EL LECHO MARINO CONVERTIDO EN ÁREA ESTRATÉGICA. ANÁLISIS DE INCIDENTES Y CAPACIDAD DE PROTECCIÓN

Miguel LÓPEZ GARAY

It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy.

Almirante James Stavridis (US Navy)

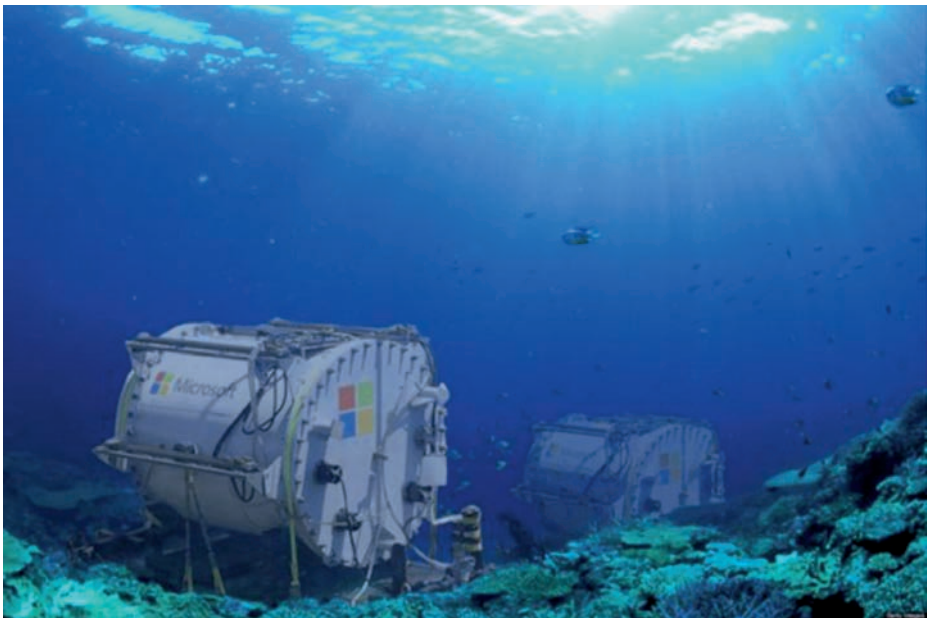
Introducción: infraestructuras críticas en el lecho marino

lo largo de la historia, los océanos han servido de puentes para acercar y conectar las distintas regiones cardinales del mundo. Desde la epopeya de los marinos españoles en 1492, que marcó el inicio de las rutas comerciales transatlánticas, hasta la actualidad, en que el 90 por 100 de las mercancías y materias primas se transportan por mar, este medio ha sido un elemento fundamental y facilitador de la globalización. Y así lo sigue siendo en la denominada «era digital», en la que el lecho marino se ha erigido como un componente esencial para sectores tan vitales como las telecomunicaciones y la energía, con cables submarinos y gasoductos que discurren a través de las distintas cuencas marinas, uniendo orillas y civilizaciones.

Como auténticos impulsores de la globalización, los cables submarinos posibilitan la comunicación instantánea entre continentes, desempeñando un papel crucial en las operaciones militares, el comercio internacional y la colaboración científica. Transformados en infraestructuras críticas, actúan como la columna

vertebral que garantiza la conectividad global y geoeconomía. Son esenciales para el comercio internacional, facilitan transacciones millonarias y transportan volúmenes inmensurables de datos, con demandas de ancho de banda en constante aumento. En el ámbito militar, aseguran el acceso a las redes de mando y control en regiones estratégicas, como son los archipiélagos canario y balear en España. Además, en el ámbito civil proporcionan comunicaciones en tiempo real y a gran velocidad entre cualquier ubicación del planeta. En el futuro próximo, también desempeñarán un papel esencial en el desarrollo de la industria energética renovable, particularmente en proyectos eólicos *offshore* y, en especial, en su integración en la red terrena. Además, comienzan a emplearse para el conexionado de distintas estructuras que permiten albergar inmensos servidores de datos en la mar, con las ventajas energéticas que ello supone.

Paralelamente, los gasoductos han emergido como infraestructuras clave que respaldan la disponibilidad de recursos y favorecen la diversificación energética, factores cruciales en el actual contexto geopolítico y ante el creciente consumo de energía, que requiere de la multiplicidad de fuentes energéticas como medida de resiliencia y seguridad, así como para estabilizar los costes, evitando posibles volatilidades en el mercado. Por ello, son clasificados igualmente como infraestructuras críticas, pilares también fundamentales para el



Centros de datos submarinos de Microsoft.
(Fuente: Asociación de Fabricantes y Distribuidores, AECOC)

mantenimiento de la industria, los servicios básicos y el consumo doméstico. Asimismo, dada la progresiva reducción del carbón, se estima que la mayor parte del petróleo y del gas circulan hoy día a través de estas infraestructuras subacuáticas, que contribuyen además a la reducción de costes y emisiones asociados al transporte de hidrocarburos. Por ello, se encuentran en expansión y, de acuerdo con el estudio elaborado por la agencia Global Energy Monitor publicado en diciembre de 2023, «la longitud de los gasoductos actualmente en construcción es suficiente para dar una vuelta y media a la Tierra» (1).

