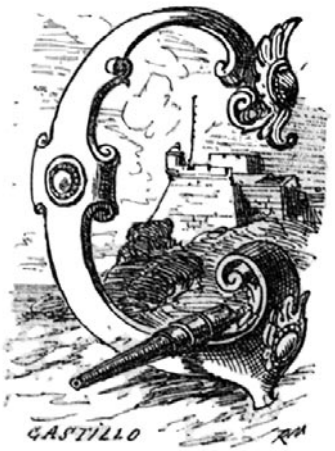
LA VULNERABILIDAD DE LAS INFRAESTRUCTURAS CRÍTICAS SUBMARINAS. CAPACIDADES Y COMETIDOS DERIVADOS DE LA NECESIDAD DE SU PROTECCIÓN

Francisco Javier GAMBOA GIBERT

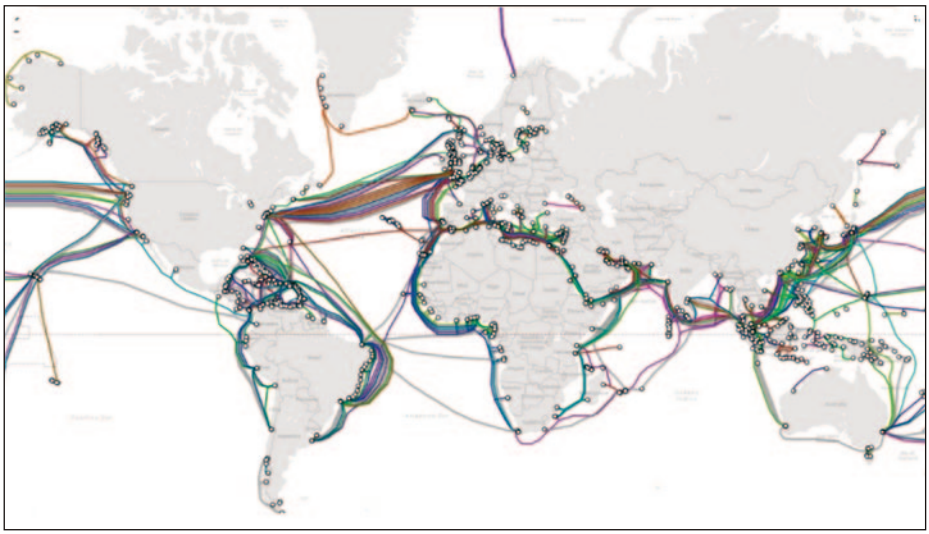


CONCEBIR la mar simplemente como un medio físico para el transporte y el comercio, como un accidente geográfico que actúa de sistema defensivo natural en un área determinada o como un entorno más para la presencia de fuerzas militares es algo que ha pasado a ser ciertamente simplista en el momento de la historia en que nos encontramos. Tres cuartas partes de nuestro planeta son agua, de la que el hombre extrae minerales, energía, alimentos, explota el turismo, a la vez que usa sus fondos marinos como vías de comunicación. Dichos recursos generan una serie de beneficios de interés comercial y posicionan a los Estados en el contexto geopolítico actual. Deténganse un momento a pensar cuál de los anteriores recursos produce mayor impacto en el entorno político-económico mundial que nos envuelve, cuál de todos ellos podría servir como elemento de presión para desestabilizar interesadamente a una importante entidad, a una nación, a una organización internacional, a una gran alianza… Cuál podría ser utilizado para resquebrajar el equilibrio geoestratégico sobre el que se mantiene la paz entre las principales potencias mundiales. Posiblemente —entre esta clasificación de recursos oceánicos— no

escoja los minerales, el turismo o la alimentación (sin duda desequilibrantes) ni tampoco las vías de comunicación. Lo más probable es que, sin llegar a detenerse demasiado en ello, tienda a elegir el ámbito de la energía —gas, petróleo...— que, desde luego, es incuestionable que se trata de uno de los máximos exponentes de proyección de poder internacional.

