS del cable de Uninett que se encuentra entre Svalbard y Noruega [5]. En la figura marcada con la letra “A” se muestra con una línea negra el cable submarino, con línea roja la derrota seguida por el buque según los datos de posicionamiento del equipo AIS y con puntos blancos las localizaciones de las señales acústicas recogidas por el sistema DAS producidas por el ruido del barco.

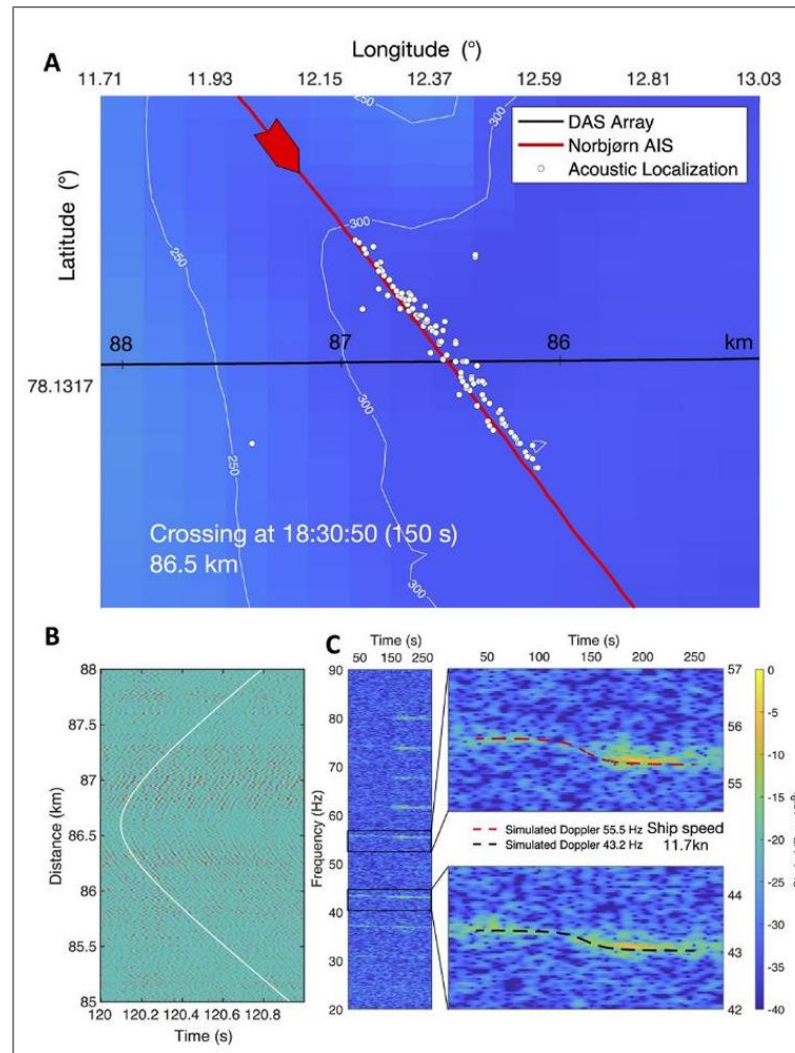


Figura 3-34. Detección de un barco mediante el sistema DAS [5].

A continuación se presenta una toma de datos real, efectuada en julio de 2024, durante el desarrollo de las prácticas del autor del presente trabajo en Red Eléctrica de España. La toma de datos se hizo por parte de la empresa Aragón Photonics sobre un cable submarino de energía eléctrica y de telecomunicaciones propiedad de Red Eléctrica. La toma consistió en adquirir datos de la fibra óptica en el momento del cruce de un barco por encima del cable submarino. En la Figura 3-35 se puede observar la hora y la distancia del cable donde ocurre el evento del cruce del barco.



Figura 3-35. Captura de datos del equipo DAS en el momento del cruce del barco por encima del cable submarino de Red Eléctrica de España [54].

3.7.4.5 Gestión de datos

Los datos procesados se almacenan en bases de datos, que pueden ser locales o en la nube. Esto permite un acceso fácil y rápido para su análisis posterior. Se utilizan herramientas de análisis de datos y visualización para interpretar los resultados. Esto puede incluir gráficos, mapas de calor o modelos tridimensionales, dependiendo de la aplicación. En aplicaciones críticas, el sistema puede configurarse para enviar alertas automáticas cuando se detectan eventos inusuales o peligrosos.

