INFRAESTRUCTURAS SUBMARINAS CRÍTICAS: EL NUEVO FRENTE EN EL MAR

Cómo la robótica y la vigilancia autónoma están transformando la defensa de los cables y gasoductos submarinos.

Capitán de Corbeta D. Francesco Barone
Submarinista
Marina Militare
Italia

RESUMEN

Este articulo presenta cómo la integración de tecnologías autónomas y sistemas robóticos puede mejorar la protección de las infraestructuras submarinas críticas, como cables y gasoductos. A partir del enfoque teórico de la Escuela de Copenhague, se expone cómo estas infraestructuras se han convertido en objetos de seguridad por su importancia estratégica, energética y digital. Se presentan casos recientes de sabotaje, como el incidente del *Nord Stream* 2, y se identifican los actores que representan amenazas reales. El análisis propone un modelo multidominio de vigilancia basado en sensores, vehículos autónomos y supervisión satelital, evaluando tanto los retos técnicos como los vacíos normativos existentes. Finalmente, se destaca el papel creciente de organizaciones internacionales y estados, como Italia, en la protección del entorno subacuático a través de políticas coordinadas. El articulo ofrece recomendaciones y nuevas líneas de análisis para avanzar en la seguridad y resiliencia de estas infraestructuras esenciales.

Palabras clave:

Securitización, Infraestructura submarina crítica, Tecnologías autónomas, Escuela de Copenhague, Seguridad internacional.

SUMMARY

This study analyzes how the integration of autonomous technologies and robotic systems can enhance the protection of critical underwater infrastructures, such as cables and pipelines. Drawing on the theoretical framework of the Copenhagen School, it explores how these infrastructures have become securitized objects due to their strategic, energy-related, and digital significance. Recent sabotage incidents, such as the *Nord Stream* 2 case, are examined, and state and non-state actors posing real threats are identified. The research proposes a multidomain surveillance model based on sensors, autonomous vehicles, and satellite monitoring, assessing both technical challenges and existing regulatory gaps. Finally, the growing role of international organizations

and states, such as Italy, is highlighted in protecting the underwater environment through coordinated policies. The thesis offers recommendations and new research avenues to advance the security and resilience of these essential infrastructures.

Key Words:
Securitization, Critical Undersea Infrastructure, Autonomous Technologies, Copenhagen School, International Security.

INTRODUCCIÓN

En un mundo interconectado y digitalizado, la estabilidad de nuestras sociedades depende en gran medida de redes invisibles que cruzan los océanos. Cables de comunicaciones, gasoductos y oleoductos submarinos conforman una infraestructura crítica que garantiza el suministro energético, la transmisión de datos y el funcionamiento de la economía global. Sin embargo, estas infraestructuras vitales permanecen fuera de la vista y, a menudo, fuera del radar político, lo que las convierte en objetivos vulnerables ante amenazas híbridas, sabotajes y conflictos geopolíticos.

Los recientes incidentes en el mar Báltico, como el sabotaje del gasoducto *Nord Stream* 2, han puesto de relieve la fragilidad de estas infraestructuras y han generado un cambio en la percepción estratégica de los espacios subacuáticos. La comunidad internacional ha comenzado a reconocer la necesidad de proteger estos activos mediante nuevas capacidades tecnológicas y doctrinas adaptadas al entorno submarino.

En este contexto, el uso de tecnologías autónomas, como vehículos submarinos no tripulados y sistemas de vigilancia inteligentes, se perfila como una herramienta clave para reforzar la seguridad y la resiliencia de las infraestructuras submarinas críticas. Su implementación plantea oportunidades innovadoras, pero también desafíos técnicos, operativos y jurídicos.

Este artículo ofrece una síntesis de un trabajo de investigación más amplio que analiza el papel de estas tecnologías desde una perspectiva multidisciplinar, combinando teoría de las relaciones internacionales —con especial atención a la Escuela de Copenhague y el concepto de *securitización*— con el estudio de casos recientes y propuestas de arquitectura tecnológica. El objetivo es acercar al lector general a un tema de creciente relevancia estratégica: la defensa de lo invisible bajo el mar.

ANTECEDENTES

El estudio de las infraestructuras submarinas críticas (CUI) ha sido durante años un ámbito poco explorado dentro de las ciencias políticas, las relaciones internacionales y los estudios de seguridad. Tradicionalmente, estas infraestructuras —como cables de telecomunicaciones o gasoductos— se trataban desde perspectivas técnicas o económicas, dejando en segundo plano su relevancia estratégica y su vulnerabilidad ante amenazas deliberadas.

Sin embargo, a partir de la última década y especialmente tras el sabotaje del *Nord Stream* 2 en 2022, se ha producido un giro en el interés académico e institucional. Investigadores de todo el mundo han comenzado a abordar estas infraestructuras desde el prisma del derecho internacional y la seguridad marítima, señalando lagunas normativas y operativas que dificultan su protección efectiva. Al mismo tiempo, centros como la OTAN o la Unión Europea han promovido informes y estrategias que evidencian el creciente riesgo de ataques híbridos sobre estos activos.

En el campo teórico, la aplicación de la teoría de la securitización de la Escuela de Copenhague ha permitido reinterpretar estas infraestructuras no solo como bienes materiales, sino como objetos de seguridad en los discursos estratégicos de los estados. Este enfoque facilita comprender cómo se justifica la adopción de medidas extraordinarias —tecnológicas, legales o militares— para protegerlas.

El análisis parte de estos avances, pero aporta una perspectiva novedosa al vincular directamente la securitización con el desarrollo de tecnologías autónomas de vigilancia. Este cruce entre teoría política, innovación tecnológica y casos empíricos recientes constituye una contribución original al estudio de la seguridad internacional en el entorno subacuático.

LA SEGURIDAD COMO CONSTRUCCIÓN: LA ESCUELA DE COPENHAGUE

Antes de adentrarnos en los aspectos técnicos y estratégicos de la defensa de infraestructuras submarinas, es importante entender cómo ha cambiado la manera de pensar la seguridad en el ámbito internacional. La Escuela de Copenhague, una de las corrientes más influyentes en los estudios de seguridad contemporáneos, propone una visión innovadora: la seguridad no es simplemente la respuesta a una amenaza objetiva, sino el resultado de un proceso político y discursivo.

Según esta teoría, desarrollada por autores como Barry Buzan y Ole Wæver, un tema se convierte en un problema de seguridad —es decir, en algo que requiere medidas excepcionales— cuando un actor securitizador (por ejemplo, un gobierno o una institución internacional) declara que existe una amenaza

existencial hacia un objeto referencial (una infraestructura, una población, un territorio). Pero este acto no es automático: debe ser aceptado por una audiencia, que legitima la transformación del asunto en una prioridad de seguridad.

Este enfoque nos permite comprender por qué ciertos temas, como el terrorismo o la migración, reciben tanta atención y recursos, mientras que otros, como la seguridad ambiental o digital, pueden pasar desapercibidos. En el caso de las infraestructuras submarinas, la securitización se ha producido recientemente, en gran parte como reacción a incidentes como el sabotaje del gasoducto *Nord Stream*.

Así, la teoría de la securitización nos ofrece una lente útil para analizar cómo actores estatales e internacionales construyen nuevas amenazas, y cómo estas construcciones justifican políticas, inversiones y tecnologías orientadas a defender aquello que se percibe en riesgo: en este caso, el corazón invisible de la conectividad y la energía global.

¿QUÉ SON LAS INFRAESTRUCTURAS SUBMARINAS CRÍTICAS Y POR QUÉ IMPORTAN?

Una red oculta bajo el mar.

Aunque no las veamos, bajo la superficie de los océanos se extiende una red de infraestructuras vitales para el funcionamiento del mundo moderno. Se trata de los cables de fibra óptica, los gasoductos, los oleoductos y otros conductos que recorren miles de kilómetros a través del fondo marino. Estas infraestructuras conectan continentes, transmiten energía, transportan datos y sostienen actividades esenciales como las finanzas, la comunicación global o la seguridad nacional.

A menudo se describe esta red como “la columna vertebral invisible” de la globalización. Solo en lo que respecta a los cables de comunicaciones, más del 95 % del tráfico de datos internacional circula por estas conexiones físicas, y no por satélite, como muchas personas creen. Los cables submarinos permiten videollamadas, transacciones bancarias, funcionamiento de redes sociales y acceso a servicios en la nube.

En paralelo, oleoductos y gasoductos submarinos transportan hidrocarburos desde los países productores hasta los centros de consumo. En regiones como el mar Báltico o el Mediterráneo, estas infraestructuras son clave para la seguridad energética de Europa, especialmente desde el inicio del conflicto en Ucrania y el esfuerzo por reducir la dependencia del gas ruso.

Pese a su importancia, las infraestructuras submarinas críticas (o CUI, por sus siglas en inglés: *Critical Undersea Infrastructure*) siguen siendo poco conocidas para el público y poco protegidas desde el punto de vista estratégico.