Sin embargo, el fondo oceánico alberga un recurso igual o aún más valioso: al menos el 99 por 100 del tráfico de voz y de internet viaja a través de una infraestructura submarina (1). Es decir, que la mayor parte de la información que mueve el mundo que nos rodea se hace mediante algo más de 500 líneas de cableado transoceánico (2). Información que, entre otros, deriva en transacciones que suman un total aproximado de 10.000 millones de transferencias financieras cada día.

España tiene alrededor de 8.000 km de costa. El 60 por 100 de las exportaciones y el 85 por 100 de las importaciones se realizan a través de sus puertos comerciales (3), y se recibe al menos el 70 por 100 del total del suministro energético del

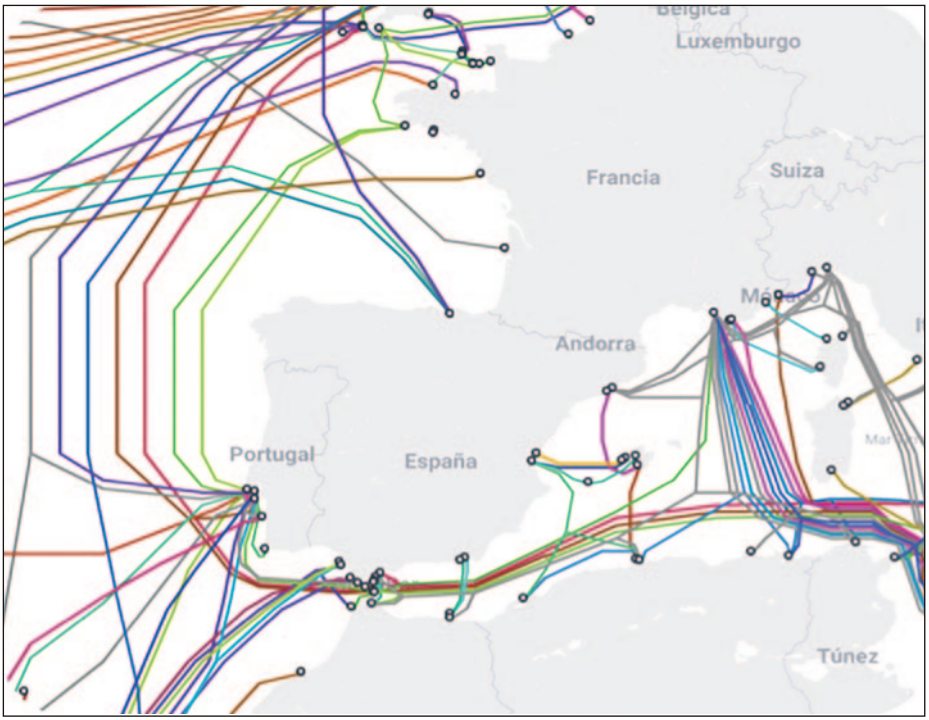


Cableado submarino desplegado a nivel mundial. (Fuente: *TeleGeography*)

(1) BAUMANN, J. (2021): «Publisher of *Subsea Cable News* uses ArcGIS for industry analysis and interactive mapping», *Submarine Telecoms Magazine*, pp. 36–37; NATO Cooperative Cyber Defense Centre of Excellence, en *Strategic importance of, and dependence on, undersea cables*, 2019.

(2) *TeleGeography*, en *https://www2.telegeography.com*

(3) COMTEL, J. (2022): «El mercado español marítimo: puertos, tráficos y terminales». *Canales sectoriales. Transporte marítimo. Puertos,* en *interempresas.net*



Cableado submarino en España. (Fuente: *TeleGeography*)

exterior (4). Pero, por si esto no diera suficiente voz al protagonismo económico de nuestras costas, su situación estratégica la convierte en una región marítima clave en la recepción de cables transoceánicos, que contienen el 94 por 100 del tráfico de internet que entra y sale del país. Dicha ubicación geográfica la sitúa como punto de acceso a conexiones con otros países y, lo que es más importante, con otros continentes. A nuestras costas llegan cables submarinos como Marea, impulsado por Microsoft y Facebook, en Bilbao, y que conecta España con Estados Unidos; Alpal-2 (Baleares-Argelia), Tata TGN-Western Europe (España-Portugal-Reino Unido); ORVAL (Valencia-Argelia); FEA o Flag Europe Asia (Málaga-Reino Unido-Egipto-China-Japón-India…), y otros muchos que hacen de nuestro país un punto de encuentro crucial en el tráfico de datos a nivel mundial.