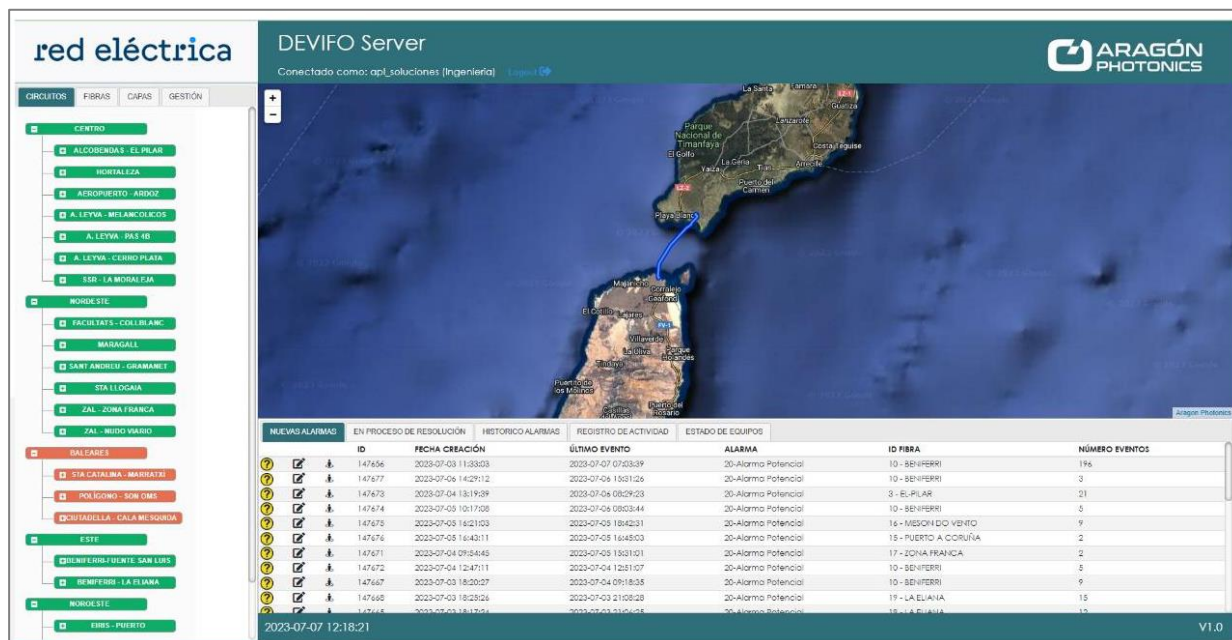


Figura 3-36. Ejemplo de un sistema de gestión de incidencias de un enlace de cable submarino [19].

4 RESULTADOS

4.1 Evaluación y análisis del sistema DAS

Una vez analizados los sistemas DAS en cómo se emplean en la monitorización de cables submarinos para detectar posibles acciones de sabotajes, se presentan los siguientes resultados:

4.1.1 Limitaciones de la tecnología DAS

La tecnología DAS en fibra óptica tiene una serie de limitaciones a pesar de su gran utilidad en la detección y monitorización de vibraciones y eventos acústicos a lo largo de largas distancias.

- Alcance limitado: Aunque la fibra óptica puede cubrir grandes distancias, el sistema DAS tiene un alcance práctico limitado debido a la pérdida de señal y la atenuación en el proceso de medición. La longitud típica en la que el DAS es efectivo suele estar entre 10 y 50 km sin amplificación, y el rango puede variar dependiendo de la sensibilidad y el equipo utilizado [16].
- Resolución espacial: La resolución espacial está determinada por la longitud de los segmentos de fibra que se pueden monitorear de manera efectiva. Normalmente, la resolución es de varios metros (0.8-10 m), lo que significa que no se pueden detectar eventos que ocurren en distancias más pequeñas. Esto puede limitar su efectividad en aplicaciones que requieren alta precisión espacial [17].
- Sensibilidad: La sensibilidad para detectar vibraciones o sonidos específicos puede ser menor en comparación con otros sensores acústicos dedicados. Esto se debe a que las señales acústicas o de vibración pueden debilitarse a medida que viajan a través de la fibra, y solo ciertos rangos de frecuencia se detectan bien [17].
- Ruido y falsas alarmas: Los sistemas son propensos a captar ruido ambiental o eventos no deseados, lo que puede generar falsas alarmas. Esto es un problema particular en entornos ruidosos o en lugares donde múltiples fuentes de vibración están presentes [18].
- Procesamiento y análisis de datos: Generan grandes cantidades de datos en tiempo real, y su procesamiento requiere una gran capacidad computacional y sistemas de análisis

avanzados. Esto puede implicar mayores costos de infraestructura y procesamiento, además de desafíos para la interpretación precisa de las señales [18].

- Limitaciones en tipos de aplicaciones: Aunque DAS es excelente para ciertas aplicaciones (detección de fugas, seguridad perimetral, y sismología), no es adecuado para aplicaciones que requieren mediciones de alta precisión en un amplio rango de frecuencias, como ciertos estudios geofísicos avanzados o mediciones de alta fidelidad en investigación científica [19].
- Costes de implementación: Aunque aprovecha las fibras ópticas existentes, los equipos DAS especializados pueden ser costosos. Además, la calibración y el mantenimiento de estos sistemas pueden implicar costes adicionales [18].
- Dependencia de la calidad de la fibra: La efectividad de un sistema depende en gran medida de la calidad de la fibra óptica y su instalación. Fibras antiguas, con empalmes defectuosos o problemas de atenuación, pueden afectar significativamente al rendimiento del sistema [16].

4.1.2 Soluciones para aumentar la limitación de distancia de la tecnología DAS

El estudio realizado en [59], presenta un diseño optimizado para ampliar la distancia de detección en un sistema DAS, logrando un alcance de hasta 300 km mediante el uso de módulos de amplificación bidireccional con fibra dopada de erbio (EDFA por sus siglas en inglés). La estrategia principal es la implementación de EDFA que amplifican tanto la señal de sonda como la luz de retrodispersión a intervalos definidos a lo largo de la fibra. Esto permite compensar la pérdida de señal causada por la atenuación de la fibra en largas distancias. Al ajustar cuidadosamente la ganancia de los EDFA en cada relé, se maximiza la señal sin introducir ruido adicional significativo.

Se emplean múltiples tramos de fibra, cada uno con una longitud de aproximadamente 50 km, para asegurar la calidad de la señal y reducir el ruido total. Este enfoque permite que la señal de DAS se transmita eficazmente a través de largas distancias sin degradarse. En este diseño, seis tramos de 50 km cada uno logran una distancia de 300 km.

Para minimizar el ruido, el sistema utiliza moduladores acústico-ópticos en cascada (AOM) que logran una alta relación de extinción (ER), reduciendo el ruido de fuga de luz que puede interferir con la señal de retrodispersión. Esta configuración permite mantener una señal clara incluso a largas distancias, asegurando una buena relación señal-ruido (SNR).

Para evitar efectos no deseados como la dispersión estimulada de Brillouin (SBS) y la inestabilidad de modulación (MI), que pueden reducir la potencia de la señal y añadir ruido, se mantiene la potencia de la sonda dentro de límites específicos y se aplica compensación de dispersión en cada tramo.

Este diseño permitió lograr una distancia de detección de 300 km con una resolución espacial de 20 metros, lo que representa un avance significativo en la tecnología DAS para aplicaciones de monitorización de infraestructura a larga distancia.

4.2 Validación de la hipótesis

La hipótesis parte de un reconocimiento claro de que los cables submarinos son infraestructuras críticas de suma importancia. Representan el 95 % del tráfico global de datos y son esenciales para la conectividad, la economía digital, las operaciones gubernamentales y la seguridad nacional. Esto se confirma mediante casos recientes de posibles sabotajes, que evidencian que actores maliciosos tienen tanto la capacidad técnica como la intención de dañar estas infraestructuras.