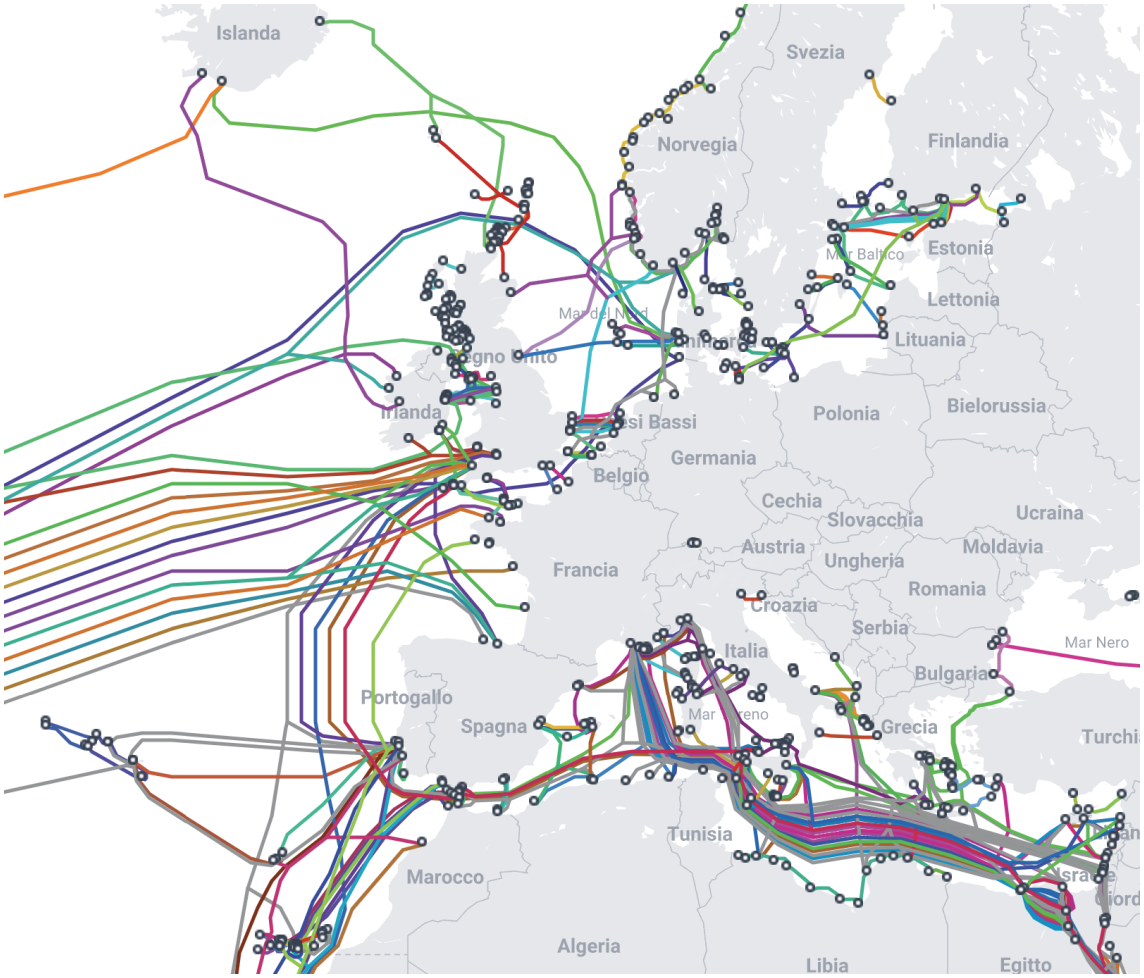

Fig. 1 – Mapa de cables submarinos en la zona euroatlántica (www.submarinecablemap.com, 14 abril 2025)

Funciones esenciales para la sociedad global.

Las CUI cumplen funciones esenciales en diversos ámbitos. Su impacto se extiende mucho más allá del sector energético o tecnológico: afectan directamente al funcionamiento del sistema financiero, la seguridad cibernética, la gestión de crisis, la defensa nacional e incluso la vida cotidiana de millones de personas.

En el caso de los cables de comunicaciones, su interrupción podría provocar desde cortes de internet hasta fallos en las bolsas de valores internacionales. A nivel militar, muchas operaciones dependen también de estas redes para la transmisión de datos clasificados, la navegación y el mando y control de sistemas distribuidos.

Por su parte, los gasoductos y oleoductos submarinos garantizan la llegada de recursos energéticos a los países consumidores. En momentos de tensión política, como ocurrió tras el sabotaje del *Nord Stream*, la interrupción de estos flujos puede desencadenar crisis energéticas con consecuencias económicas y sociales de gran alcance.

Además, se están desarrollando nuevas infraestructuras bajo el mar: sensores de vigilancia, estaciones de carga para drones submarinos, e incluso centros de datos sumergidos, lo que incrementa la importancia estratégica del entorno subacuático.

Una vulnerabilidad estratégica creciente.

El crecimiento de esta red ha traído consigo una creciente exposición a riesgos. Las CUI se encuentran en entornos remotos, de difícil acceso, donde el control efectivo es limitado. La profundidad del mar, las condiciones ambientales, la opacidad jurídica y la falta de vigilancia constante las convierten en objetivos vulnerables ante sabotajes, accidentes o ataques híbridos.

El término “zona gris” se utiliza para describir las acciones deliberadas que se sitúan entre la paz y la guerra, difíciles de atribuir y responder. Este tipo de amenazas se adapta muy bien al medio submarino: un buque puede dañar un cable intencionadamente, un actor estatal puede usar medios civiles para ocultar actividades hostiles, o un ciberataque puede alterar el funcionamiento de una infraestructura sin dejar rastro físico.

La falta de normativas internacionales específicas, unida a la dispersión de responsabilidades entre actores públicos y privados, agrava esta vulnerabilidad. En muchas ocasiones, ni siquiera se puede determinar con claridad quién debe proteger, mantener o vigilar una infraestructura concreta cuando cruza varios espacios marítimos bajo diferentes jurisdicciones.

¿Quién controla el fondo del mar?

Una característica particular del entorno subacuático es la multiplicidad de actores implicados en la instalación y gestión de las CUI. Aunque a menudo se asocia su propiedad con los estados, en realidad la mayoría de los cables y ductos son construidos, operados y mantenidos por empresas privadas o consorcios internacionales. Esto dificulta la coordinación de medidas de protección y complica la respuesta ante incidentes.

Además, el marco jurídico actual, basado principalmente en la Convención de las Naciones Unidas sobre el Derecho del Mar (UNCLOS), ofrece una cobertura parcial. Establece derechos y deberes en zonas marítimas específicas, pero no prevé mecanismos operativos eficaces para prevenir, atribuir o sancionar actos

hostiles contra las CUI, especialmente cuando ocurren fuera de las aguas territoriales.

En este contexto, la seguridad de las infraestructuras submarinas depende de una cooperación internacional eficaz, del desarrollo de nuevas capacidades tecnológicas y de una mayor concienciación política y estratégica sobre su papel central en la seguridad del siglo XXI.

AMENAZAS REALES Y CASOS RECIENTES

Nord Stream 2: el incidente que lo cambió todo

El 26 de septiembre de 2022, el mundo fue testigo de un hecho sin precedentes: tres explosiones submarinas destruyeron parcialmente los gasoductos *Nord Stream* 1 y 2, frente a las costas de la isla danesa de Bornholm. Aunque no estaban operativos en ese momento, ambos conductos estaban presurizados con gas natural. La fuga provocó la liberación de más de 220.000 toneladas de metano, uno de los gases de efecto invernadero más potentes, generando alarma medioambiental y geopolítica.

Este acto fue rápidamente interpretado como un sabotaje deliberado. Aunque las investigaciones de Suecia y Dinamarca han concluido sin identificar responsables, las autoridades de seguridad y los analistas coinciden en que se trató de una operación encubierta, probablemente ejecutada por actores estatales o paraestatales. El caso reveló lo vulnerable que puede ser una infraestructura clave incluso en el corazón de Europa, en tiempos de paz aparente.

Además de sus consecuencias ambientales y energéticas, el incidente tuvo un impacto inmediato en la agenda de seguridad europea. Por primera vez, se habló abiertamente de la necesidad de proteger las CUI como se protege una base militar o una central eléctrica, tanto a nivel nacional como a través de alianzas como la OTAN o la Unión Europea.

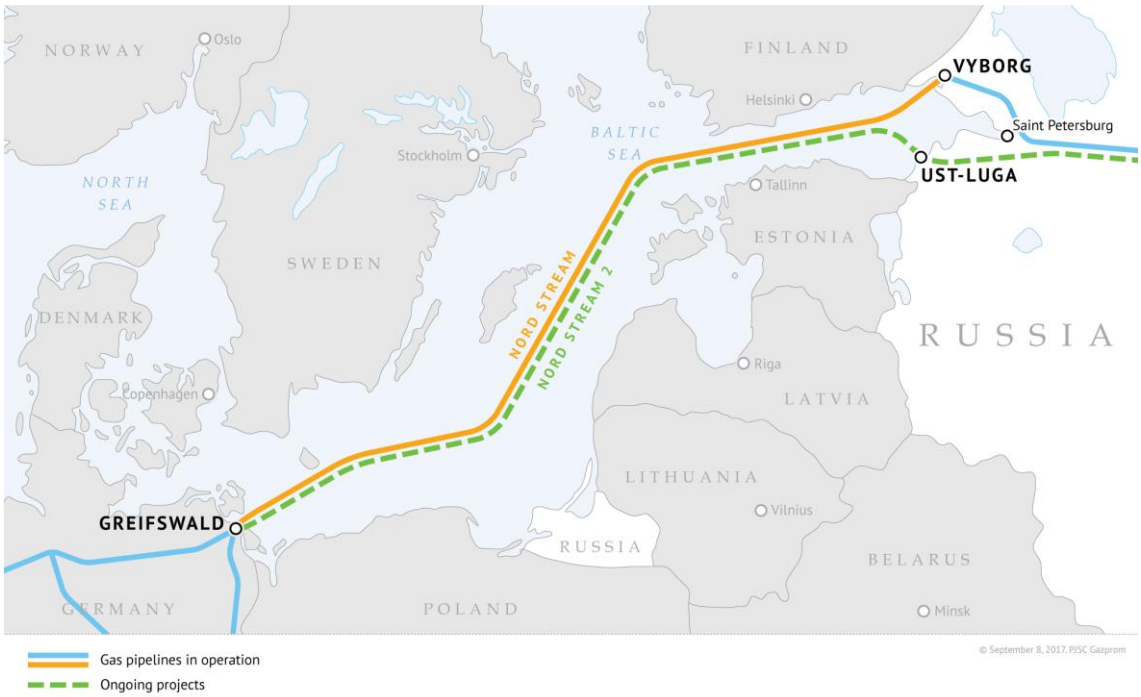

Fig. 2 – Los dos gasoductos *Nord Stream* (Source: *Gazprom*)

Incidentes posteriores: un patrón preocupante.