Como cabe imaginar, la protección de todo este entramado submarino que se sitúa en el fondo de nuestras aguas jurisdiccionales ha pasado a ocupar un

(4) «El sector energético en España», en *es.statista.com*

puesto cada vez más importante dentro del marco general de actuación de nuestras Fuerzas Armadas. La defensa de la infraestructura submarina y la disuasión de cualquiera de sus potenciales amenazas son esenciales para contribuir a la proyección de estabilidad como una de las Líneas de Acción Estratégicas definidas por el *Concepto de Empleo de las Fuerzas Armadas* (CEFAS, 2021), de modo que seamos capaces de dar respuesta a los retos de seguridad a los que se enfrenta nuestro país como Estado soberano y como aliado.

A continuación, se presentan algunos puntos interesantes que permiten comprender, en líneas generales, las dimensiones y características de la infraestructura submarina como elemento crítico en la defensa de los intereses de nuestra nación.

El activo estratégico

Big Data, Internet de las Cosas, 5G… Inmersos en pleno desarrollo de la Revolución Industrial 4.0, la relevancia que adquiere la infraestructura submarina resulta más que evidente cuando se advierte que es, ni más ni menos, la ruta comercial económica que transporta el producto más importante de la era de la información: los datos. Infinidad de datos viajan en el interior del cableado que se halla bajo nuestros océanos. Y a medida que esa demanda de datos continúa creciendo (computación en la nube, implementación de la tecnología 5G…), el volumen de estos datos que viajan a través de la infraestructura submarina crece exponencialmente. Se espera que, a medio plazo, la demanda de ancho de banda se duplique cada dos años (5).

Es fácil, por tanto, deducir que las implicaciones derivadas de la seguridad de esta infraestructura crítica son claras. Quien controla las líneas tiene un poder más que considerable. Dado que los datos se han convertido en un activo estratégico cada vez más importante, los riesgos no son menos considerables según qué circunstancias. El mismo Parlamento Europeo determina en un estudio analítico sobre el tema que la pérdida de comunicaciones durante horas, o incluso apenas minutos, podría tener repercusiones desastrosas en operaciones sensibles que conlleven implicaciones financieras importantes. Sirva como referencia la pérdida absoluta de comunicaciones que sufrió en octubre de 2022 la isla de Shetland (Escocia), que provocó cortes en servicios de telefonía, banda ancha y móviles. El incidente se suma a otro ocurrido una semana antes cuando se dañó el que conectaba las Feroe y las Shetland (6).

---

(5) Kim, J. (2022): «Submarine Cables: the Invisible Fiber Link Enabling the Internet», en *https://dgtlinfra.com/submarine-cables-fiber-link-internet/*

(6) «Damaged cable leaves Shetland cut off from mainland», en *https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102*

Aunque se desconoce si se trató de una cuestión accidental, sumió a la isla en una situación de emergencia.

Todo esto nos lleva a reflexionar acerca de una de las vulnerabilidades más palpables que caracterizan actualmente a la infraestructura submarina: la falta de protección física ante la posibilidad de ataques estructurales al cableado submarino. Sirva como aliciente a los potenciales agresores que el emplazamiento del cableado es público y los medios para llevarlo a cabo no demasiado sofisticados y, por tanto, fácilmente accesibles.