La tecnología DAS se analiza como una herramienta clave debido a su capacidad de transformar cables de fibra óptica en sensores distribuidos que monitorizan eventos en tiempo real. A partir de los resultados del análisis del sistema, se destacan las capacidades técnicas para detectar vibraciones y cambios físicos asociados a amenazas humanas intencionadas, como intentos de corte o interferencia. Esto es posible gracias al uso de técnicas de retrodifusión Rayleigh, que permite una sensibilidad extraordinaria a lo largo de toda la fibra. A diferencia de tecnologías tradicionales, DAS permite monitorizar longitudes extensas de cables, con capacidad de localización de eventos con una alta precisión. Además, permite supervisión continua incluso en condiciones hostiles, proporcionando información en tiempo real que puede ser utilizada para implementar respuestas proactivas y minimizar el daño.

La hipótesis también plantea que la implementación de estos sistemas fortalece la resiliencia frente a sabotajes. Los datos y análisis del trabajo demuestran que la detección en tiempo real permite una intervención temprana ante actividades sospechosas, reduciendo significativamente la probabilidad de daño crítico. El DAS, al integrarse con sistemas de análisis predictivo, permite asignar recursos de vigilancia y respuesta de manera más eficiente, optimizando la gestión de costes operativos.

Por el contrario, aunque esta tecnología representa un avance significativo, su implementación enfrenta desafíos. Actualmente, la tecnología DAS tiene un alcance limitado, lo que puede dejar segmentos de cables sin supervisión. Además, la adopción de esta tecnología requiere inversiones significativas en infraestructura y capacitación y la implementación a gran escala puede requerir soluciones de interoperabilidad y la estandarización de protocolos de datos.

La validación de la hipótesis demuestra que este sistema es una solución innovadora y eficaz para abordar la amenaza que representan los sabotajes a los cables submarinos. Además, el análisis realizado confirma que el DAS fortalece la resiliencia de estas infraestructuras críticas al reducir significativamente los tiempos de respuesta ante incidentes, optimizando recursos y proporcionando una solución más adaptable y eficiente que las medidas tradicionales.

Sin embargo, esta validación es parcial, ya que presenta limitaciones que deben ser consideradas. Una de las principales restricciones radica en su alcance operativo, que actualmente no cubre toda la longitud de los cables submarinos. Esto deja segmentos significativos sin monitorización activa, creando vulnerabilidades potenciales que pueden ser explotadas por actores maliciosos. Además, el uso exclusivo de DAS no garantiza una protección integral, especialmente en escenarios complejos donde las amenazas pueden combinar sabotajes físicos con ciberataques u otras formas de interferencia.

4.3 Medidas para mejorar la seguridad de los cables submarinos

Una de las medidas más efectivas para mejorar la seguridad de los cables submarinos es la implementación de sistemas DAS en tramos estratégicos de estas infraestructuras. La selección de las

zonas estratégicas debe basarse en un análisis exhaustivo que evalúe la vulnerabilidad y criticidad de cada tramo de cable. Por ejemplo, cables que conectan países con alta dependencia de datos internacionales deben priorizarse para la instalación de estos sistemas. Complementariamente, los datos recogidos por el sistema DAS deben integrarse con sistemas de análisis predictivo e inteligencia artificial para identificar patrones que puedan predecir y prevenir futuros incidentes. Sin embargo, es importante reconocer que el alcance de esta tecnología está limitada a una longitud específica, por lo que su implementación debe ser parte de una estrategia más amplia que incluya tecnologías complementarias.

La naturaleza global de las redes de cables submarinos hace que su protección sea una responsabilidad compartida entre países [21]. Una recomendación fundamental es fomentar la cooperación internacional a través de organismos multilaterales como la OTAN y la Unión Europea. Estas organizaciones pueden desempeñar un papel crucial en la creación de marcos legales y operativos que permitan la monitorización conjunta y una respuesta coordinada ante incidentes que afecten a infraestructuras en aguas internacionales.

La cooperación debe centrarse en la estandarización de protocolos de seguridad y en el intercambio de información en tiempo real sobre amenazas potenciales. Por ejemplo, la creación de una base de datos global que registre incidentes de daño a cables submarinos, ya sea accidental o intencionado, facilitará la identificación de patrones y actores recurrentes. Además, las operaciones conjuntas, como patrullas marítimas internacionales y el uso compartido de tecnologías avanzadas de monitorización, permitirán una vigilancia más eficaz en tramos de cables vulnerables.

Otra dimensión importante de la cooperación internacional es el desarrollo de capacidades colectivas para la recuperación rápida de cables dañados. Esto incluye la creación de equipos especializados multinacionales que puedan movilizarse rápidamente para reparar cables en caso de incidentes graves, minimizando así las interrupciones en los servicios esenciales. Este enfoque colaborativo no solo fortalece la seguridad de los cables submarinos, sino que también fomenta la confianza y la estabilidad entre naciones en un contexto de creciente competencia geopolítica.

La monitorización continua y efectiva de los cables submarinos requiere el desarrollo y despliegue de UUV equipados con sensores avanzados [50]. Estos dispositivos son capaces de operar de forma independiente, realizando inspecciones regulares a lo largo de los cables y detectando anomalías que podrían indicar un intento de sabotaje o daño accidental. Representan una solución rentable y flexible, ya que pueden programarse para cubrir grandes áreas submarinas sin la necesidad de intervención humana constante.

La inversión en UUV debe incluir la integración de estos dispositivos con sistemas como DAS, creando un ecosistema de monitorización que combine vigilancia activa y detección en tiempo real [60]. Por ejemplo, pueden complementar al DAS al proporcionar una visión directa de las áreas donde el sistema detecta anomalías, confirmando la naturaleza de la amenaza y ayudando a los operadores a tomar decisiones informadas. Asimismo, los avances tecnológicos en inteligencia artificial y aprendizaje automático permitirán a los UUV identificar patrones sospechosos de manera autónoma, aumentando su eficiencia y reduciendo la necesidad de supervisión directa.

