La seguridad del ciberespacio se desarrolla también en el fondo de los océanos y mares

Cyberspace security is also developed at the bottom of the oceans and seas

Capitán de Corbeta Roberto Vargas Flores. Magíster en Derecho, Economía y Gestión, con mención en Relaciones Internacionales del Programa en Defensa y Dinámicas Industriales del Instituto Superior de Armamento y Defensa (ISAD) de la Universidad Paris II, Panthéon – ASSAS. Posee el título de Estudios Militares Superiores de la Escuela de Guerra de Francia con la certificación profesional nivel 8 (experto) en Gestión de Mando y Estrategia. Es Licenciado en Ciencias Marítimas Navales (Comando General) por la Escuela Naval del Perú (2008). Es calificado en guerra de superficie y sistemas de armas. Ha seguido el Programa de Formación de Oficiales de la Marina Nacional Francesa a bordo del Buque Escuela *Jeanne D'Arc*, en las especialidades de navegación nivel dirección y en seguridad fundamental. Hizo el Curso Básico de Inteligencia y el Curso Básico Estado Mayor en la Escuela Superior de Guerra Naval. Ha prestado servicios a bordo del B.A.P. *Herrera*, B.A.P. *Carvajal*, B.A.P. *Quiñones*, B.A.P. *Montero*, B.A.P. *Bolognesi* y como Segundo Comandante del B.A.P. *Castilla* en la Amazonía. En dependencias terrestres, ha servido en el Instituto de Educación Superior Tecnológico Público Naval – CITEN. Es graduado del Programa de Comando y Estado Mayor Conjunto de la Escuela Superior Conjunta de las Fuerzas Armadas. Actualmente, se desempeña como Subjefe de la Escuela de Guerra de Superficie.

Resumen: La importancia que representan en la actualidad los cables submarinos de fibra óptica para los Estados y las compañías transnacionales, los convierten en activos estratégicos que deberían ser protegidos adecuadamente, contar con una normatividad legal que permita gestionarlos, y con protocolos de actuación preestablecidos; ya que, de no atribuirse esa responsabilidad, implicaría arriesgar el normal funcionamiento de todo un país, en caso sean estos atacados o afectados por fenómenos naturales u antrópicos.

Este trabajo se propone analizar los orígenes de los cables submarinos, reflexionar en cómo estos podrían ser afectados, y establecer las implicancias que tienen en la seguridad y defensa de un Estado. El estudio es del tipo analítico-descriptivo porque se basa en un análisis de datos históricos con la finalidad de ayudar a comprender la real envergadura del objeto de estudio: los cables

submarinos. La data fue recolectada, en su mayoría, de libros en línea y páginas web de instituciones relacionadas a la investigación.

Palabras clave: Activo crítico, cables submarinos, seguridad y defensa nacional.

Abstract: *The importance that submarines fiber optic cables currently represent for States and transnational companies makes them strategic assets that should be adequately protected., with legal regulations to manage them and with pre-established action protocols, since, if this responsibility is not attributed, it would imply risking the normal functioning of an entire country, in case it is attacked or affected by natural phenomena or anthropic causes. The purpose of this work is to analyze the origins of submarine cables, to reflect on how they could be affected and to establish the implications they have on the security and defense of a State. The study is analytical-descriptive because it is based on an analysis of historical data in order to help understand the real importance of the object of study (submarine cables). The data was collected mostly from online books and web pages of institutions related to the research.*

Keywords: *Critical asset, submarine cables, national security and defense.*

Introducción

La red mundial de cables submarinos de datos es una infraestructura crítica vital para la actual dependencia informática y digital, que viene siendo reconfigurada después de la pandemia del covid-19, en la que se vieron expuestas grandes falencias de los Estados en sus diferentes sectores que lo componen; sin embargo, también estas lecciones aprendidas han contribuido a romper paradigmas relacionados a la comunicación, gestión, educación, salud, entre otros, en ambientes digitales.

Dado que los cables se extienden por el mar, atraviesan fronteras nacionales y, a menudo, están ocultos bajo tierra, con frecuencia han caído en el olvido y han recibido una atención limitada por parte de los responsables políticos. A raíz de la actividad naval rusa, desde el 2014, y de las conmociones geopolíticas provocadas por la guerra de Rusia en Ucrania, la vulnerabilidad de las infraestructuras marítimas está recibiendo cada vez más atención pública y política.

Arellano (2022) menciona: "Se estima que, en el presente año, 5,000 millones de usuarios (es decir, 63% de la población mundial)[1] hace uso del ciberespacio. En los últimos años, se ha presenciado el crecimiento exponencial de una progresiva dependencia a la Internet para actividades como la comunicación, las finanzas, el comercio, la geopolítica, el entretenimiento y la educación. En la actualidad, 99% de la información en el ciberespacio circula a través de cables de fibra óptica distribuidos a lo largo de una plataforma submarina mundial".

En ese sentido, ciertos gobiernos vienen demostrando su preocupación por elevar el nivel de protección y resguardo de esta red de cables submarinos, ya que su vulneración o afectación podría traer serias consecuencias en la gestión pública, privada y en la población, y tener incidencia directa en las políticas de seguridad y defensa nacional.