El ataque al *Nord Stream* no fue un caso aislado. Desde entonces, se ha producido una serie de incidentes que confirman la tendencia hacia una escalada de amenazas híbridas en el entorno subacuático.

En enero de 2022, el corte de un cable de comunicaciones en el archipiélago noruego de Svalbard dejó incomunicado por horas el centro de control satelital más septentrional de Europa. A pesar de las sospechas sobre la posible implicación de buques pesqueros rusos, no se lograron pruebas concluyentes.

En octubre de 2023, el gasoducto *Balticconnector*, que conecta Finlandia y Estonia, sufrió daños importantes junto con varios cables submarinos adyacentes. Las autoridades finlandesas identificaron a un carguero de bandera china, el *Newnew Polar Bear*, como posible causante del daño, aunque se declaró como un “accidente”. Lo más inquietante fue la coincidencia temporal y geográfica de múltiples averías, lo que sugiere una posible operación coordinada.

El año pasado otros incidentes afectaron cables entre Suecia y Lituania, instalaciones cerca de la estación aérea de Evenes en Noruega y cuatro cables submarinos en el mar Rojo, coincidiendo con la escalada de tensiones en la región.

Estos hechos, aunque diferentes en naturaleza y contexto, tienen en común la dificultad para atribuir responsabilidades, el uso de medios civiles para fines

potencialmente hostiles y la ausencia de mecanismos internacionales eficaces para investigar y sancionar estas acciones.

¿Quién está detrás de estas amenazas?

Los principales sospechosos en este tipo de incidentes suelen ser actores estatales con intereses estratégicos en las zonas afectadas. Rusia y China son mencionados con frecuencia por su capacidad técnica, su historial de operaciones encubiertas y sus ambiciones geopolíticas.

Rusia, por ejemplo, ha desarrollado una llamada "flota en la sombra": una red opaca de buques sin identificación clara, que opera en regiones clave como el mar Báltico. Estos barcos, que aparentan actividades comerciales o pesqueras, pueden desplegar drones, sensores o incluso explosivos en proximidad a infraestructuras críticas. Según varios informes occidentales, esta flota está vinculada a los servicios de inteligencia y cumple funciones de vigilancia y sabotaje.

China, por su parte, ha ampliado su presencia en el sector de los cables submarinos de comunicaciones mediante empresas como *Huawei Marine*, generando preocupaciones sobre la posible recolección de datos sensibles y la instalación de dispositivos de vigilancia. Además, su actividad marítima en zonas alejadas de su territorio, incluyendo el Mediterráneo, ha llamado la atención de las autoridades europeas.

También existen actores no estatales, como organizaciones criminales o mercenarios, que podrían ser contratados para realizar actos de sabotaje. La opacidad del entorno subacuático, unida a la facilidad para disfrazar operaciones como accidentes, hace que estas amenazas sean particularmente difíciles de controlar.

Lo que revelan los casos: vulnerabilidad y descoordinación

Los estudios de caso recientes ponen de manifiesto dos grandes debilidades:

1. Falta de sistemas de vigilancia permanente en el fondo marino. A diferencia del espacio aéreo o terrestre, el entorno submarino carece de sensores constantes que puedan detectar actividades anómalas o identificar responsables con rapidez.
2. Descoordinación normativa y operativa. Al tratarse de infraestructuras transnacionales, muchas veces no está claro quién debe actuar, cómo compartir la información o qué protocolos seguir ante una emergencia.

Esto ha llevado a la necesidad urgente de redefinir la seguridad marítima en clave multidominio, integrando capacidades navales, cibernéticas, espaciales y

subacuáticas. En este nuevo enfoque, las tecnologías autónomas, como los drones submarinos y los sistemas de inteligencia artificial, jugarán un papel fundamental.

TECNOLOGÍAS AUTÓNOMAS PARA LA VIGILANCIA Y DEFENSA

Un nuevo paradigma en la seguridad marítima

Ante la creciente complejidad de las amenazas subacuáticas, la vigilancia tradicional basada en patrullas navales o medios tripulados ya no es suficiente. El entorno submarino exige sistemas que puedan operar a grandes profundidades, durante largos periodos de tiempo y con capacidad de detección avanzada. Aquí entran en juego las tecnologías autónomas, que marcan un cambio de paradigma en la defensa de infraestructuras críticas submarinas (CUI).

Estas tecnologías incluyen vehículos submarinos no tripulados (UUV), tanto de tipo autónomo (AUV) como operado a distancia (ROV), vehículos de superficie no tripulados (USV), sensores inteligentes, estaciones de recarga en el fondo marino, y algoritmos de inteligencia artificial (IA) para el análisis de datos. La combinación de estos elementos permite establecer una arquitectura de vigilancia continua y reactiva, incluso en áreas alejadas o difíciles de patrullar.

¿Qué sistemas se utilizan? Clasificación y ejemplos.

Los AUV (*Autonomous Underwater Vehicles*) son drones submarinos que se desplazan de forma autónoma siguiendo rutas preprogramadas. Se utilizan para realizar inspecciones de rutina, detectar objetos anómalos o mapear el lecho marino.

Los ROV (*Remotely Operated Vehicles*), en cambio, son controlados desde buques de superficie mediante cables y se emplean principalmente para intervenciones técnicas, como reparar un cable dañado o inspeccionar una anomalía detectada.

También existen vehículos híbridos, que pueden funcionar como AUV en fase de patrulla y como ROV cuando necesitan mayor control. Estos modelos ofrecen flexibilidad y son clave en misiones mixtas de vigilancia y mantenimiento.

Por su parte, los USV (*Unmanned Surface Vehicles*) operan en la superficie del mar y pueden actuar como nodos de comunicación, plataformas de detección o puntos de enlace con satélites y buques de mando.

A esto se suman nuevos desarrollos como estaciones de recarga submarinas, que permiten extender la autonomía de los AUV sin necesidad de recuperarlos,

y los primeros prototipos de centros de datos sumergidos, que buscan reducir el impacto energético y mejorar la conectividad bajo el mar.

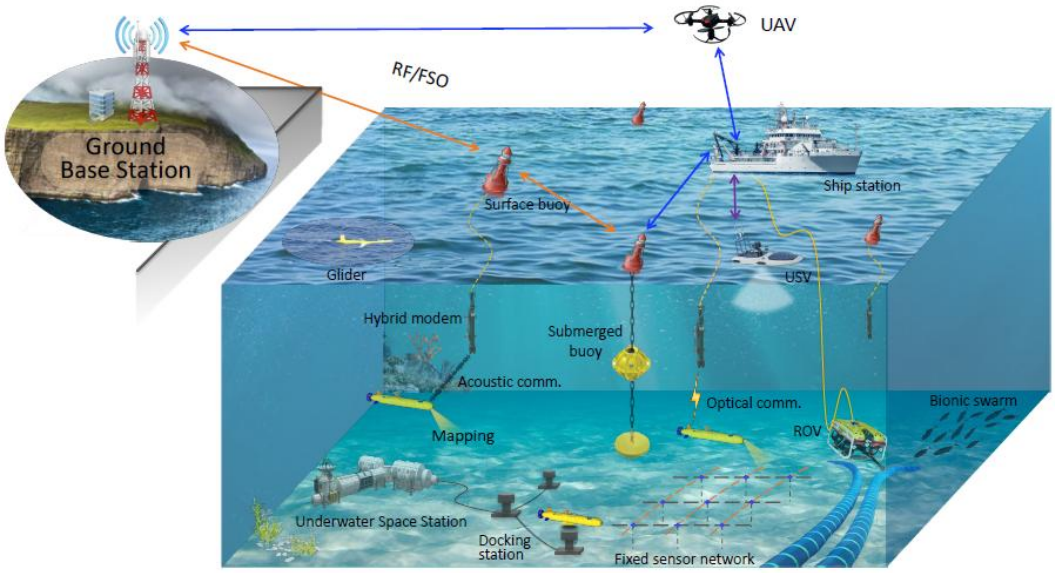

Fig. 3 - Representación de una red integrada de vigilancia en la dimensión submarina (Xu *et al.*, 2024)

Sensores inteligentes y vigilancia permanente

Un componente fundamental de estos sistemas son los sensores inteligentes, especialmente los acústicos. Entre ellos destaca el *Distributed Acoustic Sensing* (DAS), una tecnología que convierte los propios cables de fibra óptica en sensores capaces de detectar vibraciones, pasos de barcos o actividades sospechosas.

Otros sensores pueden medir temperatura, presión, movimientos sísmicos o incluso identificar patrones de ruido generados por hélices, anclas o robots subacuáticos. Todos estos datos se recogen y se envían, mediante conexiones acústicas o vía satélite, a un centro de control terrestre donde se procesan en tiempo real.

Este enfoque permite alcanzar una verdadera *underwater situational awareness*, es decir, una conciencia situacional del entorno subacuático que permite anticiparse a las amenazas y responder con rapidez.