Además de estos aparatos, se recomienda explorar el desarrollo de vehículos submarinos híbridos que combinen funciones de monitorización y reparación. Estos dispositivos podrían ser desplegados rápidamente para solucionar problemas menores en los cables, mitigando posibles interrupciones antes de que se conviertan en incidentes mayores. La implementación de estos vehículos no solo mejorará la

capacidad de vigilancia, sino que también incrementará significativamente la resiliencia de las infraestructuras críticas submarinas.

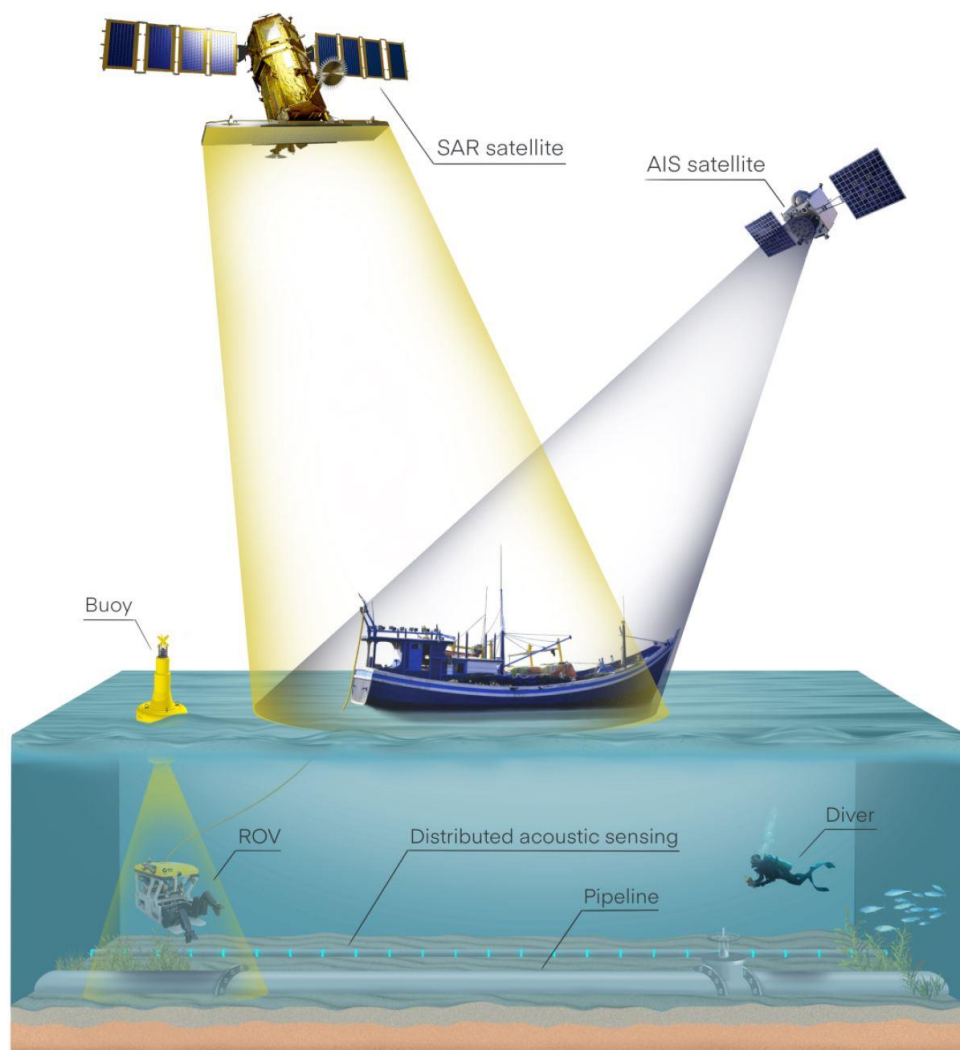


Figura 4-1. Ilustración conceptual de un sistema de vigilancia de Infraestructuras Críticas Submarinas que combina la tecnología DAS, boyas, imágenes y datos satelitales para prevenir actos de sabotaje [60].

La protección de los cables submarinos requiere un marco legal internacional actualizado que refleje las amenazas contemporáneas y establezca sanciones efectivas para disuadir actos de sabotaje o interferencia no autorizada [21]. Los tratados y acuerdos internacionales existentes, son insuficientes para abordar las complejidades actuales, especialmente en un contexto de tensiones geopolíticas crecientes y avances tecnológicos que facilitan el sabotaje.

Se recomienda que los Estados miembros de organismos internacionales trabajen en la actualización de estos tratados para incluir disposiciones claras sobre monitorización, atribución de responsabilidades y sanciones severas. Por ejemplo, los nuevos marcos legales deben especificar las obligaciones de los estados para proteger cables dentro de sus zonas económicas exclusivas, así como sus derechos y responsabilidades en aguas internacionales. Además, se deben establecer procedimientos claros para la cooperación internacional en la investigación de incidentes y en la persecución de actores responsables, ya sean estatales o no estatales.

A nivel nacional, los gobiernos deben desarrollar políticas específicas que incentiven la inversión en tecnologías de protección y establezcan medidas de seguridad obligatorias para las empresas que operan cables submarinos [24]. Estas políticas pueden incluir la implementación obligatoria de sistemas avanzados como DAS y la colaboración con agencias de seguridad para garantizar una protección integral. La actualización legislativa también debe abordar las amenazas cibernéticas, asegurando que los sistemas de comunicación asociados a los cables submarinos estén protegidos contra ataques que puedan comprometer su integridad.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

El trabajo realizado evidencia la importancia crítica de los cables submarinos como la columna vertebral de la conectividad global. Estos cables no solo permiten la transmisión de datos a nivel mundial, sino que también soportan transacciones financieras, comercio internacional, comunicaciones estratégicas y operaciones gubernamentales esenciales. Representan, en esencia, el sustento tecnológico de la economía global y la seguridad nacional en un mundo interdependiente y digitalizado.