El presente artículo propone visualizar la importancia de la red de cables submarinos y la necesidad de mejorar la estrategia y la capacidad actual para resguardar su integridad a fin de garantizar el desarrollo y seguridad del país, reduciendo el riesgo de que esta fuera afectada. Para ello, planteamos la siguiente interrogante: ¿En qué medida se puede afirmar que la red de cables submarinos debe ser considerada como activo crítico de un Estado? En ese sentido, se analizó las informaciones actuales disponibles en bibliotecas digitales o páginas web con información confiable, que permitan, finalmente, arribar a conclusiones y recomendaciones respecto al tema.

Los cables submarinos: reflexiones

La red de cables submarinos es la infraestructura crítica central de la era digital, pues permite la accesibilidad al ciberespacio en un mundo cada vez más inalámbrico, dependiente de esta red de cables de fibra óptica instalada en el fondo del océano.[2] La primera conexión transoceánica a través de cables se realizó en 1858, entre Irlanda y Canadá.[3] Sin embargo, solo funcionó durante tres semanas antes de romperse sin posibilidad de reparación.

---

1 Recuperado de: https://dgtlinfra.com/submarine-cables-fiber-link-internet/ (Submarine Cables: the Invisible Fiber Link Enabling the Internet - Dgtl Infra, s. f.)

2 Data Centre Development DCD. D. Swinhoe. What is a submarine cable? Subsea fiber explained, Data Center Dynamics, 26 de Agosto 2021. Recuperado en línea de https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiber explained/#:%7E:text=Subsea%20or%20submarine%20cables%20are,from%20one%20point%20to%20another.

3 Cables submarinos, internet bajo el agua. Recuperado de: https://www.telefonica.com/es/sala-comunicacion/blog/cables-submarinos-internet-bajo-el-agua/

En la actualidad, existen más de 1,3 millones de kilómetros de cables de fibra óptica que se encuentran extendidos en las profundidades de los océanos y que permiten la interconexión y distribución de información de 4,950 millones de usuarios[4] en todo el mundo. El 99 % de estos intercambios de información,[5] la economía global y los servicios digitales dependen de esta red submarina, que está formada por 530 cables activos y proyectados según los datos de *TeleGeography*.[6]

En el Perú, existen 21,89 millones de usuarios de Internet[7] que se comunican con el mundo a través de cuatro cables submarinos, que tienen puertos de amarre en territorio nacional,[8] lo que representa un reto estratégico debido a la dependencia de la población a este servicio. Sin embargo, dado que los cables se extienden en el mar, su seguridad ha sido olvidada con frecuencia y ha recibido una atención limitada por parte de los responsables, no solo a nivel nacional, sino también mundial.

> La seguridad de los cables submarinos es un elemento poco estudiado de la seguridad internacional…su protección es un ámbito demasiado esencial de la política internacional como para seguir siendo un apéndice técnico del análisis de seguridad…aunque hay una creciente concienciación, sigue habiendo una falta de cuidado entre los responsables políticos. (Bueger, Liebetrau y Franke, 2022)[9]

El mar como entorno conflictivo

En el siglo XVII, el jurista holandés Grotius consideraba que el mar era un bien común de la humanidad por no ser urbanizable y, por tanto, no constituía un territorio, sino solo una zona de tránsito.[10] Hoy, por el contrario,

---

4 Hootsuite. Digital 2022 Global Overview Report. Enero 2022, Recuperado de: https://www.hootsuite.com/resources/digital-trends

5 La Mesure de la force. Tratado de Estrategia de la Escuela de Guerra. Motte Soutou De Lespinois Zajec. Edición 2021. (P.152)

6 TeleGeography. Submarine Cable Frequently Asked Questions. Recuperado de: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

7 Datareportal. Digital 2022: Perú. Simon Kemp. Recuperado de: https://datareportal.com/reports/digital-2022-peru

8 Mapa de cable submarino. TeleGeography. Última actualización 10 de noviembre 2022. Recuperado de: https://www.submarinecablemap.com/country/peru

9 Security threats to undersea communications cables and infrastructure – consequences for the EU. Christian Bueger, Tobias Liebetrau, Jonas Franke. June 2022.

10 Hugo Grotius, Mare liberum, 1609.

tiene zonas parcialmente ocupadas, explotadas y habitadas, es decir, cuasi territorios, pero que, por su estatus ambiguo e interdependiente, complica más las relaciones internacionales.

Hervé Coutau-Bégarie, tras la guerra anglo-argentina de 1982 por la posesión de las islas Malvinas, señalaba que el mar "antes era un simple escenario de conflicto, ahora se ha convertido en un objeto de conflicto". Por lo tanto, el mar se ha transformado en un espacio de exploración y explotación de recursos, que ha demandado de tratados internacionales para la aceptación y adaptación de diversas infraestructuras en los océanos alrededor de los continentes,[11] de manera que su importancia política y estratégica lo convierte en una de las principales razones de las rivalidades internacionales, tendencia que se ve agravada por la ambigüedad de su estatuto jurídico, pues el mar puede concebirse como una *res communis* (cosa común, perteneciente a todos) o una *res nullius* (cosa de nadie, perteneciente a nadie).