Inteligencia artificial para detectar lo anómalo

La cantidad de datos generada por sensores, satélites y vehículos es inmensa. Para procesarlos de forma eficiente, se utilizan algoritmos de inteligencia artificial capaces de identificar patrones, detectar anomalías y lanzar alertas automáticas.

Por ejemplo, si una embarcación altera su ruta habitual, apaga su sistema de identificación o se aproxima a una infraestructura sin justificación, el sistema lo reconoce como comportamiento sospechoso. Estas herramientas permiten distinguir entre una actividad normal —como la pesca— y una potencial operación hostil.

También se utiliza fusión de información, una técnica que combina datos de diferentes fuentes (submarinas, satelitales, humanas, meteorológicas) para ofrecer una visión integrada y coherente del entorno marino. Esto ayuda a reducir errores y a tomar decisiones más rápidas y fundamentadas.

Ventajas y desafíos de las soluciones autónomas

Las tecnologías autónomas ofrecen múltiples ventajas: permiten vigilancia constante sin exponer personal, cubren grandes áreas con menor coste y reaccionan con mayor rapidez ante incidentes. Además, su despliegue puede disuadir a posibles agresores, al demostrar que las infraestructuras están monitorizadas.

Sin embargo, también presentan desafíos: necesitan una normativa clara que regule su uso en aguas internacionales; requieren inversión en mantenimiento y ciberseguridad; y deben integrarse en una estrategia coordinada con medios humanos y políticos.

Estas tecnologías no reemplazan a la diplomacia ni a la vigilancia convencional, pero se convierten en un complemento indispensable en la nueva arquitectura de seguridad subacuática del siglo XXI.

COOPERACIÓN INTERNACIONAL Y NUEVOS MARCOS JURÍDICOS

¿Quién protege el fondo del mar?

La defensa de las infraestructuras submarinas críticas no puede ser responsabilidad de un solo estado. Estas redes —que cruzan fronteras marítimas, conectan continentes y pertenecen en muchos casos a empresas privadas— requieren una cooperación internacional sólida y coordinada. Sin embargo, hasta hace poco, el tema apenas figuraba en las agendas de seguridad global.

El sabotaje al *Nord Stream* 2 fue un punto de inflexión. A partir de entonces, organizaciones como la OTAN y la Unión Europea han comenzado a desarrollar estrategias específicas para proteger estas infraestructuras, reconociendo que su vulnerabilidad constituye una amenaza directa para la seguridad colectiva, la economía y la estabilidad geopolítica.

La OTAN: una respuesta en clave estratégica

La OTAN ha incorporado explícitamente la protección de las CUI en su Concepto Estratégico de Madrid (2022). Posteriormente, ha creado varias estructuras dedicadas al tema, entre ellas el *Critical Undersea Infrastructure Coordination Cell* en Bruselas (2023), integrada en la División de Retos de Seguridad Emergentes. Esta célula tiene como misión coordinar la respuesta civil-militar, facilitar el intercambio de inteligencia y reforzar la preparación de los aliados.

Al mismo tiempo, el Comando Marítimo Aliado (MARCOM) en Northwood ha establecido un centro de seguridad submarina que supervisa actividades en zonas clave como el Báltico y el mar del Norte. La combinación de estas dos sedes —una operativa, otra de coordinación— representa un modelo integral de vigilancia y respuesta.

La OTAN también ha intensificado sus ejercicios militares con tecnologías autónomas, como el *Dynamic Messenger*, y ha promovido investigaciones a través de su Organización de Ciencia y Tecnología para mejorar el conocimiento del entorno subacuático.

La Unión Europea: normativa y resiliencia

A pesar de que la protección de las infraestructuras críticas submarinas (CUI) sigue siendo competencia primaria de los estados miembros, la Unión Europea ha comenzado a desempeñar un papel más estructurado en este ámbito. Desde la Directiva 2008/114/CE sobre las Infraestructuras Críticas Europeas, la UE ha intentado establecer una base jurídica común para identificar y proteger aquellos activos cuya destrucción tendría un impacto transfronterizo significativo. Sin embargo, las limitaciones de este marco inicial, como la exclusión de sectores clave como los cables submarinos, han hecho evidente la necesidad de una acción más coordinada y ambiciosa.

La evolución posterior de las políticas de ciberseguridad —a través de estrategias como la *Cybersecurity Strategy* de 2013, las directivas NIS y NIS2, y el reciente *Cyber Resilience Act*— ha contribuido a fortalecer la resiliencia del entorno digital europeo, reconociendo la dimensión estratégica de las infraestructuras de red que operan también en el ámbito submarino. La protección de estas infraestructuras se ha ido incorporando progresivamente dentro del marco de la seguridad energética, digital y marítima, dando lugar a una creciente interconexión entre ámbitos políticos tradicionalmente separados.

Una señal de esta evolución es la creación en enero de 2023 de una *task force* conjunta OTAN-UE para la protección de las infraestructuras críticas, seguida por la adopción en marzo de la nueva Estrategia de Seguridad Marítima de la UE. Esta estrategia reconoce explícitamente los riesgos híbridos y cibernéticos

que afectan a las infraestructuras subacuáticas, e impulsa la colaboración civil-militar, la innovación tecnológica y la coordinación operativa como pilares para afrontar esta amenaza creciente.

En suma, la Unión Europea ha comenzado a asumir un papel más proactivo en la protección de las CUI, buscando superar la fragmentación normativa y fortalecer su autonomía estratégica frente a vulnerabilidades externas e interferencias estatales hostiles. Esta tendencia se alinea con un proceso de securitización en curso, aunque todavía en una fase embrionaria y condicionado por la soberanía de los estados miembros.

Italia: estrategia nacional y liderazgo subacuático en el Mediterráneo

Italia ha integrado progresivamente la dimensión subacuática en sus políticas estratégicas nacionales, reconociendo su creciente valor en términos de seguridad, innovación tecnológica y autonomía estratégica. En respuesta al nuevo contexto geopolítico posterior a 2022, el país ha promovido un conjunto coordinado de iniciativas que reflejan un claro proceso de securitización, en línea con el enfoque de la Escuela de Copenhague. Las infraestructuras críticas submarinas, como los cables y gasoductos, se han convertido así en objetos referenciales de seguridad, legitimando la adopción de medidas extraordinarias a nivel normativo, tecnológico y operativo.

Entre las principales herramientas de esta estrategia destaca el Polo Nacional de la Dimensión Subacuática (PNS), con sede en La Spezia. Se trata de un centro multidisciplinar que promueve sinergias entre la *Marina Militare*, universidades, centros de investigación, empresas emergentes y tecnológicas, con el objetivo de reforzar las capacidades nacionales en vigilancia, protección e innovación en el entorno subacuático. El PNS actúa como catalizador tecnológico y como acelerador de la autonomía estratégica italiana en el “futuro dominio *underwater”*, especialmente en lo que respecta a la defensa de las infraestructuras críticas submarinas.

Otro pilar clave es el *Piano del Mare* 2023-2025, aprobado por el Comité Interministerial para las Políticas del Mar. Este plan estratégico establece una visión integrada del mar como espacio prioritario para la inversión, el desarrollo y la seguridad nacional, impulsando la protección de los intereses marítimos italianos y consolidando a Italia como nodo clave de conectividad y seguridad en el Mediterráneo.

Paralelamente, Italia ha iniciado el proceso de proclamación de una Zona Económica Exclusiva (ZEE) a través de la ley n.º 91 de 2021, que amplía su jurisdicción más allá de las 12 millas náuticas. Esta medida se refuerza con la creación de una autoridad nacional para el control de actividades subacuáticas,

lo que permitirá ejercer un control más eficaz sobre sus aguas y sobre las infraestructuras críticas allí presentes.

Con estas iniciativas, Italia ofrece un ejemplo de respuesta integral a las amenazas híbridas y a la creciente competencia geopolítica bajo el mar. Su enfoque combina legislación, innovación tecnológica y coordinación institucional, posicionando al país como un actor proactivo en la defensa de las infraestructuras críticas submarinas en el Mediterráneo.

Hacia un nuevo marco legal internacional

Uno de los grandes desafíos en la protección de las CUI es la insuficiencia del derecho marítimo internacional. La UNCLOS establece principios generales sobre libertad de navegación, instalación de cables y responsabilidades estatales, pero no ofrece mecanismos eficaces para la protección de infraestructuras frente a actos hostiles en zonas económicas exclusivas o alta mar.

Varios expertos y organizaciones proponen la creación de un acuerdo multilateral vinculante, específico para la protección de infraestructuras críticas submarinas. Este instrumento debería establecer obligaciones claras en cuanto a vigilancia, atribución de responsabilidades y cooperación transfronteriza.

Mientras tanto, algunos estados han comenzado a firmar acuerdos bilaterales y coaliciones ad hoc, y se han realizado simulacros conjuntos para preparar respuestas coordinadas ante posibles sabotajes o incidentes.

Una tarea compartida: instituciones, Estados y sector privado

Finalmente, no se puede olvidar que más del 80 % de los cables submarinos están en manos privadas. Empresas de telecomunicaciones, operadores energéticos y fabricantes de sistemas deben estar integrados en los planes de seguridad, compartir información y colaborar con autoridades civiles y militares.

Solo un enfoque verdaderamente multi actor y multidominio permitirá construir una red resiliente y segura, capaz de resistir amenazas híbridas y garantizar la continuidad de los servicios esenciales para nuestras sociedades.

