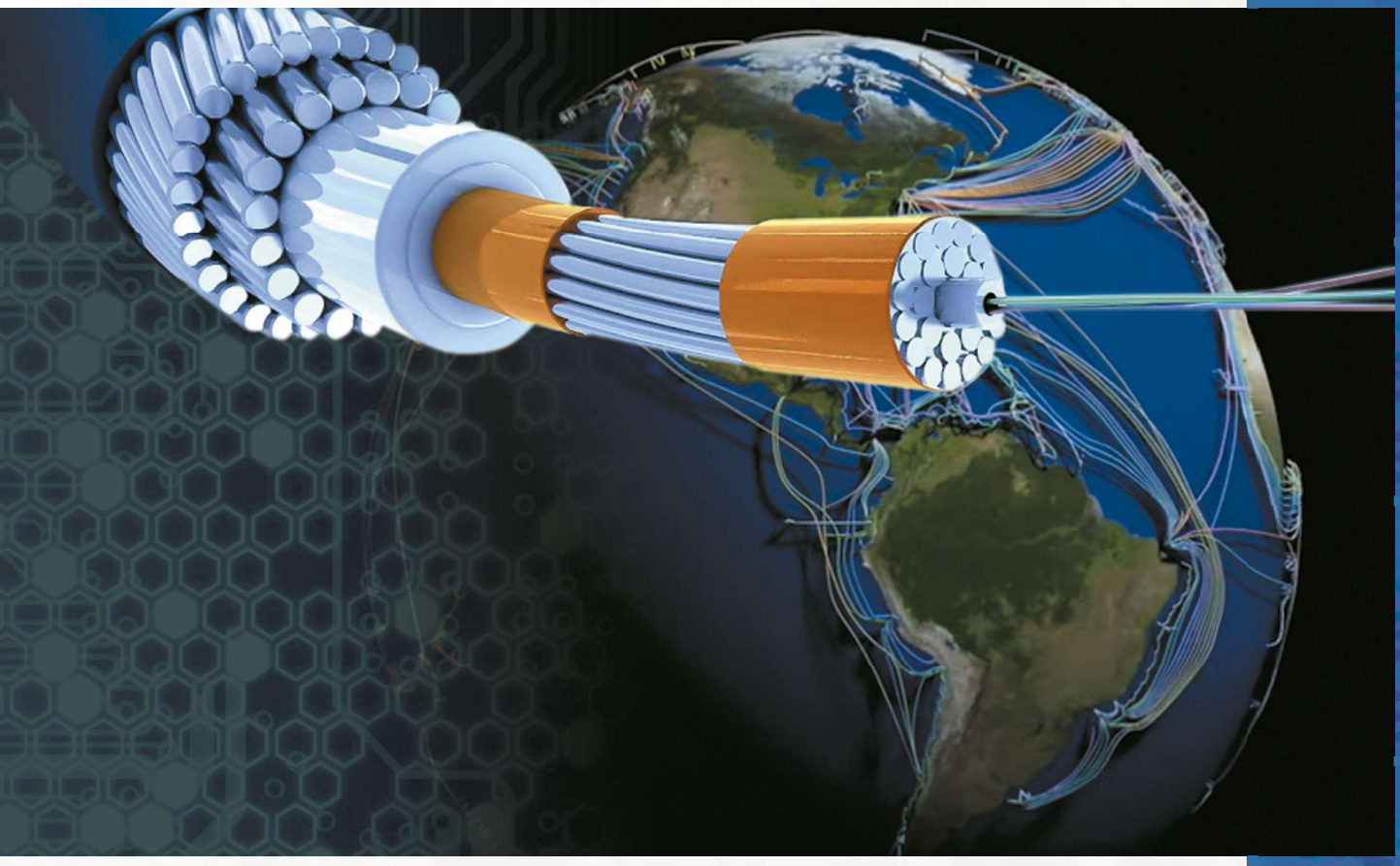
Esta investigación propone analizar la evolución e importancia de los cables submarinos, reflexionar cómo el mar se constituye como un entorno conflictivo, señalar las amenazas a esta infraestructura crítica y finalmente establecer cómo se encuentra la seguridad de los cables submarinos en el Perú. El estudio es tipo analítico-descriptivo porque se basa en un análisis de datos históricos con la finalidad de ayudar a comprender la real importancia del objeto de estudio (cables submarinos).