En el primer caso, el mar debería ser gestionado por y para toda la humanidad, pero esto ignora el hecho de que pocas naciones tienen los medios efectivos para hacerlo. En el segundo caso, el mar pertenece a quienes pueden controlarlo y donde pueden controlarlo. Este segundo caso prevalece de facto: concretamente, los espacios marítimos siempre han tendido a constituir "un campo libre para el libre saqueo", según la fórmula del jurista y geopolítico Carl Schmitt.[12] Por lo tanto, quien quiera hacer respetar sus intereses debe presentarse ante el sistema internacional con medios de poder disuasivos.

Por tal motivo, el mar ya no es un espacio completamente liso y desértico, ahora está lleno de zonas ambiguas en las que las plataformas y tuberías de petróleo, campos eólicos, cables submarinos y otros equipamientos, han creado una reestructuración y transformación del estatus del mar en un nuevo entorno operativo, como lo confirma una investigación preliminar sueca en relación a las explosiones del oleoducto Nord Stream[13] durante el año 2022:

---

11 L. Wedin, Estrategia marítima en el siglo XXI, p. 70-71 et 143-144.

12 Carl Schmitt, Le Nomos de la Terre [1950], Paris, PUF, 2008, p. 48.

13 France24, Fiscalía sueca halla signos de "sabotaje" en las explosiones de Nord Stream, Yurany Arciniegas, 18 de noviembre 2022.

> El fiscal sueco a cargo de la investigación preliminar de las roturas a gran escala en los oleoductos Nord Stream 1 y 2 confirmó este 18 de noviembre que los investigadores hallaron rastros de explosivos en el lugar. Para los investigadores, hay pistas de "sabotaje grave" en los conductos del mar Báltico, que transportaban gas de Rusia a Europa.

En otras palabras, las características intrínsecas del mar —el fondo marino— ofrecen la oportunidad para llevar a cabo operaciones militares especiales quirúrgicas, sin que se pueda reclamar ni atribuir la acción a un actor de forma precisa. Asimismo, el medio marino no tiene población que gestionar, su estatus internacional impide excluir a los neutrales y su enorme tamaño impide la idea de un control total. La inmensidad del mar hace muy difícil la localización y control de los buques, de ahí las palabras del marino-novelista Monsarrat: "El océano es el mejor escondite del mundo".[14]

Dependencia de una infraestructura de cable submarino operativa

El sistema financiero, y en especial la negociación en el mercado mundial, depende del enlace de fibra óptica, pues permite operar y transmitir la masa de información necesaria a gran velocidad y a larga distancia entre sus actores. Por lo tanto, la pérdida de comunicaciones durante unos minutos u horas puede tener repercusiones desastrosas en operaciones sensibles para ese preciso momento; de modo que, cualquier forma de daño a estos cables tendrá un impacto significativo en la economía y en la soberanía digital.

Sin Internet, la mayoría de las empresas no podrían mantener sus rutinas de trabajo, conectar con clientes, autoridades y empresas, ni siquiera generar beneficios. Basado en esto, los cables submarinos juegan un rol fundamental en el dominio del ciberespacio y en el campo geoestratégico del mundo actual, tanto como para los instrumentos de poder: diplomático, informativo (comunicaciones), militar y económico.

En el ámbito de la seguridad y defensa, los Estados también dependen, en gran medida, de la conectividad digital. En la era de la guerra digital y las plataformas integradas, la mayoría de las capacidades de defensa de los Estados están conectadas digitalmente. Esto se refiere a las estructuras de mando y control, pero también a los sistemas de armas integrados, incluidos unidades de combate, drones y buques.

14 Nicholas Monsarrat. La Mer cruelle [1951], Paris, Phébus, 1999, p. 106.

Por otro lado, la vida social actual necesita más que nunca de las conexiones a Internet. Las redes sociales y los mensajeros en línea ofrecen formas rápidas y eficaces de comunicarse y organizarse. Gran parte de la comunicación de crisis y la alerta de catástrofes dependen, actualmente, de las tecnologías de Internet, lo que las hace insustituibles en estos escenarios.

En suma, diversas actividades críticas dependen cada vez más de una conexión estable y segura a Internet. Los sectores de transporte, salud, agricultura, vivienda, y otros de la administración pública, intensifican aún más la dependencia a Internet, que les permite brindar los servicios públicos esenciales correspondientes.

Cables vulnerables a desastres ocasionados por la naturaleza y por actividades humanas

De acuerdo a los desarrolladores del blog *Cloudflare*, que operan en más de cien países del mundo y brindan una perspectiva sobre la resiliencia de Internet, monitoreando las interrupciones de las comunicaciones, solo durante los diecinueve primeros días del 2022 hubo cuatro interrupciones importantes de Internet: en Gambia, por un problema con sus cables; Kazajistán, a causa de disturbios; Burkina Faso, debido a un complot golpista; y Tonga, por un desastre de origen natural. Sin embargo, este blog señala que, durante la última década, ciertos gobiernos han optado por interrumpir este servicio a fin de controlar o limitar la comunicación entre los ciudadanos y el mundo exterior.