REFLEXIONES FINALES

Las infraestructuras críticas submarinas, durante mucho tiempo invisibles para la opinión pública y ausentes en los debates estratégicos, han pasado a ocupar un lugar central en las políticas de seguridad internacional. Su vulnerabilidad ante amenazas híbridas —desde sabotajes encubiertos hasta ciberataques— ha

revelado la necesidad de repensar la seguridad marítima desde una perspectiva multidominio y tecnológica.

Este articulo ha mostrado cómo, tras eventos como el sabotaje del *Nord Stream*, los estados, las organizaciones internacionales y los actores privados han comenzado a desarrollar respuestas concretas. El uso de tecnologías autónomas, la creación de marcos legales más eficaces y el impulso a la cooperación civil-militar son hoy elementos indispensables para garantizar la protección de estos activos esenciales.

Italia representa un caso paradigmático de esta evolución, al transformar el discurso de la seguridad en políticas públicas ambiciosas que conjugan defensa, innovación y soberanía. En conjunto, estas iniciativas señalan una nueva fase en la securitización del espacio subacuático, en la que ya no se trata solo de vigilar el mar, sino de comprenderlo, anticiparse y protegerlo.

En definitiva, el futuro de la seguridad marítima pasa por el conocimiento profundo del dominio subacuático. La vigilancia permanente, la cooperación entre sectores civiles y militares, y el uso inteligente de la tecnología no son una opción, sino una necesidad urgente. Solo entendiendo el mar desde sus profundidades podremos garantizar un entorno más seguro, resiliente y sostenible para las próximas décadas.

(4468)

Madrid, 19 de mayo de 2025
EL CAPITÁN DE CORBETA

Fdo.: Francesco BARONE.

BIBLIOGRAFÍA

Aben, E. (2024) “Does the internet route around damage? - Baltic Sea cable cuts”, Ripe Labs, https://labs.ripe.net/author/emileaben/does-the-internet-route-around-damage-baltic-sea-cable-cuts/ [Consulta: 2 de marzo de 2025].

Abner, M., & Bauk, S. (2024) “On Underwater Data Centers: Surveillance, Monitoring, and Environmental Management in the Baltic Sea”, *JITA - Journal of Information Technology and Applications (Banja Luka) - APEIRON*, *24*(2). https://doi.org/10.7251/JIT2402142A [Consulta: 24 de enero de 2025].

Adam, N., Ali, M., Naeem, F., Ghazy, A. S., & Kaddoum, G. (2024) “State-of-the-Art Security Schemes for the Internet of Underwater Things: A Holistic Survey”, *IEEE Open Journal of the Communications Society*, *5*, 6561-6592. https://doi.org/10.1109/OJCOMS.2024.3474290 [Consulta: 27 de enero de 2025].

Advanced Navigation. (2024). *How Hydrus Micro-AUV leads the way in modern naval defense*, https://www.advancednavigation.com/robotics/micro-auv/hydrus/ [Consulta: 2 de febrero de 2025].

Aitken, A.J. (2018) “The next generation MCM platform – not yet full autonomy”, *Warship 2018 – Procurement of Future Surface Vessels, 11th – 12th September 2018, London, UK* [Consulta: 18 de enero de 2025].

Akbari, A. and Moazen, T.M. (2020) “Nord Stream 2 and the strategic balance of power”, *Petroleum Business Review,* 4(1) [Consulta: 18 de enero de 2025].

Bae, I. and Hong, J. (2023) “Survey on the Developments of Unmanned Marine Vehicles: Intelligence and Cooperation”, *Sensors*, 23(10), p. 4643. Available at: https://doi.org/10.3390/s23104643 [Consulta: 19 de enero de 2025].

Bai, Z. (2022) “The Cooperative Game of Energy Between Russia, US and EU—Based on the Perspective of Nord Stream 2 Pipeline”, *Journal of Innovation and Social Science Research*, 9(4). Available at: https://doi.org/10.53469/jissr.2022.09(04).06 [Consulta: 28 de enero de 2025].

Balzacq, T. (2005) “The Three Faces of Securitization: Political Agency, Audience and Context”, *European Journal of International Relations*, *11*(2), 171-201. https://doi.org/10.1177/1354066105052960 [Consulta: 16 de marzo de 2025].

Balzacq, T., Guzzini, S., Williams, M. C., Wæver, O., & Patomäki, H. (2015) “What kind of theory – if any – is securitization?” *International Relations*, *29*(1),

96-96. https://doi.org/10.1177/0047117814526606 [Consulta: 9 de febrero de 2025].

Bashfield, S. (2024) “Defending seabed lines of communication”, *Australian Journal of Maritime & Ocean Affairs*, pp. 1–13. https://doi.org/10.1080/18366503.2024.2363607 [Consulta: 15 de marzo de 2025].

Batzella, F. (2022) “Engaged but constrained. Assessing EU actorness in the case of Nord Stream 2”, *Journal of European Integration*, 44(6), pp. 821–835. https://doi.org/10.1080/07036337.2022.2043853 [Consulta: 15 de febrero de 2025].

Bazzarello, L. (2023) *Underwater surveillance with Maritime Unmanned Systems: usage of Artificial Intelligence against the threat of mines,* Tesis doctoral, Università di Pisa. Disponible en: https://www.researchgate.net/profile/Lorenzo-Bazzarello/publication/378858848 [Consulta: 10 de octubre de 2024].

Besch, S., Brown, E. (2024a) “A chinese-flagged ship cuts Baltic Sea internet cables. This time Europe was more prepared” *Carnegie Endowment*. https://carnegieendowment.org/emissary/2024/12/ [Consulta: 23 de febrero de 2025].

Besch, S., Brown, E., (2024) “Securing Europe's Subsea Data Cables: Challenges and Recommendations”, *CEIP: Carnegie Endowment for International Peace*. https://coilink.org/20.500.12592/3tq7wav [Consulta: 23 de febrero de 2025].

Boscariol, M. (2020). *Stato di eccezione, securitizzazione e tikkun internazionale*. Tesis Doctoral. Università Sacro Cuore di Milano. Disponible en https://publicatt.unicatt.it/retrieve/0ea09840-4e66-4a9a-b9db-5df934f0dc2c [Consulta: 20 de noviembre de 2024].

Boscariol, M. (2021) “Securitizzazione e stato di eccezione: Sulle origini schmittiane della Scuola di Copenaghen” *Ragion pratica, Rivista semestrale* 2/2021, pp. 561-582, https://doi.org10.1415/102328 [Consulta: 11 de enero de 2025].

Brake, D. (2019) “Submarine Cables: Critical Infrastructure for Global Communications”, *Information Technology & Innovation Foundation: Washington, DC, USA,* https://itif.org/publications/2019/04/19/ [Consulta: 18 de enero de 2025].

Bueger, C. (2022) *Security threats to undersea communications cables and infrastructure – consequences for the EU.* European Parliament coordinator: Policy Department for External Relations Directorate General for External Policies of the Union. https://www.researchgate.net/profile/Christian-Bueger/publication/361306264 [Consulta: 12 de marzo de 2025].

Bueger, C., Liebetrau, T. (2021) “Protecting hidden infrastructure: The security politics of the global submarine data cable network”, *Contemporary Security Policy*, *42*(3), 391-413. https://doi.org/10.1080/13523260.2021.1907129 [Consulta: 23 de enero de 2025].

Buzan, B., Wæver, O. and Wilde, J. de (1998) *Security: a new framework for analysis*. Boulder, Colorado: Lynne Rienner Publishers, Inc.

Cai, L. and Sun, Q. (2020) “Multiautonomous underwater vehicle consistent collaborative hunting method based on generative adversarial network”, *International Journal of Advanced Robotic Systems*, *17*(3), 1729881420925233. https://doi.org/10.1177/1729881420925233 [Consulta: 03 de febrero de 2025].

Calcagno, E., Marrone, A. (2023) *The Underwater Environment and Europe’s Defence and Security*. Istituto Affari Internazionali, 13. https://www.iai.it/en/pubblicazioni/c04/underwater-environment-and-europes-defence-and-security [Consulta: 10 de febrero de 2025].

Cannarozzo, M. (2024) “Un passo nel futuro della dimensione subacquea: Il Programma U212 NFS”, *Rivista Marittima, settembre – ottobre 2024* pp. 54-66. https://www.marina.difesa.it/mediacultura/editoria/marivista/ [Consulta: 20 de marzo de 2025].

Cassy, G. (2024) “How the UK could become a global leader in the subsea domain”, *Chatham House*, https://www.chathamhouse.org/2024/02/ [Consulta: 25 de marzo de 2025].

Chabert, V. (2022) “La nuova strategia per i fondali marini a tutela degli interessi strategici della Francia” *Opinio Juris*, 40-45, https://iris.uniroma1.it/retrieve/5e691d4c-3e1a-4269-a2c6-508abcf3a258/ [Consulta: 13 de enero de 2025].

Chen, M. and Zhu, D. (2018) “A Novel Cooperative Hunting Algorithm for Inhomogeneous Multiple Autonomous Underwater Vehicles”, *IEEE Access*, 6, pp. 7818–7828. Available at: https://doi.org/10.1109/ACCESS.2018.2801857. [Consulta: 15 de febrero de 2025].

Chen, X., & Zhou, T. (2023) “Negligible Warming Caused by Nord Stream Methane Leaks”, *Advances in Atmospheric Sciences*, *40*(4), 549-552. https://doi.org/10.1007/s00376-022-2305-x [Consulta: 20 de febrero de 2025].

Coito, J. (2021). *Maritime Autonomous Surface Ships: New Possibilities—and Challenges— in Ocean Law and Policy*. Trabajo academico. U.S. Naval War College. Disponible en: https://digital-commons.usnwc.edu/ils/vol97/iss1/19/ [Consulta: 03 de marzo de 2025].

