LA GESTIÓN DE LOS RIESGOS CIBERNÉTICOS EN LOS SISTEMAS DE SEGURIDAD EN BUQUES Y EMPRESAS NAVIERAS

Amador CASTRO PEREIRA
Capitán de la Marina Mercante

(Reservista voluntario)

Introducción

AS tecnologías cibernéticas se han convertido en esenciales para el funcionamiento y la gestión de los numerosos sistemas cruciales para la seguridad y la protección del transporte marítimo, así como la del medio marino. En algunos casos, estos sistemas han de cumplir las normas internacionales y las prescripciones nacionales de las administraciones marítimas responsables del abanderamiento de los buques que enarbolen su pabellón en calidad de país de abanderamiento.

Las amenazas y vulnerabilidades actuales y emergentes relacionadas con la digitalización, la integración y automatización de los procedimientos y sistemas del transporte marítimo lamentablemente son ya más que una realidad y, según los analistas y expertos en seguridad, la previsión es que este tipo de amenazas y ataques cibernéticos se vayan incrementado con el tiempo y con mayor violencia. La vulnerabilidad generada por el acceso, la interconexión o el establecimiento de redes entre estos sistemas puede dar lugar a riesgos cibernéticos que deberían abordarse.

Existe una serie de sistemas marítimos o náuticos de tipo crítico y vulnerable, y entre los más comúnmente conocidos por su uso generalizado en la flota

Oficial de guardia en el puente de navegación de un buque mercante, controlando el tráfico marítimo y la seguridad de la navegación. (Fuente: internet)

civil o mercante internacional podrían ser, entre otros: el puente de mando y control del buque, los sistemas de manipulación y gestión de la carga, de propulsión y gestión de las máquinas y de control de suministro eléctrico, de vigilancia y control de acceso restringido, de servicio a los pasajeros y de organización de los mismos, las redes públicas de internet para los pasajeros, los sistemas administrativos y de bienestar de la tripulación y los de telecomunicaciones, así como otros equipos de comunicaciones radio.

Tanto la tecnología marítimo-portuaria de la información (sistemas que se centran en el uso de los datos como información) como los sistemas técnicos de tecnología operacional (uso de los datos para controlar o vigilar procesos físicos) deberían ser convenientemente protegidos, puesto que presentan riesgos para sistemas y procedimientos cruciales vinculados al funcionamiento de sistemas críticos y que son parte integral del transporte marítimo. Dichos riesgos pueden derivar de la vulnerabilidad originada por el funcionamiento, integración, mantenimiento y proyecto inadecuados de los sistemas de índole cibernética y de amenazas cibernéticas, bien sean intencionadas o no.

Las amenazas pueden aparecer mediante actuaciones malintencionadas (por ejemplo, piratería informática o introducción de programas informáticos maliciosos) o como una consecuencia no deliberada de actuaciones bien inten-

cionadas (mantenimiento de los programas informáticos o permisos de usuarios). Estas actuaciones ponen de manifiesto alguna vulnerabilidad (programas informáticos anticuados sin actualizar debidamente o barreras de control de acceso ineficaces) o bien aprovechan alguna vulnerabilidad de la tecnología operacional o de la información. Para que la gestión de los riesgos cibernéticos sea eficaz, deberían considerarse ambos tipos de amenazas en su conjunto.

La vulnerabilidad también puede derivarse de un proyecto, integración y/o mantenimiento inadecuados de los sistemas, así como de lapsus en la disciplina cibernética. En general, cuando se pone de manifiesto o se aprovecha alguna vulnerabilidad de la tecnología operacional y/o de la información, bien directamente (con contraseñas poco seguras que dan lugar a accesos no autorizados) o indirectamente (por la ausencia de segregación de las redes informáticas), puede haber implicaciones para la protección y confidencialidad e integridad y disponibilidad de la información. Asimismo, también puede haber implicaciones para la seguridad, sobre todo poniendo en peligro sistemas cruciales, como por ejemplo en la navegación en el puente o en sistemas principales de propulsión del buque.