Por ejemplo, si se llegara a producir un fenómeno natural de gran magnitud en el mar, podría provocar un daño significativo a un cable submarino. Cito lo manifestado por Levy (2022):

> El pasado 15 de enero de 2022, el volcán submarino Hunga Tonga-Hunga Ha'apai, ubicado en el Pacífico Sur, frente a la costa de Tonga, entró en erupción y, como consecuencia, cortó los cables submarinos de acceso a Internet, lo que dejó prácticamente incomunicada la isla…de tal manera que la coordinación de las misiones de ayuda o rescate se dificultaron. Durante varios días fue casi imposible obtener información sobre lo que allí sucedía y, de no ser por los teléfonos satelitales, los pobladores de Tonga hubieran quedado totalmente incomunicados.[15]

15 ¿Qué le pasaría a la humanidad si el servicio de internet fuera interrumpido? Gabriel E. Levy B. 03 de agosto 2022. Recuperado de: https://andinalink.com/la-dependencia-de-la-humanidad-a-la-conectividad-submarina/#_ftnref2

Como vemos, existen amenazas de origen natural y también causadas por actividades humanas, intencionadas o no, que ponen en riesgo esta infraestructura crítica. Según las estadísticas del Comité Internacional de Protección de Cables (ICPC por sus siglas en idioma inglés), cerca del 70% de los daños que sufren los cables en el mundo son causados accidentalmente por la pesca y el fondeo, a pesar de que estos están claramente marcados en las cartas marítimas.

Con el fin de mitigar, proteger y promover un plan de resiliencia de los cables submarinos de telecomunicaciones en el mundo, en relación a la categoría de amenaza de *actividades humanas no intencionadas*, el ICPC recomienda a los Estados algunos principios generales[16] basados en buenas prácticas gubernamentales. Entre ellos, se recomienda "respetar y aplicar las obligaciones de los tratados (en particular la Convención de las Naciones Unidas sobre el Derecho del Mar [CNUDM]) y el derecho internacional consuetudinario que define la jurisdicción de los Estados sobre los cables submarinos y su protección", así como "comprometerse con otros Estados a nivel mundial y regional para la protección de estos, ya que las acciones de otros Estados pueden afectar en gran medida a la propia conectividad de un Estado".

En consecuencia, los Estados han visto por conveniente establecer una sólida cooperación con el sector privado para mantener y resguardar su propia infraestructura crítica, cuya interrupción o destrucción produciría un grave impacto en la nación, disponiendo de medios para detectar problemas en los sistemas informáticos y puedan, en caso sea necesario, hacer uso de sus Fuerzas Armadas para esta gestión de protección y mantenimiento.[17] Sin embargo, por ahora, no existe un sistema internacional integrado de control y reparación.

Por otro lado, la CNUDM en sus artículos 79, 87 y 112 establece que todos los Estados pueden tender libremente cables y tuberías submarinas en el lecho de alta mar más allá de la plataforma continental. También señala que, los Estados ribereños tienen el derecho (pero no la obligación) de adoptar normas para proteger los cables submarinos en sus aguas territoriales,[18]

---

16 Buenas prácticas gubernamentales para proteger y promover la resiliencia de los cables submarinos de telecomunicaciones. ICPC. Actualizado el 11 de febrero del 2022.

17 La voz del sur. Es. Pepe Contreras. La Armada controla la actividad naval de Rusia en torno a la red de cable global. 24 de octubre del 2022. Recuperado de https://www.lavozdelsur.es/actualidad/sociedad/armada-controla-actividad-naval-rusia-en-torno-red-cable-global_284767_102.html

18 United Nations Convention on the Law of the Sea, Artículo 21(c), 1982. Recuperado en línea: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

es decir, mantienen el derecho de establecer condiciones para la entrada de cables en su territorio o en su mar territorial. En consecuencia, para tender un cable submarino hacia la costa a través del mar territorial de otro Estado, los propietarios de la infraestructura necesitan la autorización correspondiente del Estado ribereño.

En cuanto a las zonas situadas fuera de las aguas territoriales de los Estados costeros, la CNUDM no obliga a ningún Estado a salvaguardar los cables submarinos, sino que les impone la obligación de adoptar normas que garanticen que los buques que enarbolen su pabellón sean castigados por destruir o dañar un cable submarino.[19] Sin embargo, para algunos críticos, estas disposiciones "se perciben a veces como anticuadas e inadecuadas para los retos de hoy en día",[20] pues se aplican sobre el fondo marino de la plataforma continental, de manera que, nos podríamos encontrar frente a una situación que podría generar un conflicto de intereses entre Estados.

Daños por actividades humanas intencionadas

Por otra parte, existe la categoría de amenaza de *actividades humanas intencionadas*, es decir, de sabotajes a esta infraestructura, sobre todo en tiempos de conflictos, como parte de las operaciones de guerra híbrida o de *zona gris*, o generadas por el terrorismo internacional u organizaciones de crimen organizado. En esta categoría, la modalidad de ataque es básicamente la interrupción provocada por corte o destrucción física del cable submarino.[21]

Al respecto, Jordán (2018), en su artículo "El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo", cita a diferentes autores para definirla como "el espacio por

19 Ibid. Artículo 113, 1982.

20 K. Scott, 'Laws governing undersea cables have hardly changed since 1884 – Tonga is a reminder they need modernizing', The Conversation, 21 January 2022; R. Beckman, 'Submarine Cables – A Critically Important but Neglected Area of the Law of the Sea', ISIL Conference, 2010, pp. 12-16.