En este contexto, los cables submarinos están expuestos a múltiples amenazas, que van desde el garreo de anclas o el arrastre de redes hasta actos de sabotaje deliberados como ha quedado demostrado con los casos analizados. Estas amenazas se ven exacerbadas por las crecientes tensiones geopolíticas y la competencia por el control de infraestructuras críticas. Además, la dependencia tecnológica actual amplifica las consecuencias de cualquier interrupción, destacando la necesidad urgente de soluciones efectivas para garantizar la protección y resiliencia de estas infraestructuras.

La implementación de la tecnología DAS surge como una solución prometedora para enfrentar estos desafíos. Este enfoque transforma las fibras ópticas existentes en sensores distribuidos capaces de detectar y localizar en tiempo real eventos anómalos asociados a posibles intentos de sabotaje o daños accidentales. La capacidad de monitoreo continuo y la detección temprana que ofrece DAS resultan especialmente relevantes en un entorno donde las amenazas físicas y cibernéticas evolucionan con rapidez.

No obstante, el análisis realizado también revela limitaciones significativas en la aplicación actual de esta tecnología. Entre los principales desafíos identificados se encuentra el alcance limitado de los sistemas sin amplificación adicional, lo que restringe su efectividad en cables de gran longitud. Además, el manejo de los grandes volúmenes de datos generados plantea retos técnicos y económicos considerables, incluyendo la necesidad de infraestructuras avanzadas para su procesamiento y almacenamiento. La sensibilidad del sistema a ruidos ambientales puede provocar falsas alarmas, complicando la interpretación de los eventos detectados y aumentando los costos operativos. Por último, la implementación inicial de esta tecnología requiere inversiones significativas, lo que podría limitar su adopción a gran escala en el corto plazo.

Estas limitaciones destacan que, aunque DAS representa un transformador avanzado, no puede considerarse una solución aislada para la seguridad de los cables submarinos. Es imperativo integrarlo dentro de un ecosistema más amplio de medidas de protección que incluya tecnologías complementarias, estrategias de cooperación internacional y marcos normativos sólidos. La tecnología DAS debe combinarse con herramientas como UUV, sistemas de monitoreo satelital y análisis predictivo basado en inteligencia artificial. Estas tecnologías pueden potenciar las capacidades de DAS, proporcionando datos adicionales y mejorando la precisión en la detección y respuesta ante incidentes.

La naturaleza transnacional de las redes de cables submarinos subraya la necesidad de colaboración internacional para garantizar su protección. Estos cables cruzan múltiples jurisdicciones y su seguridad no puede depender únicamente de los esfuerzos individuales de los Estados. Se recomienda fomentar acuerdos multilaterales que permitan el intercambio de información en tiempo real, el desarrollo de estándares comunes y la implementación de estrategias conjuntas para responder a incidentes. Organismos internacionales como la Unión Europea o la OTAN pueden desempeñar un papel clave en la coordinación de estos esfuerzos, facilitando la creación de marcos legales y operativos que promuevan la seguridad compartida.

Asimismo, es crucial actualizar los marcos legales internacionales para reflejar las amenazas contemporáneas a los cables submarinos. Estas actualizaciones deben incluir sanciones efectivas contra actos de sabotaje, así como protocolos claros para la cooperación internacional en la investigación y respuesta a incidentes. La creación de capacidades colectivas, como equipos multinacionales especializados en reparación rápida de cables dañados, también contribuiría a fortalecer la resiliencia de estas infraestructuras críticas.

En síntesis, el trabajo confirma que la tecnología DAS tiene un potencial significativo para transformar la seguridad de los cables submarinos. Su capacidad de detección en tiempo real es crucial para mitigar las amenazas modernas y garantizar la continuidad de los servicios esenciales que dependen de estas infraestructuras. Sin embargo, su máxima efectividad solo puede lograrse dentro de un enfoque integrado que combina tecnología avanzada, cooperación internacional y políticas robustas de protección. Este enfoque integral no solo fortalecerá la resiliencia de los cables submarinos, sino que también contribuirá a garantizar la estabilidad económica y la seguridad global en un mundo cada vez más interconectado. La implementación de DAS, junto con medidas complementarias, marca un paso decisivo hacia un futuro más seguro para la infraestructura de telecomunicaciones global.

5.2 Líneas futuras

En cuanto a las líneas futuras, se plantea la necesidad de superar las limitaciones actuales de DAS mediante la investigación y el desarrollo de soluciones innovadoras, especialmente en superar las limitaciones en el alcance de detección, para poder llegar a cubrir todas las zonas de cables donde la tecnología actual no es capaz de alcanzar.

El uso de algoritmos avanzados de inteligencia artificial IA y análisis de Big Data será esencial para clasificar y diferenciar con precisión los eventos detectados por los sistemas de monitorización. Por ejemplo, el análisis predictivo, combinado con el aprendizaje automático, puede anticipar incidentes antes de que ocurran, mejorando la asignación de recursos y la respuesta proactiva a las amenazas.

Los UUV están llamados a desempeñar un papel crucial en la monitorización directa de las áreas afectadas. Equipados con sensores avanzados y capacidades de análisis autónomo, estos dispositivos no solo complementarán a los sistemas DAS, sino que también podrán realizar reparaciones menores en cables dañados. Los avances en tecnología híbrida permitirán la creación de vehículos que combinen monitoreo y capacidad de intervención, incrementando significativamente la resiliencia de estas infraestructuras críticas.

En el futuro, el despliegue de constelaciones de satélites más sofisticadas, equipadas con inteligencia artificial a bordo, permitirá una monitorización autónoma y en tiempo real. Estas constelaciones podrán detectar y alertar automáticamente sobre actividades sospechosas, facilitando respuestas más rápidas y efectivas a las amenazas.

La naturaleza transnacional de los cables submarinos requiere la actualización de los marcos legales internacionales para abordar amenazas modernas. Los nuevos tratados deben incluir sanciones efectivas para actos de sabotaje y protocolos claros para la cooperación internacional en la investigación de incidentes. Además, se propone la creación de equipos multinacionales especializados en la reparación rápida de cables dañados, promoviendo la resiliencia compartida y la seguridad global.