Esta pequeña introducción nos sirve para poner el foco en cómo el avance de las tecnologías submarinas ha generado un incremento exponencial del empleo de los lechos marinos en todos los ámbitos de la sociedad, abriendo sendas oportunidades de desarrollo y, por ende, entrañando nuevos riesgos y amenazas a la seguridad nacional. Las sanciones impuestas a Rusia tras la invasión de Ucrania y los incidentes en el mar del Norte o en el Báltico han puesto de manifiesto la importancia de proteger las infraestructuras críticas submarinas.

A lo largo de este artículo analizamos el valor estratégico de las infraestructuras submarinas y exploramos algunos de los últimos incidentes para exponer las principales amenazas que pueden poner en riesgo su funcionamiento.

Historia de incidentes y ataques contra cables submarinos

A pesar de su papel crucial en la conectividad global, las infraestructuras submarinas enfrentan una serie de amenazas que ponen en riesgo su integridad y operatividad. Los incidentes más comunes abarcan desde daños causados por el fondeo de barcos hasta consecuencias derivadas de desastres naturales, especialmente los relacionados con la actividad sísmica, como fue el caso del terremoto en Tohoku ocurrido en 2011 al este de Japón que, además de consecuencias desastrosas en tierra, tuvo un gran impacto en la cadena de suministro (2); o la explosión del volcán submarino Hunga Tonga-Hunga Ha'apai frente a la costa de Tonga en enero de 2022, que ocasionó la destrucción del único cable submarino de internet, dejando al país desconectado durante cinco semanas del resto del mundo, lo que impactó directamente en su economía.

Igualmente, el efecto de las actividades humanas —como la pesca de arrastre y la construcción de islas artificiales y plataformas— plantea riesgos significativos para cualquier infraestructura subacuática. Los cortes accidentales ocurren

---

(1) «Global gas pipeline expansion: Nearly US$200 billion under construction, with Asia building over 80%». *Global Energy Monitor: Briefing*, diciembre de 2023, en *https://globalenergymonitor.org/wp-content/uploads/2023/11/GEM_Global_gas_pipeline_expansion.pdf*

(2) RANGHIERI, F.; ISHIWATARI, M.: «Learning from Megadisasters. Lessons from the great East Japan Earthquake». *The World Bank*, 2014, en *https://openknowledge.worldbank.org/entities/publication/db0df170-6101-526e-8fc8-d0e448196fc4*

con más frecuencia de lo que se podría pensar, y distintos estudios basados en el uso generalizado de sistemas de identificación automática (AIS) indican que hasta el 77 por 100 de los fallos en cables submarinos se deben a fondeos y actividades de pesca de arrastre (3) . Estas acciones, a menudo llevadas a cabo sin intención, tienen consecuencias significativas en la conectividad y entrañan reparaciones muy costosas.

Desde una perspectiva estratégica, un ataque deliberado contra los cables submarinos podría proporcionar una ventaja considerable al oponente. Entre otras muchas lecciones aprendidas de las operaciones navales durante la Primera Guerra Mundial, descubrimos una de las primeras misiones de disrupción de infraestructuras submarinas. Tras la declaración de guerra en agosto de 1914, el cablero británico HMTS *Alert* fue destacado para cortar los cables submarinos alemanes en el canal de la Mancha, restringiendo de forma notable las comunicaciones telegráficas desde y hacia Alemania (4). A lo largo de la guerra, los alemanes también dedicaron esfuerzos significativos y una considerable inventiva al corte de cables, la mayoría realizados desde U-boats (5). Inicialmente, estos ataques se centraron en los que conectaban Gran Bretaña y Francia a través del Báltico con Rusia. Y cuando los otomanos entraron en la guerra, algunos de los cables del mar Negro también fueron cortados.

También hubo casos de cortes de cables en aguas controladas por el enemigo en la Segunda Guerra Mundial. Así, en 1940 Italia realizó algunos sabotajes en el Mediterráneo, principalmente entre Malta y Gibraltar (6), y estas operaciones fueron esenciales en el teatro del Pacífico. La literatura de uno de los períodos más retratados de la historia nos deja numerosas anécdotas sobre la unidad especial de los Marines de los Estados Unidos, conocida como «Hombres Rana», que realizaron diversas misiones de sabotaje submarino para cortar cables japoneses en un intento de aislar a las fuerzas niponas y obstaculizar su comunicación estratégica para contribuir a la superioridad aliada.

Posteriormente, durante la Guerra Fría, Estados Unidos y la URSS llevaron a cabo operaciones encubiertas para monitorizar y, en algunos casos, intentar interrumpir cables cruciales para la comunicación y el mando y control del

---

(3) Informe Annual sobre industria Offshore, Kingfisher. Annual Report 2022. «Offshore Renewable and Cable Awareness». Talking Points. Kingfisher Information Service, enero de 2022. Disponible en: *https://www.seafish.org/document/?id=60baf5ab-995e-4f0f-bb08-3617ca2c3a6f*

(4) «The security of subsea cables: an enduring naval challenge». *Maritime Foundation*, diciembre de 2022, en *https://www.maritimefoundation.uk/publications/maritime-2023/the-security-of-subsea-cables-an-enduring-naval-challenge/*

(5) KLEIN, Christopher: «How German U-Boats Were Used in WWI. And Perfected in WWII». *History,* 21 de marzo de 2022, en *en https://www.history.com/news/u-boats-world-war-i-germany*