Para que la gestión de los riesgos cibernéticos sea eficaz, también se deberían considerar las repercusiones que tienen en la seguridad y en la protección la manifestación o el aprovechamiento de la vulnerabilidad de los sistemas de tecnología de la información. La causa podría ser la conexión indebida a sistemas

Buque de carga general tipo portacontenedor realizando operaciones de carga/descarga en una terminal portuaria. (Fuente: internet)

de tecnología operacional o lapsus de procedimientos que hayan tenido el personal operacional o terceras partes que ponen en peligro dichos sistemas (el uso indebido de medios extraíbles, como un lápiz o una tarjeta de memoria del tipo USB...).

Al examinar las fuentes de posibles amenazas y vulnerabilidades, así como de las estrategias posibles para mitigar estos riesgos, las organizaciones deberían examinar varias opciones de control de la gestión de los riesgos cibernéticos. Entre estos controles posibles, mencionar los controles de la gestión, los operacionales o de procedimiento y los técnicos.

La seguridad cibernética, una exigencia urgente en el mundo marítimo según la Organización Marítima Internacional

La Organización Marítima Internacional (OMI) ha reconocido desde hace ya varios años la necesidad urgente de crear una cultura de seguridad y protección del transporte marítimo frente a la amenaza real de los riesgos cibernéticos, y ha tomado en consideración la importancia de elevar el nivel de concienciación sobre las amenazas y las vulnerabilidades conexas con los riesgos cibernéticos. Asimismo, también reconoce que la industria marítima en su totalidad, así como las administraciones públicas y las autoridades de los Estados, deberían agilizar el trabajo necesario para salvaguardar el transporte marítimo ante las amenazas y vulnerabilidades cibernéticas actuales y

Sede de la OMI en Londres. (Fuente: internet)

emergentes, y considera de vital importancia para los buques y compañías navieras que se lleve a cabo una gestión debidamente organizada de la ciberseguridad que responda a las necesidades de las personas a bordo de los buques con objeto de alcanzar y mantener un nivel elevado de seguridad y de protección del medio ambiente.

Uno de los objetivos principales del Código Internacional de Gestión de la Seguridad operacional del buque y la prevención de la contaminación (IGS) —conocido como Código ISM y que se aplica a la flota mercante internacional de acuerdo a las exigencias del Convenio Internacional para la Seguridad de la Vida en el Mar (SOLAS)— es la exigencia de establecer prácticas de seguridad en las operaciones del buque y en el medio de trabajo; evaluar todos los riesgos señalados para los buques, el personal y el medio ambiente; tomar las oportunas precauciones, y mejorar continuamente los conocimientos prácticos del personal de tierra (compañías navieras) y de a bordo sobre la gestión de la seguridad.

La OMI afirma que todo sistema de gestión de la seguridad aprobado por la correspondiente administración marítima de Estados de abanderamiento de los buques debería tener en cuenta la gestión de los riesgos cibernéticos, de conformidad con los objetivos y prescripciones del Código ISM, y alienta a las administraciones a garantizar que los riesgos cibernéticos se aborden debidamente en los sistemas de gestión de la seguridad a más tardar en la primera verificación anual del Documento de Cumplimiento (DoC) de la compañía después del 1 de enero de 2021.

International Safety Management (ISM Code). Código Internacional de la gestión operacional del buque y la empresa naviera. (Fuente: internet)

Para contar con orientaciones detalladas sobre la gestión de los riesgos cibernéticos, la industria marítima y la comunidad mercante en su conjunto deberían remitirse a las directrices de la OMI a modo de recomendaciones (MSC-FAL.1/Circ. 3, 5 de julio de 2017) y a las prescripciones de los gobiernos miembros y de las administraciones del Estado de abanderamiento, así como a las normas internacionales, normas del sector y mejores prácticas pertinentes en materia de ciberseguridad, entendiendo esta como aquella capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. Dicho de otro modo, la capacidad de resistir a un determinado ciberincidente.