Collective C.A.S.E. (2006) “Critical Approaches to Security in Europe: A Networked Manifesto”, *Security Dialogue*, *37*(4), 443-487. https://doi.org/10.1177/0967010606073085. [Consulta: 25 de enero de 2025].

Comisión Europea (2023) *EU-NATO Task force on the resilience of critical infrastructure – Final assessment report* https://commission.europa.eu/system/files/2023-06/ [Consulta: 10 de febrero de 2025].

Comunicación conjunta de la Comisión Europea al Parlamento Europeo y al Consejo, de 21 de febrero de 2025, *Plan de acción de la UE sobre la seguridad de los cables*. Disponible en: EUR-Lex - 52025JC0009 - EN - EUR-Lex [Consulta: 15 de abril de 2025].

Congressional Research Service (2023) *Protection of Undersea Telecommunication Cables: Issues for Congress*. https://www.congress.gov/crs-product/R47648 [Consulta: 17 de marzo de 2025].

Consejo de la Unión Europea (2023) *Strategia per la sicurezza marittima dell'Unione Europea.* https://www.consilium.europa.eu/media/67499/st14280-en23 [Consulta: 25 de febrero de 2025].

Convención de las Naciones Unidas sobre el Derecho del Mar. Disponible en: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf [Consulta: 20 de febrero de 2025].

DemiRkol, A. (2023) "A Perspective on Critical Security Concept and International Migration Nexus through Copenhagen School: The Quest for Societal Security" *Lectio Socialis*, *7*(1), 23-32. https://doi.org/10.47478/lectio.1146768 [Consulta: 03 de febrero de 2025].

Deruda, A. (2024) "Cavi sottomarini nel mirino: Strategie NATO contro i sabotaggi", *Agenda Digitale*, https://www.agendadigitale.eu/ [Consulta: 30 de enero de 2025].

Dimitrov, N., Karakolev, K. (2024) "Seabed Critical Infrastructures" *Information & Security: An International Journal*, *55*(2), 133-148. https://doi.org/10.11610/isij.5566. [Consulta: 28 de enero de 2025].

Dol, H., Blom, K., Van Riet, M., & Van De Sande, J. (2022) "High-bandwidth acoustic data communication for stand-off identification by autonomous underwater vehicles", *OCEANS 2022, Hampton Roads*, 1-10. https://doi.org/10.1109/OCEANS47191.2022.9977353 [Consulta: 06 de febrero de 2025].

European Defence Agency (2023) *Critical Seabed Infrastructure Protection (CSIP)*. https://www.pesco.europa.eu/project/critical-seabed-infrastructure-protection-csip/ [Consulta: 6 de marzo de 2025].

Floyd, R. (2007) "Human Security and the Copenhagen School's Securitization Approach: Conceptualizing Human Security as a Securitizing Move", *HUMAN SECURITY JOURNAL*, *5*, 38-49 [Consulta: 15 de febrero de 2025].

Franchino, C. (2024) *Il dominio undewater: Italia, Europa e Stati Uniti tra geopolitica, risorse e sicurezza*. Centro Studi Americani – Ministero degli Affari Esteri e della Cooperazione Internazionale. https://centrostudiamericani.org/ [Consulta: 5 de febrero de 2025].

Fridbertsson, N.T. (2023) *Protecting critical maritime infrastructure – the role of technology*. https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc [Consulta: 14 de enero de 2025].

Frugiuele, A. (2024) "Cavi sottomarini. Tra fragilità e risposte securitarie: NATO, UE e il ruolo dell'Italia", *Cybersecurity Italia*, https://www.cybersecitalia.it/32313/ [Consulta: 30 de enero de 2025].

General Secretariat of the Council. (2023). *Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan*. Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2023/10/24 [Consulta: 17 de febrero de 2025].

Gili, A. (2022) "Cavi: Interessi di stato in gioco", *Istituto per gli studi di politica internazionale*, https://www.ispionline.it/it/pubblicazione/36487/ [Consulta: 1 de febrero de 2025].

Gili, A. (2024a) "Cavi sottomarini: Le nuove autostrade dei dati", *Istituto per gli studi di politica internazionale* https://www.ispionline.it/it/pubblicazione/193654/ [Consulta: 12 de febrero de 2025].

Gili, A. (2024b) "Oceani: È la corsa al nuovo Eldorado", *Istituto per gli studi di politica internazionale*, https://www.ispionline.it/it/pubblicazione/172769/ [Consulta: 12 de febrero de 2025].

González-García, J., Gómez-Espinosa, A., Cuan-Urquizo, E., García-Valdovinos, L. G., Salgado-Jiménez, T., & Cabello, J. A. E. (2020) "Autonomous Underwater Vehicles: Localization, Navigation, and Communication for Collaborative Missions", *Applied Sciences*, *10*(4), 1256. https://doi.org/10.3390/app10041256 [Consulta: 19 de febrero de 2025].

Gresh, G. F. (2023) "Europe's new maritime security reality: Chinese ports, Russian bases, and the rise of subsea warfare", *Brookings,* https://www.brookings.edu/articles/ [Consulta: 12 de febrero de 2025].

Hasan, K., Ahmad, S., Liaf, A. F., Karimi, M., Ahmed, T., Shawon, M. A., & Mekhilef, S. (2024) "Oceanic Challenges to Technological Solutions: A Review of Autonomous Underwater Vehicle Path Technologies in Biomimicry, Control, Navigation, and Sensing", *IEEE Access*, *12*, 46202-46231. https://doi.org/10.1109/ACCESS.2024.3380458 [Consulta: 12 de febrero de 2025].

Horn, A. M. (2022). *Subsea Technology*. 21st International Ship and Offshore Structures Congress (ISSC 2022). https://www.issc2022.org/ [Consulta: 29 de enero de 2025].

Instituto Español de Estudios Estratégicos (2024a). *Geopolítica azul. Los océanos, espacios clave en el nuevo orden global* (Cuadernos de Estrategia, n. 227). Ministerio de Defensa, Secretaría General Técnica. Disponible en: publicaciones.defensa.gob.es [Consulta: 13 de febrero de 2025].

Isac, H., Asan, D., Popa, C., & Popa, N.-S. (2024) "Optimizing the efficiency of lighting sources for underwater inspections", *TechHub Journal*, *7*, 177-182. https://doi.org/10.47577/techhub.v7i.118 [Consulta: 04 de marzo de 2025].

Iuvinale, G., Iuvinale, N. (2025) "Attacchi ai cavi sottomarini: Strategie di sicurezza e resilienza", *Agenda Digitale*, https://www.agendadigitale.eu/sicurezza/ [Consulta: 12 de febrero de 2025].

Joint White Paper for European Defence Readiness 2030, presentado por la Alta Representante de la Unión para Asuntos Exteriores y Política de Defensa de la Comisión Europea el 19 de marzo de 2025. Disponible en: https://www.eeas.europa.eu/eeas/white-paper-for-european-defence-readiness-2030 [Consulta: 15 de abril de 2025].

Kapur, S., & Mabon, S. (2018) "The Copenhagen School goes global: Securitisation in the Non-West", *Global Discourse*, *8*(1), 1-4. https://doi.org/10.1080/23269995.2018.1424686 [Consulta: 16 de marzo de 2025].

Karner, M., Peltola, J., Jerne, M., Kulas, L., & Priller, P. (2024). *Intelligent Secure Trustable Things* (Vol. 1147). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54049-3.

Kauranen, A., Siebold, S. (2024) "As sabotage allegations swirl, NATO struggles to secure the Baltic Sea", *Reuters*, https://www.reuters.com/world/sabotage-allegations-swirl-nato-struggles-secure-baltic-sea-2024-12-03/ [Consulta: 12 de febrero de 2025].

Kaushal, S. (2023) "Stalking the seabed: How Russia targets critical undersea infrastructure", *Royal United Services Institute (RUSI)* https://www.rusi.org [Consulta: 12 de febrero de 2025].

Klein, N. (2019) *Maritime Autonomous Vehicles within the International Law Framework to Enhance Maritime Security*, Trabajo academico. U.S. Naval War College. Disponible en: https://digital-commons.usnwc.edu/ils/vol95/iss1/8/ [Consulta: 03 de marzo de 2025].

Knudsen, O. F. (2001) "Post Copenhagen security studies: Desecuritizing securitization", *SAGE Publications*, *32*(3), 355-368 [Consulta: 02 de marzo de 2025].

Koshino, Y. (2024) "Submarine Cables in the Indo-Pacific: Expanding the EU's Role", *EUISS* https://policycommons.net/artifacts/17852801/18748641 [Consulta: 10 de marzo de 2025].

Kumar, R. (2023). Securing the Digital Seabed: Countering China's Underwater Ambitions. *Journal of Indo-Pacific Affairs*, *6*(8), https://www.airuniversity.af.edu/JIPA/Display/Article/3588497 [Consulta: 10 de marzo de 2025].

Lacerenza, V., Minuto, M. (2023) “La dimensione subacquea della Marina Militare”, *Rivista Marittima*, *7* (luglio-agosto 2023), 21-26, https://www.marina.difesa.it/mediacultura/editoria/marivista/ [Consulta: 20 de marzo de 2025].

Liebetrau, T., & Bueger, C. (2024) “Advancing coordination in critical maritime infrastructure protection: Lessons from maritime piracy and cybersecurity”, *International Journal of Critical Infrastructure Protection*, *46*, 100683. https://doi.org/10.1016/j.ijcip.2024.100683 [Consulta: 11 de marzo de 2025].