¿Es la red de cables submarinos un activo crítico de un estado?



The research proposes to analyze the evolution and importance of submarine cables, reflect on how the sea is constituted as a conflictive environment, establish the threats to this critical infrastructure and finally establish how the security of submarine cables is in Peru. 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).

Teniente Coronel EP Willians Osada Bazán

ORCID 0000-0001-6506-832X

Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones por la Escuela Superior de Guerra del Ejército del Perú – Escuela de Posgrado, Maestro en Educación, con mención en Docencia Universitaria e Investigación Pedagógica por la Universidad San Pedro, Bachiller en Ciencias Militares (Arma de Caballería) por la Escuela Militar de Chorrillos y Bachiller en Administración de la Universidad Nacional Federico Villareal; además, es Licenciado en Ciencias Administrativas de la Universidad Nacional de Piura. Ha sido Observador Militar en la Misión de Estabilización de la ONU en la República Democrática del Congo (MONUSCO) y ha formado parte del Batallón Contraterrorista Nº 324 – VRAEM como Ejecutivo de la unidad. Ha ejercido la docencia en la Escuela Militar de Chorrillos, Escuela Superior de Guerra del Ejército – Escuela de Posgrado y, actualmente, en la Escuela Superior Conjunta de las Fuerzas Armadas.

Osada, W. y Vargas , R. (2023). ¿Es la red de cables submarinos un activo crítico de un estado? Revista *Pensamiento Conjunto,* Año 11, pp. 44-55. ISSN° 2707-367X

Fecha de recepción: 9 de mayo de 2023
Fecha de aceptación: 11 de julio de 2023
Fecha de publicación: 12 de julio de 2023

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 COVID-19, donde 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 la red de cables se extiende 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 - Ucrania, la vulnerabilidad de las infraestructuras marítimas – en este caso la red de cables submarinos - está recibiendo cada vez más atención pública y política.

De acuerdo a lo señalado por Arellano (2022) estimó que, para el 2022 alrededor de *5 billones de usuarios (es decir, 63%de la población mundial)*[1] *emplea el ciberespacio, observando además, el crecimiento exponencial de*

1 "Las estimaciones estadísticas de la población mundial que hace uso del internet corresponden al 20 de mayo de 2022 con una distancia de 1.35 millones de kilómetros, se espera que para el año 2023 haya 486 sistemas de cable y 1.306 aterrizajes actualmente activos o en construcción de localización en la costa"; recuperado de: https://dgtlinfra.com/submarine-cables-fiber-link-internet/

PALABRAS CLAVE: ACTIVO CRÍTICO, CABLES SUBMARINOS, CIBERESPACIO, SEGURIDAD Y DEFENSA NACIONAL..
KEYWORDS: CRITICAL ASSET, SUBMARINE CABLES, CYBERSPACE, SECURITY AND NATIONAL DEFENSE.

la dependencia al internet para actividades como la educación, finanzas, comercio, geopolítica y entretenimiento; un punto importante a tener en cuenta es que *99%*[2] *de la información en el ciberespacio circula mediante la red de cables de fibra óptica distribuidos a través de la plataforma submarina mundial.* En ese sentido, *los gobiernos tienen miras en la red de cables submarinos como una infraestructura crítica que merece un alto nivel de protección* (Carter et al, 2009, citado por Arellano, 2022, p. 1)

Lo expresado por Carter demuestra la preocupación de los Estados por elevar el nivel de protección y resguardo de esta red de cables submarinos, ya que la vulneración o afectación a esta red podría traer serias consecuencias en su estructura pública, privada y en su población, teniendo además incidencia directa en las políticas de seguridad y defensa nacional.

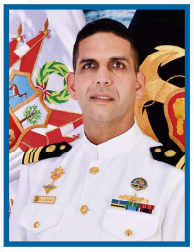
El presente artículo propone visualizar la importancia de la red de cables submarinos y la necesidad de mejorar la estrategia y capacidad actual para resguardar su integridad a fin de garantizar el desarrollo y seguridad del país y minimizar el impacto en caso fuera afectada, para lo cual planteamos la siguiente interrogante: ¿En qué medida la red de cables submarinos debe ser considerada como activo crítico de un Estado? En ese sentido, se analizó investigaciones de los últimos tres años, así como bibliotecas y fuentes especializadas digitales.