Directrices de la OMI para la gestión de los riesgos cibernéticos marítimos

Estas directrices facilitan recomendaciones de alto nivel sobre la gestión de los riesgos cibernéticos para proteger el transporte marítimo, tanto de los existentes como de los emergentes. También recogen elementos funcionales para apoyar una gestión efectiva de estos riesgos.

El riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posible que podría causar fallos operacionales, de seguridad o de protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas.

(Fuente: internet)

Elementos de gestión de riesgos cibernéticos recomendados por la OMI

La gestión de los riesgos cibernéticos se refiere a todos los procedimientos elaborados y seguidos para detectar, analizar y limitar un incidente y responder ante él. Es decir, consiste en elaborar unos procesos de identificación, análisis, evaluación y comunicación de riesgos de índole cibernética y de aceptación, evitación, transferencia o mitigación de esos riesgos hasta un nivel aceptable, teniendo en cuenta los costos y las ventajas para los interesados de las actuaciones emprendidas.

El objetivo de esta gestión es contribuir a la seguridad y a la protección del transporte marítimo, operacionalmente resiliente ante los riesgos cibernéticos. La gestión eficaz de los riesgos cibernéticos debería garantizar la concienciación adecuada en todos los niveles de una organización para las funciones y responsabilidades del sistema de gestión de los riesgos cibernéticos. Dicha gestión debería empezar en el nivel de la dirección superior de la compañía naviera, que tendría que enraizar en todos los niveles de la organización la cultura de conocimiento de los riesgos cibernéticos y garantizar la existencia de un régimen englobador y flexible de gestión de los mismos que esté en funcionamiento continuo y se evalúe constantemente mediante mecanismos eficaces de retroalimentación.

Un planteamiento aceptado para conseguir esto es evaluar y comparar de forma completa las posturas vigentes y las posturas deseadas de la gestión de los riesgos cibernéticos. Gracias a esa comparación, pueden aparecer lagunas que podrían resolverse mediante la preparación de un plan de gestión de riesgos cibernéticos y vulnerabilidades detectadas, de modo que permitan a la compañía naviera y al buque aplicar del mejor modo sus recursos.

Las directrices de la OMI presentan elementos funcionales que contribuyen a la gestión efectiva de los riesgos cibernéticos. Estos no son secuenciales; todos deberían ser simultáneos y continuos en la práctica e incorporarse debidamente en un marco de gestión de los riesgos.

Elementos funcionales de gestión

— Identificar: definir las funciones y responsabilidades del personal en la gestión de los riesgos cibernéticos e identificar los sistemas, activos, datos y capacidades que, si se interrumpen, plantean riesgos para las operaciones de los buques.
— Proteger: implantar procedimientos y medidas para el control de los riesgos, así como planificación para contingencias, a fin de proteger ante cualquier suceso cibernético y garantizar la continuidad de las operaciones del transporte marítimo.

— Detectar: crear las actividades necesarias para detectar un suceso cibernético oportunamente.
— Responder: crear e implantar actividades y planes para dar resiliencia y restaurar los sistemas necesarios para las operaciones o servicios de transporte marítimo que hayan sido afectados por un suceso cibernético.
— Recuperar: determinar medidas para copiar y restaurar los sistemas cibernéticos necesarios para las operaciones de transporte marítimo que hayan sido objeto de un suceso cibernético.

Estos elementos funcionales abarcan las actividades y los resultados deseados de la gestión eficaz de los riesgos cibernéticos común a todos los sistemas cruciales que afectan a las operaciones marítimas y al intercambio de información, y constituyen un proceso continuo con mecanismos eficaces de retroalimentación.

(Fuente: internet)

Legislación europea y española en materia de ciberseguridad aplicable al sector del transporte marítimo como servicio esencial

En el ámbito europeo cabe destacar la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva o Reglamento NIS Directive (*Directive Security of Network and Information Systems*).

Su transposición al ordenamiento jurídico español se llevó a cabo mediante el Real Decreto-ley 12/2018, de 7 de septiembre. Esta norma legal regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los digitales, estableciendo mecanismos que, con una perspectiva integral, permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, y fijando un marco institucional de cooperación que facilita la coordinación de las actua-

ciones realizadas en esta materia, tanto a nivel nacional como con los países de nuestro entorno, en particular dentro de la Unión Europea.