21 "En cuestión de dos días, cinco cables submarinos de fibra óptica han sido cortados en distintos puntos de Europa. Dos de ellos afectaron a las islas Shetland, al norte de Escocia, dejando a sus 23.000 habitantes sin teléfono ni Internet. Los otros tres se produjeron cerca de Marsella, el nudo de conexiones digitales más importantes del Mediterráneo. Las rutas Marsella-Barcelona, Marsella-Lyon y Marsella-Milán quedaron interrumpidas, provocando alteraciones no solo en el Internet europeo, sino también en la red asiática e incluso en la estadounidense". El Diario.es Carlos del Castillo, Actualizado el 25/10/2022. Recuperado de: https://www.eldiario.es/tecnologia/cortes-cables-submarinos-aumentan-temor-sabotaje-ruso-internet-europeo_1_9649519.html

excelencia del *hybrid warfare*, otro *buzzword* nacido en la comunidad de defensa norteamericana, aceptado como variante de amenaza híbrida según declaraciones oficiales de la Alianza Atlántica y de la Unión Europea".[22]

Es por ello que el mar, precisamente el fondo marino, posee estas características de *zona gris*, ya que se puede generar una acción sin confirmar el autor, pues en esta zona hay asuntos que no son siempre bien definidos,[23] además, "la competición estratégica entre dos o más Estados discurre por debajo del umbral de la violencia política y del conflicto armado menor" (Baqués, 2017, 26). "En una zona gris se procura no cruzar líneas rojas que desemboquen en una contienda militar con costes altamente elevados y consecuencias imprevisibles" (Mazarr, 2015, 58).

Aunque los cortes podrían ser en su mayoría por origen natural o accidental, no se puede descartar la posibilidad de un daño intencionado y coordinado para generar graves consecuencias en términos de conectividad y continuidad de los servicios. Por ejemplo, en la historia naval peruana, durante la guerra del Pacífico, el 31 de mayo de 1879, el Almirante Miguel Grau en una carta dirigida al Director de Marina[24] informa lo siguiente:

> En la mañana del 27 me dirigí nuevamente al fondeadero con el intento de rastrear y cortar el cable submarino. Me aproximé con tal fin hasta 600 metros de la población para alargar las rastras y, no obstante de que en tierra se notaba mucho movimiento de tropas y preparativos de defensa, arrié mis embarcaciones y, con ellas por un lado y el buque por otro, pude tornar el cable y cortarlo sin ser absolutamente molestado durante la operación.

Últimamente, acciones similares se han planteado más de una vez como hipótesis en los altos círculos estratégicos militares de la Organización del Tratado del Atlántico Norte (OTAN), tejiéndose como posibilidad acciones de espionaje o ataques a esta infraestructura para ocasionar una oscuridad digital que impacte a las capacidades nacionales de un Estado:[25] "A raíz de la

22 Colom, Guillem. 2018. «Análisis de la actualidad internacional: contextualizando la guerra híbrida», Ciber Elcano, 32: 4-9.

23 Oldham, 2015; Votel et al., 2016

24 Las Memorias de Grau. Campaña Marítima. Grau se niega a bombardear a pobladores indefensos en Antofagasta. Ricardo Cuya Vera. 25 de octubre del 2017. Recuperado de: https://www.grau.pe/campana-maritima/grau-se-niega-a-bombardear-a-pobladores-indefensos-en-antofagasta/

25 Security threats to undersea communications cables and infrastructure – consequences for the EU. Christian Bueger, Tobias Liebetrau, Jonas Franke. June 2022, p. 9.

actividad naval rusa desde 2014 y las ondas geopolíticas enviadas por la guerra de Ucrania de 2022, la vulnerabilidad de las infraestructuras marítimas está recibiendo ahora una creciente atención pública y política".

Con la tecnología actual, se puede prever una variedad de modalidades de ataque sobre estos cables, entre ellas la interceptación o la interrupción de datos por corte o destrucción. En definitiva, esta acción en tierra parece más accesible que en el fondo marino, pero no se puede descartar totalmente la práctica del "piggybacking"[26] en el empalme final de un cable submarino que se encuentra en aguas profundas, debido a los requisitos técnicos favorables que ofrecen las operaciones en el mar para una actuación discreta y eficaz.

Los investigadores Pierre Morcos y Colin Wall, en un artículo publicado en junio del 2021 en el sitio web del CSIS titulado "Invisible and Vital: Los cables submarinos y la seguridad transatlántica", afirman que "hay varios objetivos concebibles que podrían conseguirse cortando un cable: cortar las comunicaciones militares o gubernamentales en las primeras fases de un conflicto, eliminar el acceso a Internet de una población objetivo, sabotear a un competidor económico o causar una perturbación económica con fines geopolíticos. Los actores también podrían perseguir varios o todos estos objetivos simultáneamente".

Desde hace unos años, fuerzas del bloque de Occidente vienen observando un aumento de la actividad de los buques rusos a lo largo de las rutas de los cables submarinos en el Atlántico Norte, en particular, el buque ruso de investigación oceanográfica *Yantar*, que ha sido visto en varias oportunidades en las proximidades de las rutas de determinados cables submarinos en el golfo de Vizcaya y en el Mediterráneo.