(6) GLOVER, Bill: «History of the Atlantic Cable & Undersea Communications. The Evolution of Cable & Wireless», 2012, en *https://atlantic-cable.com/*

adversario. Así, submarinos nucleares de ambas naciones se desplegaron en misiones secretas para instalar dispositivos de escucha y rastreo en dichos cables. Estas operaciones eran parte de la intensa rivalidad entre las superpotencias enfrentadas en materia de inteligencia estratégica y, en particular, en misiones más propias de guerra electrónica. En la década de los 70, se puso en marcha la Ivy Bells, una operación encubierta llevada a cabo por los Estados Unidos y el Reino Unido durante la Guerra Fría que tenía como objetivo principal la instalación de dispositivos de escucha en cables submarinos soviéticos en el mar de Ojotsk, una región estratégica para la Unión Soviética que le otorga salida al Pacífico. La interceptación de las comunicaciones submarinas soviéticas (7) era empleada para la obtención de inteligencia mediante una técnica que se conoce como *submarine snooping,* o espionaje submarino, y que implica la adquisición de información al interceptar las señales de los cables en el lecho marino. Como parte del espionaje gubernamental extranjero se podría, llegado el caso, comprometer la infraestructura y la seguridad de datos, pues el 99 por 100 de los datos internacionales son transportados bajo el agua (8).

Estos ejemplos sirven para arrojar luz sobre algunas de las operaciones militares en el lecho marino que tuvieron como objetivo obstaculizar las comunicaciones enemigas y desorganizar las infraestructuras militares del adversario. Operaciones históricas a la orden del día, pues el corte de cables submarinos utilizados para la transmisión de datos y comunicaciones afectaría a la capacidad para coordinar y responder ante una amenaza y menoscabaría el funcionamiento de las infraestructuras civiles.

Incidentes de actualidad contra gasoductos

En relación con los gasoductos, caben destacar como incidente de actualidad las explosiones del Nord Stream —el «famoso» gasoducto que conecta Alemania con Rusia— en septiembre de 2022, que se producían en un contexto de nuevas sanciones a Rusia por parte de la UE y que causaron daños severos sobre esta infraestructura.

Numerosas agencias de inteligencia y organizaciones de seguridad han clasificado el suceso como un acto deliberado de sabotaje. Sin embargo, la dificultad para definir su autoría —y el alcance de la propaganda sobre el sabotaje— ha

---

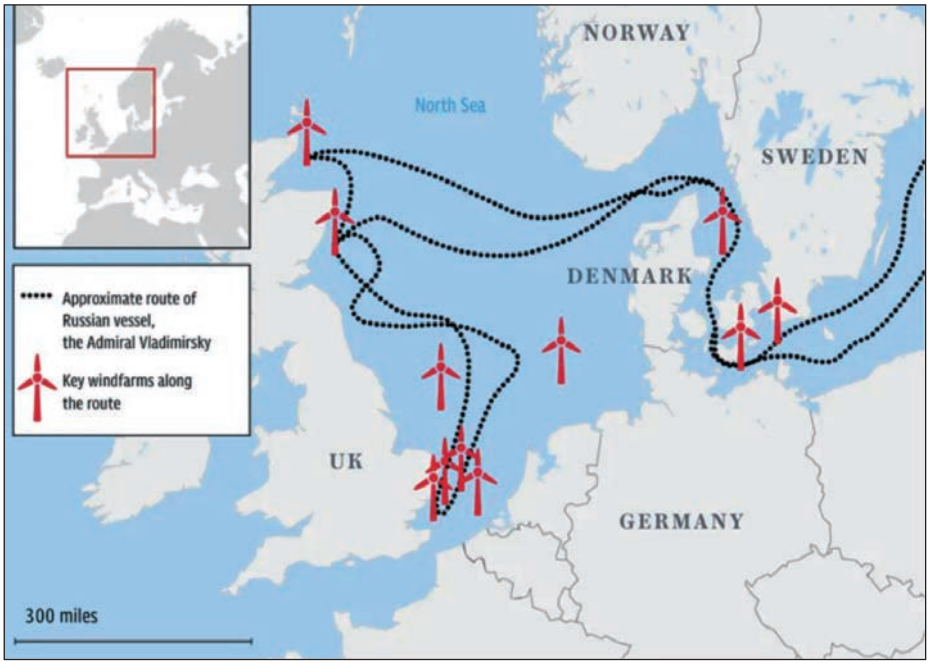
(7) WENDORF, M.: «Operation Ivy Bells: The US Top-Secret Program That Wiretapped a Soviet Undersea Cable». *Interesting Engineering*, 3 enero 2022, en *https://interestingengineering.com/innovation/operation-ivy-bells-the-us-top-secret-program-that-wiretapped-a-soviet-undersea-cable*

(8) MAIN, D.: «Undersea Cables Transport 99 Percent of International Data». *Newsweek*, 2 de abril de 2015, en *https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072*

derivado en la aparición de diversas teorías sobre los posibles autores, que abarcan desde acusaciones hacia Rusia y a Estados Unidos o incluso a un grupo proucraniano. Sin embargo, todas ellas han sido negadas enérgicamente por los respectivos gobiernos.