LOS CABLES SUBMARINOS: EVOLUCIÓN E IMPORTANCIA

En 1858 se realizó la primera conexión transoceánica a través de cables entre Irlanda y la isla Terranova (Canadá),[3] que permitió trasmitir un mensaje telegráfico de la reina Victoria al que fuera presidente estadounidense James Buchanan, el mensaje tardó 17 horas en ser enviado; sin embargo, significó un gran salto en las comunicaciones.

A inicios de 2023, se estima que hay 1,4 millones[4] de kilómetros de cables submarinos que se encuentran extendidos en las profundidades de los océanos, que permiten la interconexión y distribución de información de 5,160 millones[5] de usuarios en todo el mundo. El 99% de estos intercambios están representados en datos digitales, economía global y servicios digitales,

2 Recuperado de: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
3 Recuperado de: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
4 Recuperado de: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
5 Recuperado de: https://www.businessempresarial.com.pe/internet-usuarios-siguen-aumentando/



Capitán de Corbeta
Roberto Vargas Flores

Magíster en Derecho, Economía y Gestión, con mención en Relaciones Internacionales del Programa en Defensa y Dinámicas Industriales por el 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".
Licenciado en Ciencias Marítimas Navales (Comando General). 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", especializándose en "Navegación nivel Dirección" y en "Seguridad Fundamental". 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.

los cuales dependen de esta red submarina que está formada por 552 cables activos y proyectados según los datos de TeleGeography.[6]

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. 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 para los instrumentos de poder: diplomático, informacional (comunicaciones), militar y económico.

La vida social actual depende más que nunca de las conexiones a internet. Las redes sociales y los mensajes en línea ofrecen formas rápidas y eficaces de comunicarse y organizarse. En suma, diversas actividades críticas dependen cada vez más de una conexión estable y segura a internet, el sector del 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.

En el ámbito de 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. 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.

Por ello, la red de cables submarinos es la infraestructura crítica central de la era digital pues permite la accesibilidad al ciberespacio y conectividad mundial. La pérdida de comunicación durante unos minutos u horas puede tener un impacto de alta criticidad en la continuidad de operaciones sensibles y pérdidas financieras. Es en ese sentido que, por su relevancia para la economía y soberanía digital, el daño a esta infraestructura física puede constituir un riesgo a la seguridad.

En definitiva, 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, los Estados 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 mundo, considerándola como una infraestructura crítica.

EL MAR COMO ENTORNO CONFLICTIVO

En el siglo XVII, el jurista holandés Grotius[7] consideraba que el mar era un bien común de la humanidad por no ser urbanizable y, por tanto, no constituía un territorio, sino sólo una zona de tránsito. Hoy, por el contrario, 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, de manera que su importancia política y estratégica lo convierte en una de las principales razones de las rivalidades internacionales, tenden-

6 Recuperado de: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

7 "Hugo Grotius fue el creador de los conceptos de ética natural y del contrato social. En su libro de 1609 Mare Liberum promueve la idea del uso libre de las vías de comunicación marítima para el beneficio de todos". Recuperado de: https://www.juntadeandalucia.es/averroes/centros-tic/14002996/helvia/aula/archivos/repositorio/250/271/html/economia/economistas/grotius.htm

cia 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). (Wedin, 2016, pp. 70-71 et 143-144)

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.[8] 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 Arciniegas (18 de noviembre de 2022) sobre una investigación preliminar sueca en relación a las explosiones del oleoducto Nord Stream durante el año 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 línea)*

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 en la mar, de ahí las palabras del marino-novelista Monsarrat "el océano es el mejor escondite del mundo" (Monsarrat, 1999, p. 106).

AMENAZAS A LA INFRAESTRUCTURA DE LA RED DE CABLES SUBMARINOS

Como punto de partida de este párrafo, resalto lo manifestado por Bueger, Liebetrau y Franke (2022):

> *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.* (p. 9)

La primera categoría de amenaza a la infraestructura de la red de cables submarinos, son los daños accidentales causados por fenómenos naturales o por acción humana no intencionada, por ejemplo, si se llegara a producir un fenómeno natural que tenga impacto en el fondo oceánico podría provocar un daño significativo a un cable submarino. En ese sentido, Levy (2022) explica:

> *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 poblado-*

8 "Carl Schmitt fue un jurista alemán, teórico político y miembro destacado del Partido Nacionalsocialista. Schmitt escribió extensamente sobre el ejercicio efectivo del poder político". Recuperado de: https://es.wikipedia.org/wiki/Carl_Schmitt

> *res de Tonga hubieran quedado totalmente incomunicados.* (En línea)

Lo mencionado anteriormente evidencia la existencia de amenazas de causa natural que ponen en riesgo esta infraestructura crítica. Si bien los cables submarinos están delimitados en las cartas marítimas, cerca del 70% de los daños que sufren estos en el mundo son causados accidentalmente por la pesca y el fondeo, como detallan las estadísticas del Comité Internacional de Protección de Cables (ICPC).