De hecho, tanto Rusia como Estados Unidos (EE. UU.) poseen unidades con grandes capacidades para actuar en el dominio cibernético en el fondo del mar para misiones especiales, las cuales pueden realizar diversas tareas,

---

26 "A nivel informático, el piggybacking consiste en obtener acceso a una red informática con la computadora del atacante, no mediante el jaqueo de una computadora que normalmente tiene acceso a dicha red. Normalmente se trata de redes inalámbricas de las que el atacante ha conseguido la contraseña y a las que accede sin conocimiento de los propietarios o gestores de las mismas. Conseguir la contraseña de una red inalámbrica es cuestión de técnica y tiempo —o de ingeniería social— y una vez dentro, el abuso puede producirse por distintas vías". Recuperado de: https://es.linkedin.com/learning/ingenieria-social-para-it/piggyback-o-el-acceso-por-exceso-de-confianza

desde instalar dispositivos de escucha para 'pinchar' las comunicaciones de todo un país,[27] hasta interrumpir las comunicaciones mundiales.[28]

Es así que, en el contexto de la guerra de Rusia en Ucrania, el presidente de EE. UU., Joe Biden, expresó su preocupación por el panorama cibernético mundial tras las sanciones que se han impuesto a Moscú por su invasión a Ucrania,[29] advirtiendo que Rusia estaba considerando una variedad de posibles vías para realizar ciberataques, entre las cuales se barajaba la hipótesis de atacar la infraestructura crítica de la red de cables submarinos que arriban a diferentes países para dejarlos incomunicados, pudiendo ocasionar una catástrofe de comunicación digital a nivel mundial.

Por lo tanto, la hipótesis de ataque a los cables submarinos es real. También lo confirmamos en el mes de setiembre del presente año, mes en que se registraron explosiones en el mar Báltico que provocaron fugas de gas natural de los gasoductos Nord Stream 1 y 2, que, según los expertos, habrían sido ocasionadas "por un sabotaje", cuya autoría aún no está clara. Posteriormente, se detectaron cortes de cables submarinos en el sur de Francia que afectaban a los principales cables de conectividad entre Asia, Europa y EE. UU.

Estos incidentes han hecho que crezca la preocupación de la OTAN en relación a posibles daños a la red de cables submarinos de fibra óptica. Jens Stoltenberg, Secretario General de la OTAN, explicó que, debido al actual contexto de guerra entre Rusia y Ucrania, existen especulaciones de que Moscú podría estar "enviando un mensaje" con estas explosiones en el gaseoducto, para demostrar que posee la capacidad de efectuar misiones especiales en el fondo del mar y así responder a las sanciones económicas impuestas por el bloque de Occidente.

---

27 El Confidencial. Pepe Cervera. Guerra fría entre EEUU y Rusia en el fondo del mar para cortar internet. 08 marzo de 2018. Recuperado en línea https://www.elconfidencial.com/tecnologia/2018-05-08/cables-submarinos-internet-tecnologia-militar-eeuu-rusia_1559024/

28 La Nación/Argentina/GDA. Belgorod, el submarino espía y asesino del Kremlin buscaría interrumpir las comunicaciones mundiales. 04 Octubre de 2022. Recuperado en línea: https://www.eleconomista.net/actualidad/Belgorod-el-submarino-espia-y-asesino-del-Kremlin-buscaria-interrumpir-las-comunicaciones-mundiales-20221004-0032.html

29 DW. El mundo. Joe Biden alerta de posibles ciberataques rusos a EE.UU. 21 de marzo de 2022. Recuperado en línea https://www.dw.com/es/joe-biden-alerta-de-posibles-ciberataques-rusos-a-eeuu/a-61207221

Importancia de la red de cables submarinos en el Perú y el mundo

En suma, todos estos elementos demuestran que esta infraestructura es de suma importancia en la geopolítica mundial y para el desarrollo de capacidades nacionales de un Estado, a través de las cuales, estos pueden atender sus necesidades vitales y desarrollar, normalmente, su vida cotidiana con el mundo. Para la mayor parte de los países, la protección de la red de transporte de información internacional es un tema de seguridad nacional, pues permite la interconexión con el resto del globo, considerándola como una infraestructura crítica.

Sin embargo, en el contexto nacional, el Plan Estratégico de Desarrollo Nacional al 2050 del Estado peruano, en el marco de riesgos y amenazas desde el entorno externo, considera:

> El informe de Riesgos Globales 2020 del Foro Económico Mundial, el cual identificó dentro de los 10 principales riesgos con mayor probabilidad de ocurrir en el mundo, a problemas relacionados al mundo cibernético (BID y OEA, 2020). Entre ellos se encontraban el riesgo de ciberataques a la infraestructura crítica y el fraude o robo de datos, por lo que se reconoce la necesidad de que la protección requerida a la infraestructura es tanto física como lógica.