Sin entrar a valorar la autoría del sabotaje al gasoducto Nord Stream, es innegable que ha aumentado la preocupación en Occidente sobre la vulnerabilidad de las infraestructuras críticas en el lecho marino. Como respuesta, tanto la OTAN como la UE se encuentran en pleno proceso de decisión para implementar planes que mitiguen los riesgos y mejoren la resiliencia de la infraestructura sumergida, especialmente importante en el mar del Norte, dado su papel estratégico para el suministro de energía a Europa y su rol en la transición a fuentes de energía más sostenibles.

El incidente en el mar Báltico puso de manifiesto un desafío que se está volviendo cada vez más global en una era de competencia estratégica, en la que predominan las denominadas «guerras híbridas» o las agresiones en la «zona gris», pues la tecnología presenta herramientas capaces de causar daños similares a los ataques convencionales, pero sin ninguna de sus consecuencias, dada la dificultad de adjudicar las autorías. Y estas acciones en la «zona gris» afectan



Ruta seguida por el buque AGOR *Admiral Vladimirsky* de la Marina de la Federación Rusa. (Fuente: *theconversation.com*)

también a las infraestructuras críticas posadas sobre el fondo marino, por lo que convierten al lecho submarino en un dominio de la guerra moderna.

En este contexto, los países nórdicos parecen liderar los avances tecnológicos y las medidas de mitigación de riesgo y han manifestado públicamente su creciente preocupación por las operaciones realizadas por buques de investigación rusos tipo *Akadémik*, detectados operando en su ZEE en lo que parece el patrón de una campaña hidrográfica para cartografiar infraestructuras sumergidas. Información de gran valor que podría nutrir a la inteligencia estratégica del enemigo tradicional y ser empleada para realizar ataques en el futuro.

En el documental *Shadow War* (9), producido por un consorcio de emisoras públicas de Suecia, Dinamarca, Finlandia y Noruega, se manifiesta la presente amenaza significativa para la infraestructura marítima y subacuática en el mar del Norte y la región del Báltico, y se sugiere que el buque de investigación oceanográfica ruso *Admiral Vladimirsky* está recopilando datos sobre los parques eólicos, gasoductos y cables de energía e internet en el mar del Norte. Además, se afirma que distintos buques rusos realizan sistemáticamente operaciones de mapeo para identificar las vulnerabilidades de la infraestructura sumergida, lo que podría facilitar ataques de sabotaje.

Asimismo, el pasado mes de octubre el gasoducto Balticconnector, que atraviesa el golfo de Finlandia, fue presuntamente dañado por una de las anclas del carguero chino *Newnew Polar Bear*. Este buque fue señalado públicamente como el principal sospechoso, aludiendo a los informes de la Oficina Nacional de Investigación de Finlandia, que indicaban que el carguero recorrió hasta 100 millas náuticas arrastrando una de sus anclas. Si bien el incidente todavía sigue indagándose, los daños fueron cuantiosos y entrañaron una reparación altamente onerosa. Además, este perjuicio reciente a la infraestructura submarina entre Finlandia y Estonia se enmarca nuevamente en la «zona gris» y, aunque se sospecha que fue intencionado, aún no se ha confirmado la atribución ni si hubo premeditación.

Gasoducto Balticconnector. (Fuente: Portal Morski)

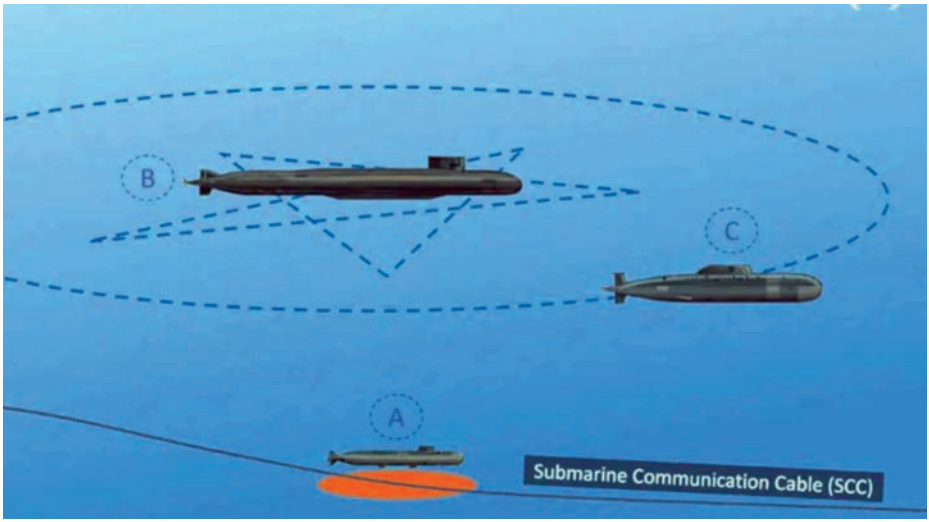
(9) «Ghost ships and espionage: Russia's huge surveillance efforts laid bare in new Nordic documentary». *Euronews*, 19 de abril de 2023, en *https://www.youtube.com/watch?v=3QFW3kLDo_M*

Riesgo actual contra la infraestructura submarina

Mientras que el daño físico accidental sigue siendo una preocupación común, las acciones deliberadas representan un riesgo todavía más siniestro. Tras los incidentes de los gasoductos Nord Stream y el Balticconnector, el interés por los cables submarinos transatlánticos ha aumentado, y las marinas ya utilizan submarinos y buques de superficie equipados con sumergibles autónomos o tripulados para explotar este nuevo entorno.