El Real Decreto 43/2021, de 26 de enero, desarrolla el anterior, fundamentalmente en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, destacando la asignación como autoridad competente respecto al sector del transporte al Ministerio de Transportes, Movilidad y Agenda Urbana (MITMA) a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana. También impone el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales y a la gestión de incidentes de seguridad, y pormenoriza la designación de autoridades competentes en materia de seguridad de las redes y sistemas de información, desarrollando los supuestos de cooperación y coordinación entre los Equipos de Respuesta ante Emergencias Informáticas (CSIRT) de referencia, y de estos con las autoridades competentes, que se instrumentan a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. Destacar que también impone el cumplimiento de las obligaciones de seguridad por parte de los operadores de servicios esenciales, que habrán de concretarse en una declaración de aplicabilidad de medidas de seguridad suscrita por el responsable de seguridad de la información del operador y también la notificación de incidentes por parte de los operadores de servicios esenciales de los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, así como de los incidentes que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, aun cuando no hayan tenido un efecto adverso real sobre aquellos, por referencia a los niveles de impacto y peligrosidad, según sea el caso, estableciendo una instrucción nacional de notificación y gestión de ciberincidentes, procedimentando la notificación de incidentes a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes a fin de permitir el intercambio de información entre los operadores de servicios esenciales y los proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia, garantizando la confidencialidad, integridad y disponibilidad de la información. Finalmente, establece la obligación de colaboración de los operadores de servicios esenciales y los proveedores de servicios digitales con las autoridades competentes, que podrán requerir asimismo la colaboración de los CSIRT de referencia para el ejercicio de su función de supervisión, y la adopción de medidas técnicas y de organización para gestionar los riesgos para la seguridad de sus redes y sistemas de información, así como notificar los incidentes que tengan efectos perturbadores significativos en los servicios que prestan.

Equipos de respuesta a incidentes de seguridad informática CSIRT de referencia

— CCN-CERT, del Centro Criptológico Nacional, perteneciente al Centro Nacional de Inteligencia (CNI), para el ámbito del sector público y de la Administración pública.
— ESPDEF-CERT, del Mando Conjunto del Ciberespacio, para el ámbito de Defensa.
— INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, para el resto de los casos, fundamentalmente para el ámbito empresarial privado.

La Marina Mercante y la industria marítima como servicios esenciales

Entre los operadores de servicios esenciales, se encuentra el Transporte Marítimo y su cadena logística asociada (empresas navieras, buques, agentes consignatarios…); es decir, en términos generales, la Marina Mercante. Estos operadores «esenciales» están obligados desde enero de 2021 al cumplimiento de una serie de requisitos y obligaciones de seguridad, y deberán aprobar unas políticas de seguridad de las redes y sistemas de información atendiendo a los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.

Dichas políticas de seguridad considerarán, como mínimo, los siguientes aspectos:

— Análisis y gestión de riesgos.
— Gestión de riesgos de terceros o proveedores.
— Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.
— Gestión del personal y profesionalidad.
— Adquisición de productos o servicios de seguridad.
— Detección y gestión de incidentes.
— Planes de recuperación y aseguramiento de la continuidad de las operaciones.
— Mejora continua.
— Interconexión de sistemas.
— Registro de la actividad de los usuarios.

La relación de medidas adoptadas se formalizará en un documento denominado *Declaración de aplicabilidad de medidas de seguridad*, que será suscrito por el responsable de seguridad de la información designado y que

se incluirá en la política de seguridad que apruebe la dirección de la organización.

La gestión de incidentes de seguridad y la obligación de notificación de incidentes de los operadores de servicios esenciales

Los operadores de servicios esenciales designarán una persona responsable de la seguridad de la información, que ejercerá de punto de contacto y coordinación técnica con la autoridad competente y los CSIRT de referencia que le correspondan y deberá comunicar a la autoridad competente a través del CSIRT de referencia los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, considerándose a tal efecto aquellos con un nivel de impacto crítico, muy alto o alto y otros que por su nivel de peligrosidad —crítico, muy alto o alto— puedan afectar, aun cuando no hayan tenido todavía un efecto adverso real, sobre la prestación de los servicios esenciales.