Control de la infraestructura submarina y vulnerabilidades

Habiendo dejado clara la trascendencia que supone poseer cierto control sobre el cableado oceánico que transporta tal ingente cantidad de datos, la pregunta que cabe hacerse es: ¿y quién controla las líneas submarinas? Existen dos modelos de propiedad de este tipo de infraestructura:

— Consorcio: múltiples propietarios, como empresas de telecomunicaciones, proveedores de servicios en la nube y empresas de servicio *over the top* (servicios de vídeo como HBO o Netflix, mensajería instantánea como WhatsApp o llamadas a través de internet como Skype).
— Privado: propietarios privados, como Amazon, Microsoft, Meta o Google, cuya necesidad de abundante ancho de banda, escasez de latencia o gran redundancia de servicios les empuja a ser, cada vez más, fuertes inversores en el tendido de cableado submarino.

Los dueños de cables son mayoritariamente compañías privadas en connivencia con los gobiernos de las primeras potencias mundiales mediante consorcios que fabrican y despliegan estas infraestructuras (7). No obstante, aproximadamente el 59 por 100 (en diciembre de 2020) de los cables submarinos globales desplegados sólo tienen propietarios privados. Y únicamente el 19 por 100 del total desplegados en todo el mundo son enteramente propiedad de entidades controladas por el Estado, es decir, propiedad directa de un gobierno o a través de una subsidiaria (estudio realizado en el año 2021 por el instituto de investigación Atlantic Council) (8). Véase pues el importante peso que adquiere el sector privado mundial en el entorno digital, influencia que tiene su impacto

(7) GALÁN, J. J. (2021): «Los riesgos (y el valor estratégico) de los cables submarinos», en *https://cincodias.elpais.com/cincodias/2021/10/11/opinion/1633954196_539682.html*

(8) SHERMAN, J. (2021). «Cyber defense across the ocean floor: The geopolitics of submarine cable security». *Atlantic Council Report*, en *https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/*

no sólo en las reglas digitales de internet, sino también en su forma física cambiante.

Analizándolo desde la perspectiva de la seguridad de la infraestructura submarina, merece también la pena detenerse a examinar el grado de influencia que pueden adquirir los actores estatales como partícipes en la construcción o copropiedad del cableado. Desde un punto de vista geoestratégico, que los gobiernos participen en el tendido de la infraestructura submarina o que sean copropietarios de la misma afecta de modo muy similar:

— Si un Estado participa en la construcción de la infraestructura, se da la posibilidad de que, previamente a la instalación, provea al cableado de equipamiento que pueda servir posteriormente de «puerta trasera» para la obtención del flujo de datos que atraviesan el cable.
— ¿Y si son copropietarios? Con la misma idea de obtener información, los Estados «intervienen» en el flujo de datos del interior del cableado que financian.

Esto es, las vulnerabilidades de la infraestructura submarina no se limitan sólo a ataques convencionales dirigidos a dañar físicamente los medios que conforman el sistema de cableado, sino que se debe contemplar en igual medida la posibilidad de que la información que viaja en el cable sea interceptada, vigilada o incluso interrumpida. En este sentido, es interesante subrayar la alta probabilidad de que este segundo tipo de ataques sea realizado más por actores estatales o *proxies* —dada la complejidad técnica y el alto coste que conllevan— que por organizaciones criminales, habida cuenta de las capacidades y medios con los que habitualmente cuentan. Además, desde un punto de vista práctico, las estaciones en tierra y las que conectan los cables con las redes terrestres son objetivos más accesibles y vulnerables para operaciones de espionaje e inteligencia (9).