Así, desde una perspectiva estratégica, el sabotaje de las infraestructuras críticas emerge como un nuevo y creciente vector de amenaza, que añade una capa adicional de riesgo, en un panorama de especial tensión internacional. Un ataque contra las principales arterias de la red de telecomunicaciones derivaría en una pérdida de control sobre sectores estratégicos, por lo que se ha convertido en una amenaza para los Estados. De la misma manera, el sabotaje de un gasoducto restringe las capacidades de abastecimiento energético, con grandes consecuencias económicas. Por ello, no es descartable la explotación de estas infraestructuras con operaciones de espionaje o sabotaje, dado que podrían cumplir con diversos objetivos militares, como interrumpir las comunicaciones oficiales, controlar el acceso a internet, debilitar la economía del adversario o causar tensiones geopolíticas que fuercen una decisión de alto nivel.

Además, dada la cantidad de datos que circulan a través de los cables sumergidos, acciones empleadas durante la Guerra Fría tales como el *submarine snooping* —que implica el espionaje directo de información al interceptar cables— plantean

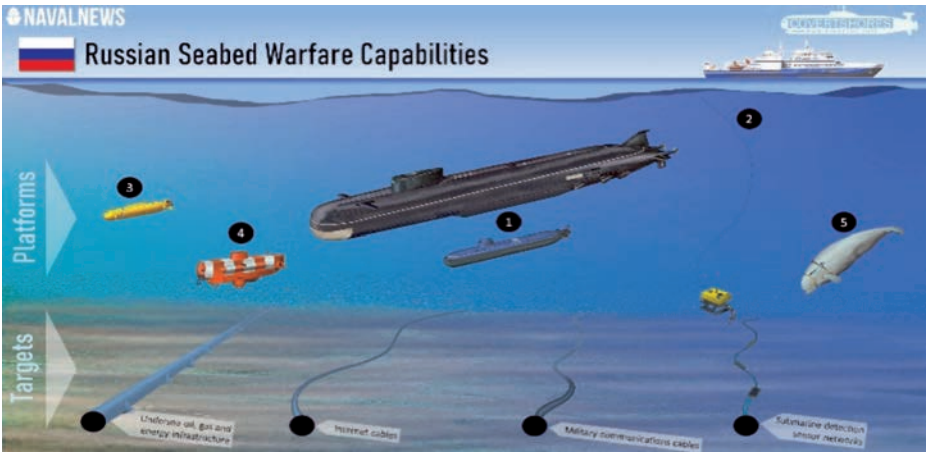


Operación general de minisubmarinos. (Fuente: SUTTON, H. I.)

serias inquietudes. En el artículo «5 Ways The Russian Navy Could Target Undersea Internet Cables» (10), se resume de forma muy esquemática cómo la Marina rusa emplea diversas tácticas para interceptar las señales transmitidas mediante cables submarinos. Primordialmente, submarinos especialmente modificados, como la clase *Delta* y el *Belgorod,* permiten transportar minisubmarinos de buceo profundo y propulsión nuclear.

Éstos son después desplegados, con capacidad para sumergirse hasta los 1.000 metros y trabajar en un área concreta del lecho marino durante varios días, proporcionando la capacidad de llevar a cabo operaciones discretas, con alcance global. Además, se pueden incluso realizar en las áreas bajo la capa de hielo, donde los barcos convencionales no pueden operar, lo que nos hace pensar en su potencial empleo en el Ártico como uno de los posibles escenarios de competencia geoestratégica en el futuro próximo.

Además, Rusia utiliza buques de investigación oceanográfica, como el AGOR (11) *Yantar*, sospechoso de desplegar vehículos operados de forma remota (ROV) y sumergibles tripulados. Este tipo de unidades pueden emplearse como plataformas para el despliegue de diversos medios, capaces de explotar todos los vectores de la guerra en el lecho marino en misiones con un gran abanico de posibilidades, que engloban desde el reconocimiento y recopilación de inteligencia hasta el despliegue de dispositivos de escucha o explosivos.



Capacidades *seabed warfare* rusas. (Fuente: *Naval News*)

(10) Sutton, H. I.: «5 Ways The Russian Navy Could Target Undersea Internet Cables». *Naval News*, 7 de abril de 2021, en https://www.navalnews.com/naval-news/2021/04/5-ways-the-russian-navy-could-target-undersea-internet-cables/

(11) *Auxiliary General Purpose Oceanographic Research*.

Por otro lado, las fuerzas navales rusas también utilizan vehículos submarinos autónomos (AUV), como el *Klavesin 2P-PM*, que pueden sumergirse hasta una cota de 6.000 m y realizar inspecciones submarinas o tareas de recopilación de inteligencia acústica y electromagnética (12). Estas tácticas demuestran la sofisticación de las operaciones rusas bajo la superficie y los esfuerzos destinados al constante desarrollo tecnológico para mantener la capacidad de comprometer la seguridad de los cables submarinos críticos en caso necesario.

Principales estrategias y capacidades de protección

A pesar de que existen discrepancias en cuanto a la definición del concepto de *seabed warfare* o guerra en el lecho marino, este nuevo dominio se está convirtiendo en una de las mayores áreas de investigación para las principales marinas, así como en un campo de exploración vanguardista y de I+D para múltiples empresas de telecomunicaciones.