Loik, R. (2024) “Undersea Hybrid Threats in Strategic Competition: The Emerging Domain of NATO–EU Defense Cooperation”, *Journal on Baltic security,* https://doi.org/10.57767/JOBS_2024_008, [Consulta: 25 de marzo de 2025].

Maglaras, L., Janicke, H., & Ferrag, M. A. (2022) “Combining Security and Reliability of Critical Infrastructures: The Concept of Securability”, *Applied Sciences*, *12*(20), 10387. https://doi.org/10.3390/app122010387 [Consulta: 06 de marzo de 2025].

Mao, Y. (2024) “Research and Applications of Autonomous Underwater Vehicles”, *Science and Technology of Engineering, Chemistry and Environmental Protection*, *1*(9). https://doi.org/10.61173/smmah335 [Consulta: 09 de marzo de 2025].

Marchesi, G. (2024) “Dimensione subacquea: importanza e vulnerabilità dei cavi sottomarini”, *Geopolitica.info*, https://www.geopolitica.info/importanza-e-vulnerabilita-dei-cavi-sottomarini/ [Consulta: 25 de marzo de 2025].

Marina Militare e Fondazione Leonardo (2023) *‘Rapporto civiltà del mare. Geopolitica, strategia, interessi nel mondo subacqueo. Il ruolo dell’Italia’*. https://www.fondazioneleonardo.com/sites/default/files/downloads/2024-05 [Consulta: 15 de enero de 2025].

Martini, F. (2024a) *La protezione dei cavi sottomarini fra intervento pubblico e interesse alla libertà dei mari*, Mercato concorrenza regole, XXVI (1–2), pp. 275–304. https://www.rivisteweb.it/doi/10.1434/116126 [Consulta: 20 de enero de 2025].

Martini, F. (2024b) *Tutela delle infrastrutture subacquee di interesse strategico per il Paese: modelli possibili di sorveglianza, intervento e deterrenza*. Centro Alti Studi della Difesa https://www.difesa.it/assets/allegati/46666/as-smm-04.2024.06.06.14.12.52.044.pdf [Consulta: 20 de enero de 2025].

Masiello, A. (2022). *Sicurezza delle reti e infrastrutture critiche nel Mediterraneo*. Italia Strategic Governance. https://cesmar.it/wp-content/uploads/2023/05/ [Consulta: 18 de marzo de 2025].

McCabe, R., Flynn, B. (2024) “Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure” *European Security*, *33*(2), 324-344. https://doi.org/10.1080/09662839.2023.2248001 [Consulta: 25 de marzo de 2025].

McDonald, M. (2008) “Securitization and the Construction of Security”, *European Journal of International Relations*, *14*(4), 563-587. https://doi.org/10.1177/1354066108097553 [Consulta: 12 de marzo de 2025].

Ministerio de Defensa. (2024). *Estrategia Nacional de Seguridad Marítima 2024*. https://www.dsn.gob.es/es/publicaciones/estrategias-sectoriales/ENSM2024 [Consulta: 5 de abril de 2025].

Ministero per la protezione civile e le politiche del mare (2024) *Relazione sullo stato di attuazione del Piano del Mare*. https://www.camera.it/temiap/2024/07/16/OCD177-7438.pdf [Consulta: 10 de abril de 2025].

Mitrescu, S. (2025). *Protecting critical maritime infrastructure in the Black Sea*. New Strategy Center. https://newstrategycenter.ro/wp-content/uploads/2025/02/Critical-Infrastructure-Study-WEB.pdf [Consulta: 29 de marzo de 2025].

Monaghan, S., Svendsen, O. (2023) *NATO’s Role in Protecting Critical Undersea Infrastructure*, Center for Strategic and International Studies (CSIS BRIEFS), https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure [Consulta: 6 de abril de 2025].

Natalizia, G., Mazziotti, M. (2024) *La NATO nel Mediterraneo allargato*. Centro Studi Geopolitica - Osservatorio di politica internazionale. https://unora.unior.it/bitstream/11574/229364/1/ [Consulta: 3 de marzo de 2025].

NATO (2022) *NATO 2022 Strategic Concept*. https://www.nato.int/cps/en/natohq/topics_210907.htm [Consulta: 8 de enero de 2025].

NATO (2023a) *FACTSHEET - DYNAMIC MESSENGER 23*. https://mc.nato.int/resources/site1/General/20230925%20FACTSHEET%20-%20DYNAMIC%20MESSENGER%2023.pdf [Consulta: 18 de enero de 2025].

NATO (2023b) *Science & Technology Trends 2023-2043 Vol. 1 e 2*. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf [Consulta: 8 de enero de 2025].

NATO (2024a) *NATO Science and Technology Organization 2023 Highlights*. https://www.sto.nato.int/public/20240223_UC_%20STO_Highlights_web.pdf [Consulta: 8 de enero de 2025].

NATO (2024b) *Secretary's general Annual report 2023*. https://www.nato.int/cps/en/natohq/opinions_223291.htm [Consulta: 18 de enero de 2025].

NATO. (2024c). *Washington summit declaration*. https://www.nato.int/cps/en/natohq/official_texts_227678.htm [Consulta: 18 de enero de 2025]

NATO. (2025). *4th Maritime Security Conference (27-28 June 2024) Proceeding protection of maritime critical infrastructures and the seabed*. Maritime Security Centre of Excellence. https://www.marseccoe.org/wp-content/uploads/2025/03/4th-Maritime-Security-Proceedings.pdf [Consulta: 8 de enero de 2025].

Nkenyereye, L., Nkenyereye, L., & Ndibanje, B. (2024) "Internet of Underwater Things: A Survey on Simulation Tools and 5G-Based Underwater Networks", *Electronics*, *13*(3), 474. https://doi.org/10.3390/electronics13030474 [Consulta: 18 de marzo de 2025].

Özcan, S. (2013) "Securitization of energy through the lenses of Copenhagen School", *International Relations*, *4*. [Consulta: 03 de marzo de 2025].

Palomeras, N., Furfaro, T., Williams, D. P., Carreras, M., & Dugelay, S. (2022) "Automatic Target Recognition for Mine Countermeasure Missions Using Forward-Looking Sonar Data", *IEEE Journal of Oceanic Engineering*, *47*(1), 141-161. https://doi.org/10.1109/JOE.2021.3103269 [Consulta: 15 de marzo de 2025].

Panero, E., Oliva, S., Cassetta, M. (2024) *Il (quasi) dominio-sottomarino: dipendenze, minacce e prospettive per proteggere, operare e primeggiare negli abissi.* Centro Studi Internazionali CESI. https://www.key4biz.it/wp-content/uploads/2024/07 [Consulta: 5 de enero de 2025].

Pawlak, J., Peters, J. (Eds.) (2021). *From the North Atlantic to the South China Sea: Allied Maritime Strategy in the 21st Century*. Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748921011

Pedrozo, R. (2025a). *Implementing Agreement to Enhance Protection of Critical Undersea Infrastructure*. Trabajo academico. Stockton Center for International Law. Disponible en: https://digital-commons.usnwc.edu/ils/vol106/iss1/7/ [Consulta: 14 de marzo de 2025].

Pedrozo, R. (2025b). *Safeguarding Submarine Cables and Pipelines in Times of Peace and War*. Trabajo academic. Stockton Center for International Law.

Disponible en: https://digital-commons.usnwc.edu/ils/vol106/iss1/2/ [Consulta: 21 de marzo de 2025].

Peruzzi, L. (2024) “Decolla il Polo nazionale dimensione subacquea”, *Analisi Difesa*, https://www.analisidifesa.it/2024/05 [Consulta: 15 de enero de 2025].

Petit, Z. (2024) “Beneath NATO’s radars: Unaddressed threats to subsea cables”, *Center for Strategic and International Studies (CSIS),* https://www.csis.org/blogs/strategic-technologies-blog, [Consulta: 18 de enero de 2025].

Pinto, M. A., Lyonnet, B., Simian, T., & Meltzheim, S. (2023) “A New High Resolution AUV-Based Synthetic Aperture Sonar for Challenging Environmental Conditions”, *OCEANS 2023 - MTS/IEEE U.S. Gulf Coast*, 1-5. https://doi.org/10.23919/OCEANS52994.2023.10337370 [Consulta: 08 de marzo de 2025].

Poli, E. (2024) “Cavi sottomarini, ecco come si muovono gli equilibri geopolitici”, *Agenda Digitale* https://www.agendadigitale.eu/sicurezza/cavi-sottomarini-le-nuove-frontiere-della-geopolitica-digitale/ [Consulta: 18 de enero de 2025].

Potter, J. R., Wengle, E., RØrstadbotnen, R. A., & Dong, H. (2024) “First Demonstration of Underwater Acoustic Communication from Sea to Shore via an Optical Fibre using Distributed Acoustic Sensing”, *2024 Seventh Underwater Communications and Networking Conference (UComms)*, 1-5. https://doi.org/10.1109/UComms64662.2024.10847975 [Consulta: 16 de marzo de 2025].

Recomendación (UE) 2024/779 del 26 febrero 2024 de la Comisión Europea, sobre infraestructuras de cable submarino seguras y resistentes. Gazzetta Ufficiale dell’Unione Europea IT serie L del 08.03.2024. Disponible en: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202400779 [Consulta: 7 de marzo de 2025].

Resolución de 31 de julio de 2023, del Comité Interministerial de Políticas del Mar, *Approvazione del Piano del Mare per il triennio 2023-2025*. Supplemento ordinario alla “Gazzetta Ufficiale” n. 248 del 23 ottobre 2023. Disponible en: https://www.gazzettaufficiale.it/eli/id/2023/10/23/23A05758/sg [Consulta: 7 de marzo de 2025].