6 BIBLIOGRAFÍA

- [1] D. Runde, E. Murphy y T. Bryja, «Safeguarding Subsea Cables. Protecting Cyber Infrastructure amid Great Power Competition,» 16 agosto 2024. [En línea]. Disponible en: <https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>. [Último acceso: 11 enero 2025].
- [2] Trama Internacional, «La importancia geoestratégica de los cables submarinos,» 21 mayo 2024. [En línea]. Disponible en: <https://tramainternacional.com/la-importancia-geoestrategica-de-los-cables-submarinos>. [Último acceso: 19 enero 2025].
- [3] F. Gamboa, «Vulnerabilidad de las infraestructuras críticas submarinas. Capacidades y cometidos derivados de la necesidad de su protección,» *Revista General de Marina*, n° 284, pp. 453-461, abril 2023.
- [4] W. Huang, K. Wang, P. Liu, W. Xing y W. Gan, «Experimental Study on Optoelectronic Submarine Cable Used for Ship Radiation Noise Detection,» *IEEE Access*, 2024. [En línea]. Disponible en: <https://ieeexplore.ieee.org/document/10806696>. [Último acceso: 30 diciembre 2024].
- [5] M. Clare, «Submarine Cable Protection and the Environment,» International Cable Protection Committee (ICPC), abril 2024. [En línea]. Disponible en: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_April_2024.pdf. [Último acceso: 19 enero 2025].
- [6] Comisión Europea, «Los cables submarinos de telecomunicaciones son esenciales para la conectividad digital de Europa,» 15 noviembre 2024. [En línea]. Disponible en: <https://digital-strategy.ec.europa.eu/es/library/subsea-telecommunication-cables-are-essential-europes-digital-connectivity>. [Último acceso: 19 enero 2025].
- [7] L. V. Pérez Gil, «Operaciones submarinas rusas encubiertas: las capacidades de la 29ª División de submarinos de la Flota del Norte,» *Revista General de Marina*, n° octubre, pp. 575-597, 2024.
- [8] A. Lott, «The Baltic Sea Cable-Cuts and Ship Interdiction: The C-Lion1 Incident,» Lieber Institute, 26 noviembre 2024. [En línea]. Disponible en: <https://lieber.westpoint.edu/baltic-sea-cable-cuts-ship-interdiction-c-lion1-incident/>. [Último acceso: 19 enero 2025].
- [9] N. Khorrami, «Subsea sabotage should spark review of critical infrastructure security,» *Binding Hook*, 9 enero 2025. [En línea]. Disponible en: <https://bindinghook.com/articles-binding->

- edge/subsea-sabotage-should-spark-review-of-critical-infrastructure-security/. [Último acceso: 10 enero 2025].
- [10] R. Álvarez Ramos, «Cable submarino; Conexión DWDM entre continentes.,» Universidad Politécnica de Madrid, 22 marzo 2017. [En línea]. Disponible en: https://oa.upm.es/49507/1/PFC_ROBERTO_ALVAREZ_RAMOS.pdf. [Último acceso: 19 enero 2025].
- [11] E. Rodríguez, «Historias de Telefónica: El cable submarino,» Movistar.es, 21 diciembre 2023. [En línea]. Disponible en: <https://www.movistar.es/blog/home/cable-submarino-que-es-historia-componentes/>. [Último acceso: 19 enero 2025].
- [12] A. Conte de los Ríos, «Los Fondos Marinos, un Espacio Complejo y Estratégico,» Revista Española de Defensa, vol 413, pp. 54-56, febrero 2024. [En línea]. Disponible en: <https://www.defensa.gob.es/Galerias/gabinete/red/2024/02/p-54-56-red-413-fondos.pdf>. [Último acceso: 19 enero 2025].
- [13] N. Arjona, «La protección de los cables submarinos de telecomunicaciones: soberanías digitales y seguridad de la red de cable submarina,» Universidad Pablo de Olavide, octubre 2023. [En línea]. Disponible en: <https://www.upo.es/revistas/index.php/ripp/article/view/8753/8297>. [Último acceso: 19 enero 2025].
- [14] H. I. Sutton, «Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables,» Naval News, agosto 2021. [En línea]. Disponible en: <https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/>. [Último acceso: 11 enero 2025].
- [15] H. Wu y J. Lai, «Taiwan suspects Chinese ships cut islands' internet cables,» AP News, 18 abril 2023. [En línea]. Disponible en: <https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70>. [Último acceso: 19 enero 2025].
- [16] M. Farid, H. Mohamad, M. Yusoff, A. Hamzah, M. Aizzuddin, N. Faiqa, P. Thansirichaisree y M. Saiful, «State-of-The-Art Application and Challenges of Optical Fibre Distributed Acoustic Sensing in Civil Engineering,» Optical Fiber Technology, octubre 2024. [En línea]. Disponible en: <https://www.sciencedirect.com/science/article/pii/S1068520024002566>. [Último acceso: 12 enero 2025].
- [17] S. Kwik, J. M. Abad, R. Martínez, J. Preciado, P. Sevillano y J. Subías, «DAS Technology: an opportunity to use fibre optics for asset monitoring and security applications in Electric Power Utilities,» *Cigre Science & Engineering (CSE)*, nº 27, 2023.
- [18] A. Nur y Y. Muanenda, «Design and Evaluation of Real-Time Data Storage and Signal Processing in a Long-Range Distributed Acoustic Sensing (DAS) Using Cloud-Based Services,» MDPI, septiembre 2024. [En línea]. Disponible en: <https://www.mdpi.com/1424-8220/24/18/5948>. [Último acceso: 19 enero 2025].
- [19] Aragón Photonics, «Detección de vibraciones por fibra óptica para cables submarinos,» s.f.. [En línea]. Disponible en: <https://aragonphotonics.com/es/industrias/energia-electrica/>. [Último acceso: 19 enero 2025].
- [20] Aragón Photonics, «HDAS. High-Fidelity Distributed Acoustic Sensor.,» s.f.. [En línea]. Disponible en: <https://aragonphotonics.com/es/productos/hdas/>. [Último acceso: 10 enero 2025].
- [21] Comisión Europea, «Recomendación (UE) 2024/779 de la Comisión sobre unas infraestructuras de cables submarinos seguras y resilientes,» 26 febrero 2024. [En línea]. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L_202400779. [Último acceso: 19 enero 2025].