En un informe al Congreso norteamericano en 2016 sobre la necesidad de dotar a la US Navy de nuevos sistemas no tripulados, el por entonces jefe de Operaciones de la Undersea Warfare Directorate remarcaba las misiones submarinas actuales y hasta el horizonte 2025, haciendo especial hincapié en la *seabed warfare* como una misión naciente que requeriría nuevos medios para mantener la superioridad estratégica. Conviene reseñar que el informe arrojaba luz sobre el hecho de que «las capacidades del adversario [en el lecho marino] ostentan unos riesgos inaceptables para otros dominios de la guerra» (13), y por ello buscaba evidenciar la necesidad de desarrollar y dotar a la Marina norteamericana de nuevos medios para alcanzar la superioridad bajo la superficie.

Posteriormente, en 2018, un trabajo del US Naval Postgraduate School (14) ya señalaba que el nuevo ámbito de la guerra alberga el gran problema de «desarrollar un concepto de operaciones para explotar la guerra en el lecho marino, tanto en entornos ofensivos como defensivos», sin exponer activos de gran valor ante un riesgo innecesario.

Desde 2020, los principales esfuerzos norteamericanos parecen centrarse en el desarrollo de un vehículo submarino no tripulado de gran desplazamiento (LDUUV) (15), como el *Snakehead*, que proporcionará capacidades de inteligencia

---

(12) «Russia Started Sea Trials of Klavesin-2 UUV in Crimea». *Naval Technology*, 18 de mayo de 2018, en *https://www.navyrecognition.com/index.php/focus-analysis/naval-technology/6234-russia-started-sea-trials-of-klavesin-2-uuv-in-crimea.html*

(13) Chief of Naval Operations Undersea Warfare Directorate: *Autonomous Undersea Vehicle Requirement for 2025*. Washington DC, 18 de febrero de 2016.

(14) CARR, C. J.; FRANCO, J.; MIERZWA, C.; SHATTUCK IV L. B.; SUURSOO, M. A.: *Seabed warfare and the XLUUV*. Naval Postgraduate School, junio de 2018.

(15) *Large Displacement Unmanned Underwater Vehicle*.

LDUUV *Snakehead*. (Fuente: *Naval News*)

y preparación del entorno (IPOE) y de vigilancia y reconocimiento (ISR), pudiendo ser desplegado desde buques de superficie o submarinos.

Por su parte, la Royal Navy, en medio de las crecientes preocupaciones sobre el aumento del riesgo a las infraestructuras en el lecho marino, ha incorporado un nuevo patrullero oceánico versátil, el MROS *Proteus* (16). Este buque ha sido militarizado a partir de una antigua unidad de apoyo a las actividades en plataformas petrolíferas y ya se encuentra en servicio y dedicado a la protección de infraestructuras críticas. Dispone de capacidades para ejercer la vigilancia de los fondos marinos y el despliegue de distintos equipos submarinos (17).

Asimismo, en el marco de la Fuerza Expedicionaria Conjunta (JEF) se han desplegado diversas unidades, lideradas por la Royal Navy, en una operación de respuesta diseñada para «disuadir y defender nuestra región de amenazas y

(16) *Multi-Role Ocean Surveillance*.

(17) «RFA *Proteus* (K60)». Royal Navy, *https://www.royalnavy.mod.uk/organisation/units-and-squadrons/support-ships/rfa-proteus*

establecer cómo podemos responder rápidamente a crisis» (18). Esta agrupación fue creada en la cumbre de la OTAN de Gales en 2014 y es liderada por el Reino Unido. Actualmente, incluye la participación de ocho naciones asociadas: Dinamarca, Estonia, Finlandia, Letonia, Lituania, Países Bajos, Noruega y Suecia. En diciembre de 2023, la JEF desplegó en el mar Báltico en una operación de respuesta tras el incidente del Balticconnector (19).

En febrero de 2022, Francia promulgó su *Estrategia de guerra en el lecho marino*, señalando la *seabed warfare* como uno de los diez objetivos estratégicos para 2030 (20). Con esta publicación, Francia se adapta a la evolución del concepto y define el lecho marino como un nuevo dominio de la guerra, similar al del ciberespacio y al del espacio exterior. Además, a lo largo del documento refiere cómo salvaguardar la capacidad de las infraestructuras francesas para asegurar la libertad de acción en un entorno cada vez más disputado y dividido entre «competición y confrontación». Bajo la premisa de que este nuevo entorno requerirá el desarrollo del conocimiento del lecho marino, su monitorización y la aplicación de medidas de control, la *Estrategia* incluye un plan de acción para integrar la *seabed warfare* en el seno de la estrategia de defensa francesa en su conjunto.

A nivel OTAN, en febrero de 2023 su secretario general anunció la creación de una Célula de Coordinación de Infraestructuras Submarinas Críticas, con el fin de coordinar —junto con los líderes del sector de las infraestructuras de energía y comunicaciones— la contribución de la OTAN a la seguridad de las infraestructuras submarinas críticas e incrementar la cooperación con la industria.

