Fuente:
ComputerWorld

En un contexto de transformación digital acelerada, los cables submarinos han revalorizado su condición de infraestructura crítica. Garantizar su integridad, física y cibernética, supone un reto mayúsculo.

Entre el 95 y el 99% del tráfico de datos mundial viaja a través de cables submarinos. Una extensa red de más de 1,3 millones de kilómetros, que viaja a través de los mares y océanos, de orilla a orilla. Hay 650 de estas infraestructuras —en funcionamiento o en previsión de hacerlo, según datos de TeleGeography—, que están operadas, fundamentalmente, por compañías privadas. Que podamos conectarnos a internet, tener una copia de seguridad de nuestros archivos del ordenador, realizar una operación bancaria con el móvil o comunicarnos con otras personas depende en gran medida de que nada les pase a los cables submarinos que cruzan el mundo de una costa a otra.

En los últimos tiempos numerosos incidentes, donde la rotura de un cable deja a un territorio sin conectividad, son la prueba de que pese a su carácter crítico, no siempre están correctamente protegidas: solo en el mar Báltico, entre 2022 y julio de 2025 se contabilizaron diez casos de rotura de cables submarinos, siete entre noviembre de 2024 y enero de 2025. En la mayoría de estos incidentes, además, se sospechó que detrás había intereses gubernamentales, con implicación de China o Rusia. En un contexto geopolítico complicado, este tipo de sucesos, en los que se mantiene cierta duda sobre si son accidentales o intencionales, ponen el foco en la necesidad de garantizar la protección. Tanto a nivel físico como de ciberseguridad.

El think tank estadounidense Atlantic Council detecta varias tendencias que amenazan la seguridad de los cables submarinos. Por un lado, enlazando con el tema geoestratégico, la presencia de gobiernos autoritarios en el diseño físico de internet, que ejercen su influencia a través de distintas compañías con varios objetivos, como enrutar los datos de forma favorable a sus intereses, interrumpir la prestación de servicios o aprovechar las infraestructuras para el espionaje. Además, el desplazamiento de los centros de gestión de red desde localizaciones próximas a los puntos de entrada de los cables hasta otras situadas a distancia incorpora nuevos niveles de riesgo. Esto es, al incorporar una capa de control virtualizada, se expande la superficie de ataque a la acción de potenciales agentes maliciosos. Por último, con el auge de tecnologías como la computación en la nube, el 5G o el IoT se ha incrementado el volumen de datos que se transmiten por estos cables, pero también su sensibilidad, ya que cada vez más sectores dependen para su desempeño de estas

herramientas. De nuevo, factores añadidos por los que revisar las políticas de ciberprotección y seguridad de estas infraestructuras críticas. De hecho, desde la Unión Europea se está tomando medidas, con un Plan de Acción de Seguridad del Cable publicado en febrero de 2025 que alude no solo a los desafíos físicos, sino también a la necesidad de ciberprotección. Pero estando la gran mayoría de cables en manos de empresas privadas, resulta fundamental el enfoque que estas tomen.

Cómo afrontar la ciberseguridad de los cables submarinos

En este nuevo escenario, las big tech se están convirtiendo en actrices principales, gracias a su creciente presencia como promotoras de proyectos: en una década, Google, Meta, Amazon y Microsoft han pasado de contar con el 10% de capacidad internacional al 71%. Preguntada por cómo abordan temas de protección y ciberseguridad de las infraestructuras, en Google se centran en el aspecto físico. “La seguridad es un factor clave en todas nuestras inversiones en infraestructura”, destacan. “Las rutas se eligen deliberadamente teniendo en cuenta muchos factores, y se utilizan métodos como el blindaje y el enterramiento del cable para proteger los cables submarinos”. Desde la compañía destacan como el mayor riesgo físico los barcos pesqueros y las anclas de los barcos, y apuntan que “la mejor protección contra estos riesgos y cualquier otro daño físico es construir una infraestructura de red que logre la resiliencia, en parte, a través de múltiples rutas de red diversas. Nuestra filosofía es crear suficientes rutas de red concurrentes a nivel metropolitano, regional y global, junto con un plano de control de software escalable, para soportar la redistribución del tráfico y minimizar la congestión de la red. Cuando se produce un daño físico, las rutas de red redundantes pueden redirigir el tráfico para minimizar la interrupción del servicio para los clientes y usuarios”.

La seguridad es un factor clave en todas nuestras inversiones en infraestructura”, aseguran fuentes de Google

Una de las compañías españolas con mayor implicación en esta red mundial es Telxius, filial de Telefónica. Desde la empresa inciden en que “los cables submarinos son más que solo infraestructura; son la columna vertebral del ecosistema digital global. En un mundo hiperconectado, los cables submarinos son esenciales y forman parte de un ecosistema digital más amplio que va más allá de la costa hacia centros de datos clave”, destacan. En lo relativo a la protección física de este tipo de infraestructuras críticas, desde la compañía apuntan a una significativa mejora en los últimos tiempos. “La accesibilidad física es limitada, de tal forma que la redundancia y la resiliencia siguen siendo esenciales para garantizar la continuidad ante daños accidentales ocasionados por la pesca, anclaje o fenómenos naturales como terremotos o deslizamientos que, de no existir redundancia, podrían afectar a la continuidad del servicio”. A nivel de ciberseguridad, se plantea una doble perspectiva. Por un lado, “garantizar diversidad y redundancia en todas nuestras rutas terrestres y submarinas, lo que nos permite mantener la continuidad del servicio con alta disponibilidad incluso ante interrupciones”. Lo ejemplifican con el caso de su ruta transatlántica, en la que Telxius ofrece lo que denominan como conectividad redundante a través de sus dos cables submarinos de última generación: Marea y Dunant.

Fuentes de Telxius consideran que “en un mundo hiperconectado, los cables submarinos son esenciales y forman parte de un ecosistema digital más amplio que va más allá de la costa hacia centros de datos clave”

Además, desde la filial de Telefónica hablan de proteger la infraestructura mediante un modelo integral de

seguridad. “En materia de ciberseguridad, Telxius adopta, para sus sistemas, redes y dispositivos IT, un enfoque multicapa y aprovecha la inteligencia artificial y el aprendizaje automático para la detección de amenazas en tiempo real”, inciden. Este modelo integral combinaría así distintos elementos, entre los que citan medidas físicas y ciberseguridad en las estaciones de amarre, auditorías periódicas y evaluación continua, planes de continuidad y recuperación ante desastres, pruebas periódicas y protocolos de actuación claros ante crisis, formación y sensibilización para reducir riesgos de ingeniería social y el uso de IA y aprendizaje automático para detección proactiva y mitigación de riesgos. “Y todo ello desde el cumplimiento normativo en áreas clave: continuidad del negocio, seguridad de la información, gestión medioambiental y eficiencia energética”, resumen. Un marco necesario para garantizar la continuidad de una infraestructura de la que depende gran parte de la vida moderna.

Disponible en:

https://www.computerworld.es/article/4098444/ciberseguridad-en-cables-su... [1]

Links
[1] https://www.computerworld.es/article/4098444/ciberseguridad-en-cables-submarinos-protegiendo-una-infraestructura-critica.html