- [22] Consejo Nacional de Seguridad Marítima, «Estrategia Nacional de Seguridad Marítima 2024,» mayo 2024. [En línea]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2024-10762. [Último acceso: 19 enero 2025].
- [23] MARCOM, «NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure,» mayo 2024. [En línea]. Disponible en: <https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui>. [Último acceso: 19 enero 2025].
- [24] A. Piñeiro, «Safeguarding the underwater – new solutions and technologies for new challenges. XIV Simposio Transregional del Poder Naval,» octubre 2024. [En línea]. Disponible en: <https://www.youtube.com/watch?v=hddoqFgDsn8>. [Último acceso: 18 noviembre 2024].
- [25] TeleGeography, «Mapa de Cables Submarinos,» [En línea]. Disponible en: <https://www.submarinecablemap.com/>. [Último acceso: 19 enero 2025].
- [26] Revista Cloud Computing, «Cómo proteger los cables submarinos de ciberataques,» septiembre 2023. [En línea]. Disponible en: <https://www.revistacloudcomputing.com/2023/09/como-proteger-los-cables-submarinos-de-los-ciberataques/>. [Último acceso: 19 enero 2025].
- [27] Congressional Research Service, «Protection of Undersea Telecommunication Cables,» agosto 2023. [En línea]. Disponible en: <https://crsreports.congress.gov/product/pdf/R/R47648>. [Último acceso: 19 enero 2025].
- [28] A. Lacasa, «La revolución bajo el mar: cómo la fibra óptica submarina ha cambiado nuestra forma de comunicarnos,» BLOGSudima, 14 noviembre 2023. [En línea]. Disponible en: <https://blogs.udima.es/ingenieria-industrial/la-revolucion-bajo-el-mar-como-la-fibra-optica-submarina-ha-cambiado-nuestra-forma-de-comunicarnos/>. [Último acceso: 19 enero 2025].
- [29] Red Eléctrica de España, *Proyectos de enlaces eléctricos submarinos de REE*, Alcobendas, 2024.
- [30] Red Eléctrica de España, «2ª Interconexión eléctrica España-Marruecos. Proyecto REMO,» s.f.. [En línea]. Disponible en: <https://www.ree.es/sites/default/files/downloadable/remo.pdf>. [Último acceso: 10 enero 2025].
- [31] L. Carter y D. R. Burnett, «Subsea Telecommunications,» de *Routledge Handbook of Ocean Resources and Management*, Routledge, 2015, pp. 349-365.
- [32] Unión Internacional de Telecomunicaciones (UIT), «Protección externa adicional para los cables terrenales marinizados,» octubre 2002. [En línea]. Disponible en: https://www.itu.int/rec/dologin_pub.asp?id=T-REC-L.28-200210-I%21%21PDF-S&lang=e&type=items. [Último acceso: 19 enero 2025].
- [33] R. García Pérez, «España en la red global de cables submarinos,» *Instituto Español de Estudios Estratégicos*, nº 32, pp. 1282-1332, 2023.
- [34] Fast Company, «Nearly all data that moves around the world goes through these undersea cables,» 04 febrero 2024. [En línea]. Disponible en: <https://www.fastcompany.com/91072728/internet-undersea-cables-data>. [Último acceso: 19 enero 2025].
- [35] E. Páez, «Cables submarinos: potenciales objetivos en zonas de conflicto,» *dpl news*, 9 diciembre 2024. [En línea]. Disponible en: <https://dplnews.com/cables-submarinos-objetivos-en-zonas-de-conflicto/>. [Último acceso: 19 enero 2025].

- [36] A. Cwalina, «Concerns grow over possible Russian sabotage of undersea cables,» Atlantic Council, 12 septiembre 2024. [En línea]. Disponible en: <https://www.atlanticcouncil.org/blogs/ukrainealert/concerns-grow-over-possible-russian-sabotage-of-undersea-cables/>. [Último acceso: 19 enero 2025].
- [37] Maritime Tales & Cutting Edge Sails, «The Great Underwater War: How Submarine Cable Sabotage Could Trigger a Global Crisis,» 21 noviembre 2024. [En línea]. Disponible en: <https://sailorspeaks.com/2024/11/21/the-great-underwater-war-how-submarine-cable-sabotage-could-trigger-a-global-crisis/>. [Último acceso: 10 enero 2025].
- [38] Gallagher Re, «Hidden Dangers: Undersea Cables and Mitigating Economic Risk,» octubre 2024. [En línea]. Disponible en: <https://dr.ajg.com/gallagherre/news-and-insights/features/2024/october/hidden-dangers-undersea-cables-and-mitigating-economic-risk/>. [Último acceso: 19 enero 2025].
- [39] L. Burdette, «Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy,» Princeton University, 5 mayo 2021. [En línea]. Disponible en: <https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>. [Último acceso: 19 enero 2025].
- [40] W. Lii, «After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience,» The Diplomat, 15 abril 2023. [En línea]. Disponible en: <https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/>. [Último acceso: 19 enero 2025].
- [41] Newsweek, «Map Shows Telecoms Cable Between Two NATO Allies Mysteriously Cut,» 19 noviembre 2024. [En línea]. Disponible en: <https://www.newsweek.com/map-shows-cable-between-finland-germany-news-mysteriously-cut-nato-1987992>. [Último acceso: 19 enero 2025].
- [42] France24.com, «Finnish police probing seven sailors over cut cables,» 1 enero 2025. [En línea]. Disponible en: <https://www.france24.com/en/live-news/20250101-finnish-police-probing-seven-sailors-over-cut-cables>. [Último acceso: 19 enero 2025].
- [43] Police of Finland, «Police investigating incidents in the Gulf of Finland in cooperation with other authorities,» 26 diciembre 2024. [En línea]. Disponible en: <https://poliisi.fi/en/-/police-investigating-incidents-in-the-gulf-of-finland-in-cooperation-with-other-authorities>. [Último acceso: 19 enero 2025].
- [44] Police of Finland, «The police transfer tanker Eagle S to Kilpilahti on Saturday,» 28 diciembre 2024. [En línea]. Disponible en: <https://poliisi.fi/en/-/the-police-transfer-tanker-eagle-s-to-kilpilahti-on-saturday>. [Último acceso: 19 enero 2025].
- [45] T. Nilsen, «Navy's Intelligence Directorate gets four more ice-classed spy ships for seafloor operations,» 25 abril 2023. [En línea]. Disponible en: <https://thebarentsobserver.com/en/security/2023/04/navys-intelligence-directorate-gets-four-more-ice-classed-spy-ships-seafloor>. [Último acceso: 19 enero 2025].
- [46] El Snorkel, «Submarino nuclear supersecreto ruso Losharik regresará pronto al servicio,» marzo 2024. [En línea]. Disponible en: <https://www.elsnorkel.com/2024/03/submarino-nuclear-ruso-supersecreto-Losharik-regresara-servicio.html>. [Último acceso: 19 enero 2025].
- [47] Defensa.com, «Satélites para proteger las Zonas Económicas Exclusivas,» 22 febrero 2021. [En línea]. Disponible en: <https://www.defensa.com/defensa-naval/satelites-para-proteger-zonas-economicas-exclusivas>. [Último acceso: 19 enero 2025].