De la misma manera, la Marina italiana está trabajando en un nuevo concepto de operaciones navales en el lecho marino. No obstante, parece que pretende integrar la *seabed warfare* en la Fuerza de Medidas Contraminas (MCM), estructura que, en palabras del comandante de las Fuerzas de Contramedidas de Minas (MARICODRAG), lleva décadas dedicada a la protección de las infraestructuras críticas y ya se encarga de la vigilancia y protección de las infraestructuras submarinas nacionales, con plataformas y sistemas tripulados y no tripulados (21).

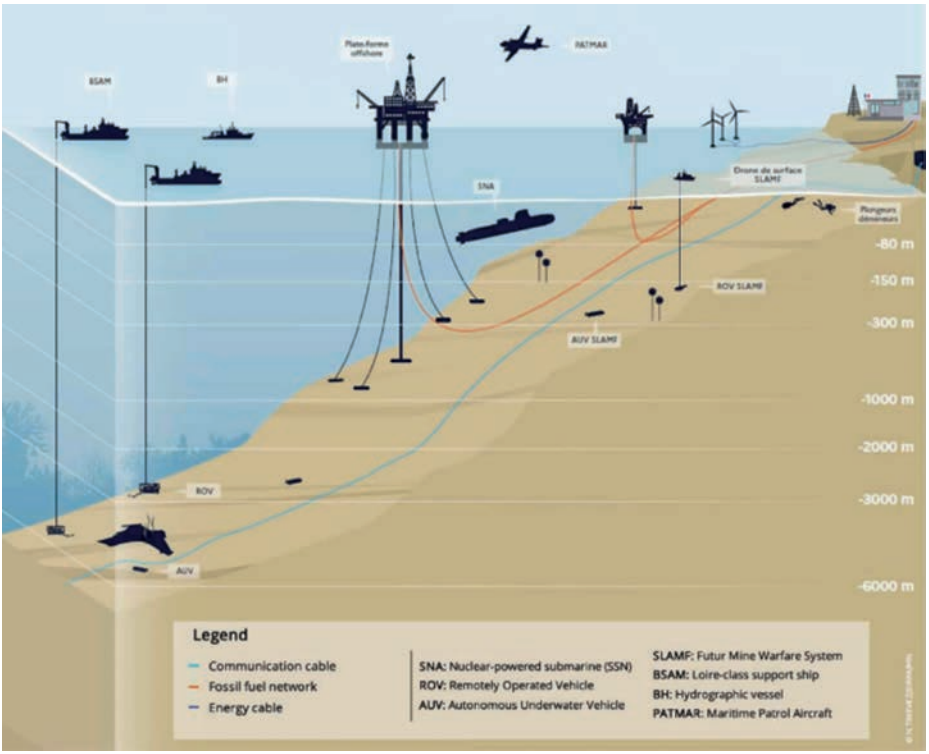
---

(18) «*Joint statement by Joint Expeditionary Force ministers*». Ministerio de Defensa del Reino Unido, en *https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-november-2023*

(19) KAURANEN, A.: «UK, Finland, Estonia practise subsea infrastructure protection in Baltic Sea». *Reuters*, 4 de diciembre de 2023, en *https://www.reuters.com/world/europe/uk-finland-estonia-practise-subsea-infrastructure-protection-baltic-sea-2023-12-04/*

(20) «Seabed Warfare Strategy». Ministère des Armées, febrero 2022, en *https://www.defense.gouv.fr/sites/default/files/ministere-armees/Maitrise%20des%20fonds%20marins%20-%20Seabed%20warfare.pdf*

(21) PERUZZI, L.: «Seabed warfare, Italian Navy current and future MCM Force capabilities». *European Defence Review*, 27 de junio de 2023, en *https://www.edrmagazine.eu/seabed-warfare-italian-navy-current-and-future-mcm-force-capabilities*



Estrategia marítima francesa sobre la explotación de los fondos marinos.
(Fuente: Marine Nationale)

Conclusiones

Con un uso al alza y convertidos en elementos cardinales de la conectividad internacional, los cables submarinos son infraestructuras críticas que facilitan la globalización. Su importancia no debe ser subestimada, y la protección de estas infraestructuras es esencial, tanto para mantener la seguridad y la fiabilidad de las comunicaciones internacionales como para garantizar el abastecimiento energético, especialmente en caso de conflicto. Sin embargo, la guerra en el lecho marino entraña numerosos retos para los Estados ribereños y la comunidad internacional, especialmente debido a la inmensidad de los océanos, la gran escala de la infraestructura a proteger, la fragilidad de los gasoductos y las muchas oportunidades de ataque que ofrece y que otorgan múltiples ventajas a cualquier posible agresor.

Sin duda, el mayor reto se enmarca entre la dificultad de monitorizar el fondo marino y la disponibilidad de las capacidades de explotación de este

nuevo ámbito de la guerra por parte de cualquier actor, lo que lo hace especialmente vulnerable. Sirva el incidente del carguero chino *Newnew Polar Bear* como una posible acción de sabotaje realizada en la «zona gris», que ejemplariza cómo tan sólo fue necesaria un ancla, arrastrada a lo largo del lecho marino en el mar Báltico, para romper un gasoducto submarino y varios cables de telecomunicaciones que conectaban Estonia y Finlandia. Esto evidencia que, en caso de conflicto, cualquier oponente con pocos recursos tendría el potencial necesario para interrumpir la conectividad del adversario, incluso sin ser detectado.