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 (11 de febrero de 2022) recomienda a los Estados algunos principios generales basados en buenas prácticas gubernamentales:

> *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… 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 línea)

Adicionalmente, 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, disponer de sus Fuerzas Armadas para esta gestión de protección y de mantenimiento. 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 altamar 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, 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. (ONU, 1982, pp. 51 -61)

En cuanto a las zonas situadas fuera de las aguas territoriales de los Estados costeros, la CNUDM en su artículo 113, no obliga a ningún Estado a salvaguardar los cables submarinos, sino que impone a todos los Estados la obligación de adoptar normas que garanticen que los buques que enarbolen su pabellón sean castigados por destruir o dañar un cable submarino (ONU, 1982, p. 61). Sin embargo, para algunos críticos estas disposiciones "se perciben a veces como anticuadas e inadecuadas para los retos de hoy en día" (Bueger, et al., 2022, p. 9), 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.

En la segunda categoría de amenazas a la infraestructura de la red de cables submarinos, encontramos las actividades humanas intencionadas, es decir, de sabotajes a esta infraestructura, sobretodo 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.

El Tratado de Paris de 1884 - sobre la protección de los cables submarinos - tipifica sólo como delito romper o dañar un cable, por lo que se presume que permitiría a los beligerantes actuar sobre los cables de manera que esta acción podría constituir un casus belli para las partes que aún no están implicadas en el conflicto lo que podría generar una guerra mayor.

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 definir el conflicto en la zona gris como "el espacio por excelencia del *hybrid warfare*, otro *buzzword* nacido en la comunidad de defensa norteamericana, aceptado en su variante de amenaza híbrida en declaraciones oficiales de la Alianza Atlántica y de la Unión Europea" (Colom, 2018, citado por Jordán, 2018, p. 132). El conflicto en la zona gris permite el "empleo intencionado, multidimensional e integrado de diversos instrumentos de poder: políticos, económicos, sociales, informacionales, diplomáticos y también militares" (Adamsky, 2015. p. 37; Mazarr, 2015, p. 86; Freier, 2016, p. 4)

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 (Oldham, 2015; Votel et al., 2016); además "la competición estratégica entre dos o más Estados discurre por debajo del umbral de violencia política y del conflicto armado menor" (Baqués, 2017, p. 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, p. 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, el 31 de mayo de 1879, el Almirante Miguel Grau en una carta dirigida al Director de Marina, señala:

> *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.* (Cuya, R., 25 de octubre de 2017, en línea)

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:

> *A raíz de la 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. (Bueger, et al., 2022, p. 9)*

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*"[9] en el empalme final de un cable submarino que se encuentra en aguas profundas, dados los requisitos técnicos favorables que ofrece las operaciones en el mar para una actuación discreta y eficaz.

Los investigadores Pierre Morcos y Colin Wall en un artículo publicado en junio de 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

9 "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 accedes 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

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 el 2014, fuerzas del bloque de occidente viene 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 los EEUU poseen de unidades con grandes capacidades para actuar en el dominio cibernético en el fondo del mar para misiones especiales, los cuales pueden realizar diversas tareas, desde instalar dispositivos de escucha para 'pinchar' las comunicaciones de todo un país, así como para interrumpir las comunicaciones mundiales. (Contreras, 24 de octubre de 2022, en línea)

Es así que en el contexto de la Guerra de Rusia en Ucrania, el presidente de los EEUU Joe Biden, expresó su preocupación por el panorama cibernético mundial tras las sanciones que se ha impuesto a Moscú por su invasión a Ucrania,[10] advirtiendo que Rusia estaba considerando una variedad de posibles vías para realizar ciberataques, entre los 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, quedando confirmado en los sucesos del mes de setiembre de 2022, 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 provocadas "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, Estados Unidos y potencialmente otras partes del mundo. 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, al demostrar que posee la capacidad de efectuar misiones especiales en el fondo del mar para responder a las sanciones económicas impuestas por el bloque de occidente. (El Periódico.com, 15 de noviembre de 2022, en línea)*