En consecuencia, un ciberataque a la infraestructura física de cables submarinos podría debilitar considerablemente la economía y el desarrollo de capacidades nacionales dependientes del dominio del ciberespacio. Conocedores de esta amenaza, el Perú viene sentando las bases para fortalecer la gobernanza digital con la aprobación del Decreto Legislativo 1412 que aprueba la Ley de Gobierno Digital y norma los ámbitos del marco de seguridad digital del Estado peruano, así como con la Ley 30999, Ley de Ciberdefensa, que tiene como finalidad defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y los recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

En contraparte, nuestro país aún no posee una red de comunicación satelital como sistema alterno que brinde servicio a las entidades públicas y poblaciones en zonas alejadas, sobre todo ante emergencias. Peor aún, no se maneja protocolos de intervención ante interrupciones o cortes a los cables submarinos. Por lo que, esta infraestructura crítica debería estar considerada en la lista de activos críticos nacionales, por la relevancia que representa para la seguridad y defensa de nuestra nación.

Esta decisión permitiría que el Estado desarrolle capacidades que fortalezcan su seguridad y resiliencia. Con estas iniciativas, el Perú podría asegurar su crecimiento, alineado con los indicadores internacionales de digitalización, y, principalmente, mantener su ubicación en el Grupo A del *Índice GovTech del Banco Mundial* junto a los países que presentan un mayor nivel en transformación digital.

Conclusiones y recomendaciones

Como conclusión principal, luego de analizar el contexto actual en relación a la seguridad cibernética y la dependencia a las comunicaciones en el mundo, entendemos que los cables submarinos son vectores estratégicos y desempeñan un papel clave como infraestructura crítica que permite desarrollar y/o mantener capacidades nacionales, y cuya afectación, destrucción o perturbación no admitiría procedimientos de solución alternativos inmediatos en el Perú, y generaría grave perjuicio a la nación. En ese sentido, como miembro de las Fuerzas Armadas del Perú y, bajo la definición del rol estratégico de "participar, en coordinación con otros sectores del Estado, en la ejecución de las políticas públicas que contribuyan al desarrollo económico, social y sostenible del país, aplicando un enfoque de seguridad multidimensional", presento las siguientes conclusiones y recomendaciones:

1. El intercambio oportuno de información se convierte en un elemento esencial para el éxito de los negocios internacionales y la vida social cotidiana. Las ventajas de acceso a Internet y la rapidez en el flujo de información que brindan los cables submarinos deben sopesarse cuidadosamente frente a las preocupaciones de seguridad a largo plazo, considerando que estos han sido objetivos en conflictos interestatales y continuarán siendo un riesgo latente de seguridad en el futuro. Por lo tanto, se recomienda que el Estado peruano, a través del Ministerio de Transportes y Comunicaciones, efectúe la evaluación y monitoreo del sistema de transporte de información internacional, por lo que se requiere la participación y cooperación del sector privado propietario de la red de cables submarinos que llegan al Perú. Asimismo, como recomendación adicional, el Estado peruano debe gestionar, con liderazgo y compromiso gubernamental, la protección de los cables submarinos, plantear estrategias para

minimizar los riesgos que podrían afectarlos, y trabajar de manera asociada y coordinada con el sector privado.

2. Bajo una perspectiva de seguridad, en nuestro país, mediante Decreto Supremo 106-2017-PCM se aprobó el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales ACN, que establece dentro de las responsabilidades del Ministerio de Defensa, elaborar y actualizar la Directiva Nacional de Seguridad y Defensa para la Protección de los ACN, así como identificar y evaluar los riesgos en materia de seguridad y defensa nacional. La red de cables cumple con los requisitos fundamentales para ser considerados como ACN: primero, su relación con los objetivos y capacidades nacionales; segundo, su importancia para el Estado; y tercero, la inexistencia de soluciones alternativas inmediatas. Por lo tanto, se recomienda que el Gobierno los reconozca como activo crítico y fortalezca las políticas de seguridad y protección de la interconexión del país con el resto del mundo, en especial si existe ya una gran preocupación por la seguridad cibernética en el Plan Estratégico.

3. La resiliencia informática de un Estado depende de la diversidad de sus conexiones con el resto del mundo: diversidad de puntos de llegada de cables en su territorio, diversidad de países conectados, diversidad de proveedores y operadores de cables. El Perú solo cuenta con cuatro troncales de cables submarinos que pueden sufrir daños de origen estructurales, accidentales o ataques internacionales. Por esta razón, se recomienda que el Estado peruano trabaje en sinergia con el sector privado, con la finalidad de impulsar un adecuado intercambio de inteligencia, normas de seguridad, evaluaciones de riesgo, capacidades de supervisión y reparación, así como sus planes de contingencia, y que contemplen un mayor respaldo en el derecho internacional para proteger los cables submarinos que llegan al territorio nacional y garantizar su resistencia.

4. Teniendo en cuenta que, la Internet es la principal amenaza que afecta la información, por su diversidad de formas y la incidencia histórica analizada, es recomendable implementar en la Institución responsabilidades claras con niveles de acceso y autoridad que permitan realizar de manera segura el intercambio de información,

y coordinar acciones de investigación y difusión de contenidos relacionados a la seguridad de la Internet con alcance nacional. Se hace necesario, también, impulsar una política que incentive compartir experiencias frente situaciones de ataque a las redes, a fin de establecer protocolos de actuación frente a casos similares.