Los últimos incidentes han puesto de manifiesto que la salvaguardia de los cables y gasoductos submarinos se erige como una prioridad, ya compartida entre gobiernos, empresas de telecomunicaciones y operadores de cables, que demandan una colaboración internacional encaminada a alcanzar el equilibrio aceptable entre el riesgo de ataque y la disposición de los medios necesarios para la defensa de las infraestructuras en un nuevo campo de batalla. Siendo esta cooperación esencial para abordar la seguridad de las infraestructuras críticas, dividiendo esfuerzos y aumentando la sinergia de medios disponibles mientras se procura una gobernanza internacional más sólida, pues actualmente existen ciertas lagunas de seguridad derivadas de la falta de acuerdos internacionales que permitan reforzar la defensa de las infraestructuras críticas en alta mar o que disuadan su sabotaje. Si bien el riesgo inherente es imposible de eliminar, la adopción de medidas preventivas es crucial para garantizar la estabilidad de la conectividad global. Por ello, cada vez se hace más necesario un acuerdo en materia de defensa de las infraestructuras críticas situadas más allá de las aguas jurisdiccionales, parecido al Tratado de Alta Mar (High Seas Treaty) de la ONU firmado en 2023 para la conservación de la biodiversidad marina.

Igualmente, cabe reseñar que los últimos incidentes demuestran la necesidad de desarrollar renovadas estrategias de seguridad marítima, que definan prioridades y planes de acción que incluyan la explotación del lecho marino como nuevo dominio de la guerra ya evolucionada hacia el multidominio. En esta línea, las estrategias publicadas evidencian el rumbo que seguirán las principales marinas del mundo y sirven de guía para aquellos Estados en proceso de implementar sus propios planes y rutas de acción. Así, la definición de las prioridades y el marco de actuación son el pilar sobre el que estudiar el balance preciso entre los medios a disponer y el riesgo remanente asumible, pues la infinidad de potenciales agresores en un área amplísima —que abarca desde el mar territorial a las cuencas marinas transatlánticas, en las que ya pueden operar múltiples vehículos submarinos— hace que el control total de este entorno sea una tarea ardua, por no decir inalcanzable.

Posteriormente, será ineludible definir las estructuras de una renovada fuerza naval, con capacidades para ejercer la vigilancia y, llegado el caso, la defensa de las infraestructuras sumergidas. El inédito despliegue de la JEF en el Báltico durante el pasado mes de diciembre es una clara muestra de que un enfoque militar para la defensa de los lechos marinos es necesario, especialmente

—dada la destacada y creciente relevancia de las infraestructuras críticas sumergidas— en un contexto global dinámico y de creciente tensión geopolítica, que los convierte en objeto de acciones en la «zona gris». Además, la participación en estructuras internacionales permite alcanzar lecciones aprendidas, a la vez que refuerza la sinergia de medios en el seno de alianzas y aumenta la interoperabilidad de plataformas, elementos necesarios para afrontar los grandes retos de esta época.

España, como país ribereño con acceso al océano Atlántico y al mar Mediterráneo, alberga un significativo entramado de cables submarinos que desempeñan un papel vital en la conectividad, tanto a nivel nacional como global. Mientras que a lo largo de la costa norte se establecen las conexiones cruciales con redes submarinas que enlazan puntos estratégicos a ambas orillas del Atlántico, la costa mediterránea es el punto de entrada de materias primas que, a través de gasoductos, suministran un gran porcentaje de los recursos fundamentales para el abastecimiento energético. Por ello, la adopción de tecnologías avanzadas y la implementación de estrategias de protección se convierten en imperativo para preservar la conectividad global y salvaguardar los intereses nacionales.

Desde el punto de vista de la seguridad marítima, uno de los cometidos de los buques en operaciones de vigilancia y seguridad marítima es la defensa de las infraestructuras críticas, que engloban desde planes de respuesta hasta acciones específicas en emplazamientos concretos, o la vigilancia general ante la creciente amenaza de acciones subversivas. Frente a una potencial agresión, la vigilancia y, si fuera necesario, la defensa de los cables submarinos y gasoductos podría ser un factor decisivo y una ventaja —o desventaja— estratégica. Por ello, el futuro parece navegar hacia el diseño de una fuerza naval con capacidad para operar en el lecho marino, dotada de suficientes medios submarinos y sensores que permitan alcanzar el control de una zona determinada del mismo, lo cual requiere tiempo, dinero y adiestramiento.

Nos gustaría concluir reforzando la idea de que el desarrollo del concepto de *seabed warfare* y la adquisición de plataformas dedicadas a la vigilancia de los fondos marinos apuntan hacia una nueva tendencia que posiblemente marcará la dinámica de las principales naciones costeras. Por ello, el concepto de operaciones navales debe evolucionar para incorporar un ámbito en desarrollo y constante evolución. Como nación costera hemos de obtener y desarrollar las capacidades operativas que posibiliten la defensa y, llegado el momento, la explotación de los recursos en los océanos, integrando estos desarrollos tecnológicos en la Armada, muchos de ellos ya disponibles en el ámbito civil. Por ello, a corto plazo, habrá que plantearse la adquisición de vehículos submarinos que, en el futuro próximo, serán un factor decisivo para la explotación del fondo marino y el control del mar en un panorama en que los conflictos tienden hacia el ámbito multidisciplinar y conjunto.

EVALO del *H-135* en el BAM *Meteoro* (P-41).
(Foto: Miguel López Garay)