Bajo estos conceptos, los cables submarinos podrían representar objetivos tentadores de acciones de sabotaje realizadas por una organización o Estado que desee provocar interrupciones en los sistemas de comunicación soportados por internet que tengan fines como: producir un serio impacto en la salud, seguridad o bienestar de la población o en el normal funcionamiento del gobierno o de la economía de un país. Los cables submarinos transportan gran cantidad del tráfico de datos global y son críticos para internet; sin embargo, en algunos Estados no cuentan con una protección integral.

En este contexto, se debe considerar que las amenazas sobre esta infraestructura crítica no respetan fronteras pues los países están conectados entre sí a través de numerosos cables, por lo que existen vulnerabilidades e interdependencias globales. De hecho, el corte simultáneo de varios de estos cables podría generar un gran impacto en las economías y en todas las actividades dependientes de las comunicaciones.

10 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

LA SEGURIDAD DE LOS CABLES SUBMARINOS EN EL PERÚ

Según el portal especializado *Datareportal*, con datos a febrero de 2023, consideran que en el Perú existen 24,31 millones de usuarios de internet[11] que se conectan con el mundo a través de cuatro cables submarinos que tienen puertos de amarre en territorio nacional,[12] lo que representa para el país un reto estratégico para garantizar su integridad y normal funcionamiento, debido a la dependencia al servicio de internet en todos los aspecto de la actividad nacional; 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 sólo a nivel nacional, sino también mundial.

El Plan Estratégico de Desarrollo Nacional al 2050 del Estado peruano, en el marco de riesgos y amenazas desde el entorno externo, considera que: "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 bases para fortalecer la gobernanza digital con la aprobación del Decreto Legislativo Nº 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 Nº 30999 "Ley de Ciberdefensa" que tiene como finalidad "defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y 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 ser considerados en la lista de activos críticos nacionales, por la relevancia que representan 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, generando grave perjuicio a la Nación. En este 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", se presenta las siguientes conclusiones y recomendaciones:

11 Recuperado de: https://datareportal.com/reports/digital-2023-peru

12 Mapa de cable submarino. TeleGeography. Última actualización 23 de junio de 2023. Recuperado de: https://www.submarinecablemap.com/country/peru

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 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 Transporte 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 afectar a este, y trabajar de manera asociada y coordinada con el sector privado.

2). Bajo una perspectiva de seguridad, en nuestro país, mediante Decreto Supremo N°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. Las redes de cables cumplen con los requisitos fundamentales para ser considerados como ACN: (1) Su relación con los objetivos y capacidades nacionales. (2) Su importancia para el Estado, (3) 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 estructural, accidental 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, el internet es la principal amenaza que afecta la información, por su diversidad de formas y la incidencia histórica analizada; es recomendable implementar en la organización responsabilidades claras con niveles de acceso y autoridad que permitan realizar de manera segura el intercambio de información, 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 BIBLIOGRÁFICAS

Adamsky, D. (2015). Cross-domain coercion: the current Russian art of strategy. Institut Français des Relations Internationales. Proliferation Papers, (p. 54). Recuperado de: https://bit.ly/2aUq2UN

Arciniegas, Y. (18 de noviembre de 2022). Fiscalía sueca halla signos de "sabotaje" en las explosiones de Nord Stream. Diario France24. Recuperado de: https://www.france24.com/es/europa/20221118-nord-stream-sabotaje-jerson-camara-tortura

Arellano (2022). 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.

Baqués, J. (2017). Hacia una definición del concepto «Gray Zone» (GZ), Documento de Investigación 2/2017. Instituto Español de Estudios Estratégicos. España.