Se puede concluir, por tanto, con vistas a establecer un proyecto de vigilancia marítima sólido y eficaz para la protección de todas las citadas vulnerabilidades, que las iniciativas público-privadas, las alianzas estratégicas entre las naciones y las empresas de telecomunicaciones son determinantes para establecer escenarios de colaboración en medio de los intereses económicos y políticos que están en juego. De hecho, tal y como se define en el CEFAS 2021, la capacidad de colaboración de nuestras Fuerzas Armadas debe incluir una perspectiva cívico-militar, es decir, para con el resto de instituciones del Estado y entidades

(9) BUEGER, C.; LIEBETRAU, T.; FRANKEN, J. (2022): «Security threats to undersea communications cables and infrastructure. Consequences for the EU». Policy Department for External Relations. *European Parliament*, en *https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf*

de la sociedad civil; en definitiva, todos aquéllos que intervengan de uno u otro modo en el proceso de vigilar y dar seguridad a la infraestructura submarina. A continuación, se sintetizan en cuatro puntos los aspectos más destacados de lo anteriormente expuesto:

1. La información es poder. El control sobre las líneas de tráfico de información submarinas es un activo clave para la seguridad y la defensa de los intereses de la nación, así como para las organizaciones internacionales, los acuerdos y las alianzas a las que se adhiere.
2. La vulnerabilidad de los cables. Se contemplan dos formas que supondrían un enfrentamiento directo a nuestros intereses: el ataque físico a la infraestructura y el espionaje del contenido que atraviesa el cableado.
3. El posible papel de los actores estatales. Muchas veces, mediante el empleo de estrategias híbridas desarrolladas en la zona gris, justo al límite de nuestro umbral de respuesta convencional; es decir, adquiriendo parte de la propiedad del cableado subacuático y obteniendo acceso a la información que la atraviesa.
4. El peso del sector privado. La propiedad del cableado, tanto en el tendido como en la gestión de la información que lo atraviesa, depende en un alto grado de entidades privadas. Entre ellas, algunas que se destacan como las de mayor poder de influencia social y económica a nivel mundial (Google, Amazon, Meta, Microsoft…). Su papel dentro de cualquier proyecto de seguridad en torno a la infraestructura que se encuentra bajo las aguas de nuestra jurisdicción ha de considerarse crucial.

Rusia como protagonista y las posibles acciones para contrarrestar una amenaza potencial

Desde un punto de vista de la evolución y el desarrollo de los medios y capacidades de reconocimiento submarino, podría decirse que la Marina de la Federación Rusa (RFN) ha dado ya numerosos indicios que sitúan a Rusia entre los países en vanguardia. Desde hace varias décadas, la Marina rusa ha trabajado en programas científicos gubernamentales con el objetivo de desarrollar sistemas capaces de vigilar y manipular todo tipo de instalaciones submarinas.

Por tanto, es evidente que las capacidades de la RFN para realizar operaciones sobre el cableado subacuático, sus nodos de comunicación, gasoductos… pueden suponer, si no lo son ya, una amenaza evidente para la consecución de los objetivos estratégicos y operacionales de la OTAN y de España. El almirante Stavridis de la US Navy, ex-SACEUR (Supreme Allied Commander Europe), ya lo advertía hace unos años: «En el caso de tensiones elevadas, el acceso al sistema de cable submarino representa un rico tesoro de inteligencia, una posible

interrupción importante para la economía del enemigo y un golpe simbólico en el pecho para la Marina rusa» (10).

Esto es, sin duda, de incuestionable interés a la hora de dirigir adecuadamente los recursos y capacidades de los que dispone el Estado para acometer de manera eficaz los objetivos que se propone en el ámbito de la vigilancia y seguridad marítima, ya que afecta directamente a la capacidad de respuesta en caso de crisis o conflicto.

La vigilancia, el seguimiento y la disuasión destinadas a la protección de la infraestructura surgen pues como acciones esenciales para neutralizar esta amenaza; una vigilancia especialmente dedicada a las actividades potenciales de la RFN o de cualquier tipo de plataforma que pueda tener relación con actividades sospechosas de acometer daños físicos contra la infraestructura o de realizar espionaje. Este espionaje a menudo se oculta bajo supuestas misiones de carácter científico, detectables por detener sus plataformas o navegar lentamente sobre un cable o con rumbos próximos al del cableado (por lo general, poco lógicos), síntomas que pueden formar parte de las *Indications and Warnings* propias de estas actividades. Dicha vigilancia se iniciaría mediante la presencia naval en el área de operaciones marítimas que se sitúa frente a las zonas costeras de mayor tráfico de red (Bilbao, Málaga, Valencia…). Además, esta nueva perspectiva habría de verse consecuentemente reflejada como un apartado añadido al adiestramiento de nuestros buques, de modo que las dotaciones de nuestras unidades se adapten eficazmente a esta área de creciente interés.