- [48] SatCen, «Critical Infrastructure,» s.f.. [En línea]. Disponible en: https://www.satcen.europa.eu/page/military_capabilities. [Último acceso: 19 enero 2025].
- [49] European Maritime Safety Agency, «Copernicus Maritime Surveillance Service,» 2024. [En línea]. Disponible en: <https://www.emsa.europa.eu/copernicus.html>. [Último acceso: 19 enero 2025].
- [50] Congressional Research Service, «Navy Large Unmanned Surface and Undersea Vehicles,» agosto 2024. [En línea]. Disponible en: <https://crsreports.congress.gov/product/pdf/R/R45757>. [Último acceso: 19 enero 2025].
- [51] Aragón Photonics, «Monitorización de líneas eléctricas con DFOS,» junio 2024. [En línea]. Disponible en: <https://aragonphotonics.com/es/industrias/energia-electrica/>. [Último acceso: 19 enero 2025].
- [52] Red Eléctrica de España, *Tecnología DAS*, Alcobendas, 2024.
- [53] RBtec Security Systems, «Distributed Acoustic Sensing for Long-Distance Monitoring,» s.f. [En línea]. Disponible en: https://www.rbtec.com/es/perimeter-sensors-and-underground-protection/cable_sensores_enterrados/sensor-acustico-distribuido-en-fibra-optica-das. [Último acceso: 19 enero 2025].
- [54] Aragón Photonics, *Presentación HDAS cables submarinos*, 2024.
- [55] ASN, «OPTODAS. The Leading Technology for Distributed Acoustic Sensing,» s.f.. [En línea]. Disponible en: <https://www.asn.com/fiber-sensing/>. [Último acceso: 10 enero 2025].
- [56] Environmental & Science Engineering, «Products & Services Showcase – 42nd Edition,» s.f.. [En línea]. Disponible en: <https://esemag.com/products-services-showcase-42/>. [Último acceso: 10 enero 2025].
- [57] UPTECH Sensing, «UTS-AS1000. Nueva generación de equipamiento de medida distribuida acústico.,» s.f.. [En línea]. Disponible en: <https://uptech-sensing.com/producto-ampliado-uts-as1000.html>. [Último acceso: 10 enero 2025].
- [58] AP Sensing, «Distributed Acoustic Sensing (DAS) Technology,» s.f.. [En línea]. Disponible en: <https://www.apsensing.com/es/tecnologia/das-dvs>. [Último acceso: 19 enero 2025].
- [59] C. Fan, H. Li, K. Zhang, H. Liu, Y. Sun, B. Yan, Z. Yan, D. Liu y P. Ping, «300 km ultralong fiber optic DAS system based on optimally designed bidirectional EDFA relays,» *Photonics Research*, vol. 11, nº 6, pp. 968-977, 2023.
- [60] G. Soldi, D. Gaglione, S. Raponi, N. Forti, E. d’Afflisio, P. Kowalski, L. M. Millefiori, D. Zissis, P. Braca, P. Willett, A. Maguer, S. Carniel, G. Sembenini y W. C., «Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies,» arXiv, febrero 2023. [En línea]. Disponible en: <https://arxiv.org/abs/2302.01817>. [Último acceso: 19 enero 2025].

ANEXO I: ASIGNATURAS DEL MÁSTER RELACIONADAS CON EL TRABAJO

COM6. Transformación Digital e Innovación.

COM8. Redes y Sistemas de Telecomunicación.

COM9. Sistemas de Información.

COM10. Seguridad de la Información.

COM11. Gestión de la Seguridad y Análisis de Riesgos.

ANEXO II: LISTADO DE ACRÓNIMOS

AIS: Automatic Information System

AOM: Acousto-Optic Modulator

AJEMA: Almirante Jefe de Estado Mayor de la Armada

CAPEX: Capital Expenditure

CP-OTDR: Chirped Pulse Optical Time-Domain Reflectometry

DAS: Distributed Acoustic Sensing

DBSCAN: Density-Based Spatial Clustering of Applications with Noise

DC: Direct Current

EDFA: Erbium-Doped Fiber Amplifier

ER: Extinction Ratio

GUGI: Glavnoye Upravlenie Glubokovodnikh Issledovani

MI: Modulation Index

OPEX: Operating Expenditure

SBS: Stimulated Brillouin Scattering

SNR: Signal-to-Noise Ratio

TIC: Tecnologías de la Información y las Comunicaciones

UUV: Unmanned Underwater Vehicle

WDM: Wavelength Division Multiplexing

ZEE: Zona Económica Exclusiva