Bueger, et al. (2022). Security threats to undersea communications cables and infrastructure – consequences for the EU. (p. 9)

Business Empresarial (12 de mayo de 2023). Digital Report 2023: Usuarios de internet siguen aumentando. Recuperado de: https://www.businessempresarial.com.pe/internet-usuarios-siguen-aumentando/

Carter et al. (2009). Submarine Cables and the Oceans: Connecting the World. The United Nations Environment Programme World Conservation Monitoring Centre Biodiversity Series

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

Contreras, P. (24 de octubre de 2022). La Armada controla la actividad naval de Rusia en torno a la red de cable global. Diario La Voz del Sur. Recuperado de: https://www.lavozdelsur.es/actualidad/sociedad/armada-controla-actividad-naval-rusia-en-torno-red-cable-global_284767_102.html

Cuya, R. (2017). Las Memorias de Grau. Campaña Marítima. Grau se niega a bombardear a pobladores indefensos en Antofagasta. Recuperado de: https://www.grau.pe/campana-maritima/grau-se-niega-a-bombardear-a-pobladores-indefensos-en-antofagasta/

El Periódico.com (15 de noviembre de 2022). El mensaje que podría estar enviando Rusia con el corte de cables. Recuperado de: https://www.elperiodico.com/es/internacional/20221115/mensaje-podria-enviar-rusia-corte-cables-internet-guerra-ucrania-europa-dv-77660458

Estado peruano (2018). Decreto Legislativo Nª 1412 "Ley de gobierno digital". Presidencia del Consejo de Ministros. Lima, Perú.

Estado peruano (2019). Ley Nª 30999 "Ley de Ciberdefensa". Congreso de la República. Lima, Perú.

Estado peruano (2022). Plan Estratégico de Desarrollo Nacional al 2050. Presidencia del Consejo de Ministros. Lima, Perú.

Freier, N. (2016). Outplayed: regaining strategic initiative in the gray zone. Carlisle: U. S. Army War College Press.

Grotius, H. (1609). Mare liberum.

Inlearning (2022). Piggyback o el acceso por exceso de confianza. Recuperado de: https://es.linkedin.com/learning/ingenieria-social-para-it/piggyback-o-el-acceso-por-exceso-de-confianza

Iscpc.Org (11 de febrero de 2022). Buenas prácticas gubernamentales para proteger y promover la resiliencia de los cables submarinos de telecomunicaciones. Recuperado de: file:///C:/Users/windows/Downloads/ICPC-Gov't-Best-Practices-for-Cable-Protection--Resilience-Version-1.2-(Spanish).pdf

Jordán (2018). El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo. Revista Española de Ciencia Política. Núm. 48. pp. 129-151. Recuperado

de: https://www.ugr.es/~jjordan/Conflicto-zona-gris.pdf

Kemp, S. (13 de febrero de 2023). Digital 2023: Perú. Datareportal. Recuperado de: https://datareportal.com/reports/digital-2023-peru

Kim, J. (4 de mayo de 2022). Cables submarinos: el enlace de fibra invisible que permite Internet. Recuperado de: https://dgtlinfra.com/submarine-cables-fiber-link-internet/

Levy, G. (2022). ¿Qué le pasaría a la humanidad si el servicio de internet fuera interrumpido? Recuperado de: https://andinalink.com/la-dependencia-de-la-humanidad-a-la-conectividad-submarina/#_ftnref2

Mazarr, M. (2015). Mastering the gray zone: understanding a changing era of conflict. Carlisle: U. S. Army War College Press.

Monsarrat, N. (1999). La Mer cruelle – 1951. París. (p. 106)

Morcos, P., y Wall, C. (2021). Invisible and Vital: Los cables submarinos y la seguridad transatlántica. Sitio web del CSIS.

Oldham, C. (2015). SOCOM: navigating the gray zone, Defense Media Network. Recuperado de: https://bit.ly/2yRNgUe

ONU (1982). 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

Telefónica (2022). Cables submarinos, internet bajo el agua. Recuperado de: https://www.telefonica.com/es/sala-comunicacion/blog/cables-submarinos-internet-bajo-el-agua/

Schmitt, C. (2008). Le Nomos de la Terre - 1950, Paris, PUF. (p. 48).

TeleGeography (2022). Submarine Cable Frequently Asked Questions. Recuperado de: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

TeleGeography (23 de junio de 2023). Submarine Cable Map. Recuperado de: https://www.submarinecablemap.com/country/peru

Votel, et al. (2016). Unconventional warfare in the gray zone, Joint Forces Quarterly. (pp. 80: 101-109)

Wedin, L. (2016), Stratégies maritimes au XXIe siècle, op. cit., pp. 70-71 et 143-144 http://cdigital.dgb.uanl.mx/la/1020014337/1020014337_085.pdf