De la mano de dichas actividades, son también interesantes otras acciones que pueden influir positivamente a la hora de hacer frente a estos cometidos:

— Fluidez en las relaciones cívico-militares, es decir, del Estado para con las principales entidades comerciales que tengan una relación directa con el contenedor (la parte física de la infraestructura) o con el contenido (que atraviesa tal infraestructura). La buena relación con tales sociedades podría llegar a proporcionar grandes ventajas; por ejemplo, apoyándonos en el uso de la información o de los sistemas que tales entidades civiles posean como medios de gestión y protección de sus activos (físicos o digitales), siempre con el objeto de proporcionar seguridad a las empresas que arriban a nuestras costas y, por ende, forman parte activa de los intereses de la nación.
— Establecer áreas de especial interés en torno a los puntos clave del tráfico de red submarina en España, de modo que sirvan como punto de partida en el proceso de dar mayor visibilidad a la importancia que adquieren en el mundo actual. Esto podría incluso llegar a abrir la puerta

(10) STAVRIDIS, J. (2016): «A New Cold War Deep Under the Sea?». The Huffington Post, en *https://www.huffpost.com/entry/new-cold-war-under-the-sea_b_8402020*

a generar un marco regulatorio específico a nivel nacional que asiente las bases necesarias para proporcionarles la seguridad específica que merecen. Cabe reseñar que, desde un punto de vista legislativo, y en base a lo establecido por el Convenio de las Naciones Unidas sobre el Derecho del Mar, los países tienen jurisdicción total sobre el cableado tan sólo dentro de sus aguas territoriales, es decir, 12 millas náuticas. Tal y como el mismo Parlamento Europeo manifiesta, el estado legal de los cables y los derechos y la responsabilidad de su protección, tanto en zonas de alta mar como en las zonas económicas exclusivas (200 MN), son ambiguos (11).

Conclusión

El devenir de la industria y el comercio mundial está supeditado a la gestión de una ingente cantidad de datos que, como se ha visto, en el 94 por 100 de los casos para España acceden a nuestro país vía infraestructura submarina. Por ende, la evolución del concepto de vigilancia y seguridad marítima ha de readaptarse consecuentemente a la protección de la información que atraviesa nuestras fronteras y que forma parte esencial de los intereses de nuestra nación. Esto implica definir medios dedicados a tales actividades para la disuasión de actores estatales amenazantes (como puedan serlo China o Rusia) u otros agresores potenciales.

BIBLIOGRAFÍA

AJEMA: *Líneas Generales de la Armada*, 2022.
Estado Mayor de la Defensa: *Concepto de Empleo de las Fuerzas Armadas, 2021*.
Submarine Telecoms Industry Report, 2022/2023, en *https://subtelforum.com/industry-report/*
Cano, J. (director *Revista SISTEMAS, Asociación Colombiana de Ingenieros de Sistemas*-ACIS): «Cables submarinos: ¿Infraestructura crítica no atendida?», en *es.linkedin.com*
Arellano, I.: «El sistema de gobernanza en el marco regulatorio de la red global de cables submarinos de fibra óptica», en *http://www.dspace.uce.edu.ec/bitstream/25000/26683/1/FJCES-CD-ARELLANO%20ISABEL.pdf*
https://radar.cloudflare.com/security-and-attacks/es
https://www.submarinecablemap.com/
https://www.adslzone.net/reportajes/internet/mapa-cables-submarinos/
https://www.bbc.com/mundo/noticias-internacional-60039852

(11) Bueger, C.; Liebetrau, T.; Franken, J. (2022): *op. cit*.

Amanecer en la isla de Alborán.
(Foto: Íñigo Franco Moreu)