5. Nuestro país aún no posee una red de comunicación satelital como sistema alterno que brinde servicio a las entidades públicas y poblaciones en zonas alejadas, sobre todo ante emergencias. Por lo tanto, se recomienda que el Estado evalúe la necesidad de adquirir un satélite de comunicaciones de uso dual —militar y civil—, a fin de cerrar las brechas de conectividad, sobre todo frente a una emergencia, así como proporcionar un ancho de banda adecuado para las comunicaciones de comando y control en un espectro de solución multidimensional.

Referencias

1. ADAMSKY, D. *Cross-domain coercion: the current Russian art of strategy*. Institut Français des Relations Internationales. Proliferation Papers, 2015. P. 54. Disponible en: https://bit.ly/2aUq2UN
2. ARELLANO. *El sistema de gobernanza en el marco regulatorio de la red global de cables submarinos de fibra óptica*. Universidad Central de Ecuador. Facultad Jurisprudencia, Ciencias Políticas y Sociales en la carrera de Derecho. Quito, Ecuador, 2022.
3. BAQUÉS, J. *Hacia una definición del concepto «Gray Zone»* (GZ), Documento de Investigación 2/2017. Instituto Español de Estudios Estratégicos. España, 2017.
4. BUEGER, et al. *Security threats to undersea communications cables and infrastructure – consequences for the EU*. 2022. P. 9.
5. CARTER et al. *Submarine Cables and the Oceans: Connecting the World*. The United Nations Environment Programme World Conservation Monitoring Centre Biodiversity Series. 2009.
6. CUYA, R. *Las Memorias de Grau*. "Campaña Marítima. Grau se niega a bombardear a pobladores indefensos en Antofagasta". 2017.

Disponible en: https://www.grau.pe/campana-maritima/grau-seniega-a-bombardear-a-pobladores-indefensos-en-antofagasta/

7. DEL CASTILLO, C. *El Diario.es*. "Varios cortes de cables submarinos aumentan el temor a un sabotaje ruso del Internet europeo". 2022. Disponible en: https://www.eldiario.es/tecnologia/cortes-cables-submarinos-aumentan-temor-sabotaje-ruso-internet-europeo_1_9649519.html
8. ESTADO PERUANO. *Plan Estratégico de Desarrollo Nacional al 2050*. Lima: Presidencia del Consejo de Ministros, 2022.
9. FREIER, N. *Outplayed: regaining strategic initiative in the gray zone*. Carlisle: U. S. Army War College Press. 2016.
10. GROTIUS, H. *Mare liberum*. 1609.
11. HOOTSUITE. *Digital 2022 Global Overview Report*. 2022. Disponible en: https://www.hootsuite.com/resources/digital-trends
12. INLEARNING. *Piggyback o el acceso por exceso de confianza*. 2022. Recuperado de: https://es.linkedin.com/learning/ingenieria-social-para-it/piggyback-o-el-acceso-por-exceso-de-confianza
13. ISCPC.ORG. *Buenas prácticas gubernamentales para proteger y promover la resiliencia de los cables submarinos de telecomunicaciones*. 2022. Disponible en: file:///C:/Users/windows/Downloads/ICPC-Gov't-Best-Practices-for-Cable-Protection--Resilience-Version-1.2-(Spanish).pdf
14. KEMP, S. "Digital 2022: Perú". *Datareportal*. 2022. Disponible en: https://datareportal.com/reports/digital-2022-peru
15. KIM, J. *Cables submarinos: el enlace de fibra invisible que permite Internet*. 2022. Recuperado de: https://dgtlinfra.com/submarine-cables-fiber-link-internet/
16. LEVY, G. *¿Qué le pasaría a la humanidad si el servicio de internet fuera interrumpido*? 2022. Recuperado de: https://andinalink.com/la-dependencia-de-la-humanidad-a-la-conectividad-submarina/#_ftnref2
17. MAZARR, M. *Mastering the gray zone: understanding a changing era of conflict*. Carlisle: U.S. Army War College Press. 2015.
18. MONSARRAT, N. *La Mer cruelle – 1951*. París, 1999. P. 106.
19. MORCOS, P. y Wall, C. *Invisible and Vital: Los cables submarinos y la seguridad transatlántica*. Sitio web del CSIS, 2021.
20. MOTTE, et al. *La Mesure de la force. Tratado de Estrategia de la Escuela de Guerra*. 2021. P.152.
21. OLDHAM, C. *SOCOM: navigating the gray zone, Defense Media Network*. 2015. Recuperado de: https://bit.ly/2yRNgUe
22. SCHMITT, C. *Le Nomos de la Terre*. 1950, Paris, PUF. 2008. P. 48.
23. TELEFÓNICA. *Cables submarinos, internet bajo el agua*. 2022. Disponible en: https://www.telefonica.com/es/sala-comunicacion/blog/cables-submarinos-internet-bajo-el-agua/
24. TELEGEOGRAPHY. "Submarine Cable Frequently Asked Questions".

2022. Disponible en: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
25. TELEGEOGRAPHY. "Submarine Cable Map". 2022. Disponible en: https://www.submarinecablemap.com/country/peru
26. VOTEL, et al. *Unconventional warfare in the gray zone, Joint Forces Quarterly*. 2016. Pp. 80, 101-109.
27. WEDIN, L. *Stratégies maritimes au XXIe siècle*. op. cit. 2016. P. 70-71 et 143-144.