Ripanti, G. (2023) *Cavi sottomarini. Dati e infrastrutture per le Comunicazioni e la Difesa*. Tesi di Laurea. LUISS Guido Carli di Roma. Disponible en: https://tesi.luiss.it/39453/1/649772 [Consulta: 10 de enero de 2025].

Rui, S. (2023) “Deep Underground Science and Engineering—Seabed structures and foundations related to deep-sea resource”, *Deep Underground Science and Engineering*, *2024;3*, 131-148. https://doi.org/10.1002/dug2.12042 [Consulta: 18 de marzo de 2025].

Runde, D., Murphy, E. and Bryja, T. (2024) *Safeguarding Subsea Cables*. Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816 [Consulta: 23 de enero de 2025].

Sadurski, L. (2022) “Regional Security Complex Theory: Why Is this Concept Still Worth Developing?”, *Athenaeum*, *75*(3), 137–153. https://doi.org/10.15804/athena.2022.75.08 [Consulta: 09 de marzo de 2025].

Sanchez, P. J. B., Papaelias, M., & Marquez, F. P. G. (2020) “Autonomous underwater vehicles: Instrumentation and measurements”, *IEEE Instrumentation & Measurement Magazine*, *23*(2), 105-114. https://doi.org/10.1109/MIM.2020.9062680 [Consulta: 15 de marzo de 2025].

Santos, M. C. D. (2018) “Identity and Discourse in Securitisation Theory”, *Contexto Internacional*, *40*(2), 229-248. https://doi.org/10.1590/s0102-8529.2018400200003 [Consulta: 13 de marzo de 2025].

Scipanov, L. V. (2024). *Doctrinal consideration about Seabed Warfare*. Romanian Military Thinking, *2024*(3). https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2024/3/SCIPANOV%2C%20SAVA.pdf [Consulta: 27 de enero de 2025].

Shattuck, Lewis IV B.; Suursoo, Melissa A.; Carr, Christopher J.; Franco, Jahdiel; Mierzwa, Cheryl (2018). *Seabed Warfare and the XLUUV*. Tesis. Naval Postgraduate School Monterey (USA) Disponible en: https://apps.dtic.mil/sti/citations/AD1060064 [Consulta: 12 de enero de 2025].

Soldi, G., Gaglione, D., Raponi, S., Forti, N., d'Afflisio, E., Kowalski, P., Warner, C. (2023) “Monitoring of underwater critical infrastructures: the Nord Stream and other recent case studies”, *arXiv preprint arXiv:2302.01817*. https://doi.org/10.48550/arXiv.2302.01817 [Consulta: 01 de marzo de 2025].

Steinberg, A., Gestermann, N., Ceranna, L., Hartmann, G., Lund, B., Dunham, E., Hupe, P., Voss, P., Larsen, T., Dahl-Jensen, T., Köhler, A., Schweitzer, J., Pilger, C., Plenefisch, T., Stammler, K., Donner, S., Gaebler, P., & Wiedle, C. (2025). *Source analysis of the 2022 Nord Stream and 2023 Balticconnector underwater explosions*. https://doi.org/10.5194/egusphere-egu24-7660 [Consulta: 30 de marzo de 2025].

Stępka, M. (2022) “The Copenhagen School and Beyond. A Closer Look at Securitisation Theory” En M. Stępka, *Identifying Security Logics in the EU Policy Discourse* (pp. 17-31). Springer International Publishing. https://doi.org/10.1007/978-3-030-93035-6_2 [Consulta: 14 de marzo de 2025].

Stritzel, H. (2007) “Towards a Theory of Securitization: Copenhagen and Beyond”, *European Journal of International Relations*, *13*(3), 357-383. https://doi.org/10.1177/1354066107080128 [Consulta: 02 de marzo de 2025].

Stritzel, H. (2007) “Towards a Theory of Securitization: Copenhagen and Beyond”, *European Journal of International Relations*, 13(3), pp. 357–383. https://doi.org/10.1177/1354066107080128 [Consulta: 26 de enero de 2025].

Tabish, N., & Chaur-Luh, T. (2024) “Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives”, *IEEE Access*, *12*, 17114-17136. https://doi.org/10.1109/ACCESS.2024.3357082 [Consulta: 17 de marzo de 2025].

Tsoy, K.A. (2022) “Nord Stream 2: The Expectations of Russian Citizens from Increasing Gas Exports to Europe”, *Management Science and Business Decisions*, 2(1), pp. 48–60, https://doi.org/10.52812/msbd.38 [Consulta: 26 de enero de 2025].

Van Riet, M. W. G., Alves, J., Arcieri, G., Bazzarello, L., De Sousa, J. B., Colin, M., Cormack, A., Dias, P., Dinale, J., Ferri, G., Fioravanti, S., Furfaro, T., Guesdon, M., Horstmann, M., Maciaś, M., Marshall, B., Morlando, L., Munafò, A., Newsum, V., … Tesei, A. (2023) “Experimental Demonstrations of CATL, the Collaborative Autonomy Tasking Layer”, *OCEANS 2023 - Limerick*, 1-9. https://doi.org/10.1109/OCEANSLimerick52467.2023.10244669 [Consulta: 20 de marzo de 2025].

Van Riet, M. W. G., Van De Sande, J., Newsum, V., & Van Vossen, R. (2022) “TEAM: a framework for full mission autonomy using collaborative, heterogenous autonomous vehicles”, *OCEANS 2022, Hampton Roads* (pp. 1-8). IEEE. https://doi.org/10.1109/OCEANS47191.2022.9977138 [Consulta: 20 de marzo de 2025].

Van Soest, H., Fine, H. (2024) “Vital yet vulnerable: Undersea infrastructure needs better protection”, *RAND* https://www.rand.org/pubs/commentary/2024/03 [Consulta: 26 de enero de 2025].

Walter, M. J., Barrett, A., Walker, D. J., & Tam, K. (2023) “Adversarial AI Testcases for Maritime Autonomous Systems”, *AI, Computer Science and Robotics Technology*, *2*. https://doi.org/10.5772/acrt.15 [Consulta: 15 de febrero de 2025].

Weingarten, J. (2023) “Developing future capabilities: Robotics and autonomous systems”, *NATO Parliamentary Assembly. URL: https://www. natopa. int/document/2023-robotics-and-autonomous-systems-report-weingarten-034-stctts* [Consulta: 07 de marzo de 2025].

Wiig, M. S., Krogstad, T. R., & Midtgaard, O. (2012) “Autonomous identification planning for my countermeasures” *2012 IEEE/OES Autonomous Underwater Vehicles (AUV)*, 1-8. https://doi.org/10.1109/AUV.2012.6380733 [Consulta: 10 de marzo de 2025].

Wilson, D.E. (2017) “Russia’s Northern Rook: Nord Stream 2 on the European Energy Chessboard”, *Independent Study Project (ISP) Collection* https://digitalcollections.sit.edu/isp_collection/2754/ [Consulta: 20 de febrero de 2025].

Wood, S. (2024) “Germany and Nord Stream 2: evolution and end of an incongruous policy”, *International Politics*, 61(4), pp. 718–741. https://doi.org/10.1057/s41311-023-00453-9 [Consulta: 18 de marzo de 2025].

Wrange, J. (2022) “Entangled security logics: From the decision-makers’ discourses to the decision-takers’ interpretations of civil defence” *European Security*, *31*(4), 576-596. https://doi.org/10.1080/09662839.2021.2021889 [Consulta: 3 de febrero de 2025].

Xu, J., Irigoien, X. and Alouini, M.-S. (2024) “State-of-the-Art Underwater Vehicles and Technologies Enabling Smart Ocean: Survey and Classifications”, arXiv. Available at: https://doi.org/10.48550/arXiv.2412.18667 [Consulta: 11 de marzo de 2025].

Yang, Q., Yin, Y., Chen, S., & Liu, Y. (2021) “Autonomous exploration and navigation of mine countermeasures USV in complex unknown environment”, *2021 33rd Chinese Control and Decision Conference (CCDC)*, 4373-4377. https://doi.org/10.1109/CCDC52312.2021.9602457 [Consulta: 08 de marzo de 2025].

Yordanova, V., & Gips, B. (2020) “Coverage Path Planning with Track Spacing Adaptation for Autonomous Underwater Vehicles”, *IEEE Robotics and Automation Letters*, *5*(3), 4774-4780. https://doi.org/10.1109/LRA.2020.3003886 [Consulta: 09 de marzo de 2025].

Zacchini, L., Topini, A., Franchi, M., Secciani, N., Manzari, V., Bazzarello, L., Stifani, M., & Ridolfi, A. (2023) “Autonomous Underwater Environment Perceiving and Modeling: An Experimental Campaign with FeelHippo AUV for Forward Looking Sonar-Based Automatic Target Recognition and Data Association”, *IEEE Journal of Oceanic Engineering*, *48*(2), 277-296. https://doi.org/10.1109/JOE.2022.3209719 [Consulta: 14 de marzo de 2025].

Zhou, J. (2022) “The (universal) human and beyond: Constituting security objects in theory and practice”, *Critical Studies on Security*, *10*(1), 16-29. https://doi.org/10.1080/21624887.2021.2012394 [Consulta: 24 de marzo de 2025].

Zhou, J., Si, Y., & Chen, Y. (2023) “A Review of Subsea AUV Technology”, *Journal of Marine Science and Engineering*, *11*(6), 1119. https://doi.org/10.3390/jmse11061119 [Consulta: 17 de marzo de 2025].