Las autoridades competentes y los CSIRT de referencia proporcionarán a los operadores de servicios esenciales y a los proveedores de servicios digitales que pudieran verse afectados por dichos incidentes la información relevante para prevenir y, en su caso, resolver el incidente.

Las autoridades competentes efectuarán la supervisión del cumplimiento de obligaciones de seguridad y de notificación de incidentes mediante actuaciones de inspección, pudiendo requerir al operador de servicios esenciales la remisión de un informe de auditoría, elaborado por una entidad externa, solvente e independiente, sobre la seguridad de sus redes y sistemas de información.

Los CSIRT de referencia colaborarán con las autoridades competentes, cuando estas se lo requieran, y facilitarán asesoramiento técnico sobre la idoneidad de las medidas de seguridad adoptadas por los operadores de servicios esenciales.

GPS/AIS Spoofing, nueva arma cibernética extendida para ataque y desestabilización del sector marítimo-portuario

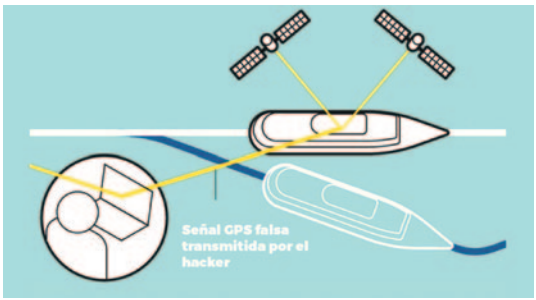
El s*poofing* se puede traducir como «hacerse pasar por otro». En términos de seguridad informática, se refiere al uso de técnicas o suplantación de identidad.

Hay barcos que están siendo víctimas de una «nueva arma misteriosa» que puede engañar a los sistemas GPS (Sistema de Posicionamiento Global) y AIS (Sistema de Identificación Automática) de una manera nunca antes vista. Nos referimos al GPS/AIS Spoofing.

La suplantación de GPS y señales identificativas AIS es un ataque en el que se utiliza un transmisor de radio ubicado cerca del objetivo para interferir con dichas señales. El atacante no transmite un dato vacío o puede transmitir coordenadas inexactas.

Si las señales GPS y AIS de un barco —utilizadas de forma generalizada para comunicar la posición del buque, rumbo y demás información de interés para la seguridad marítima de la navegación— son víctima de s*poofing*, el capitán del buque, así como las autoridades marítimas (Control del Estado Rector de Puerto o *Port State Control*, servicios SAR, aduanas, Fuerzas Armadas o Fuerzas y Cuerpos de Seguridad del Estado, etc.), creerán que el barco está en otro lugar diferente y se aumentará el riesgo de accidentes, creando un total desconcierto. Es mejor no tener información que pensar que sí la tienes pero que sea falsa.

(Fuente: internet)



Cómo falsifica un *hacker* las señales de GPS.
(Fuente: internet)

Esto no es algo puntual y empieza a ser cada vez más habitual. Nadie sabe quién está detrás de esta suplantación de identidad, ni cuál podría ser su propósito final. Estos barcos «ciberatacados» podrían ser sujetos de prueba de un sofisticado sistema de guerra electrónica o daños colaterales en un conflicto o crisis.

El problema es que actualmente los capitanes de los barcos (igual que los pilotos) se han acostumbrado a que los GPS, cartografías electrónicas tipo ECDIS o WEBDIS sean totalmente fiables y ni se plantean que no sea de esta manera.

En los Estados Unidos, el Centro de Estudios de Defensa Avanzada, con sede en Washington, ha realizado investigaciones a fondo sobre lo que está sucediendo en los últimos años. De hecho, también ha publicado información sobre GPS Spoofing por parte de Rusia en la región de Crimea, en otras partes de Europa y en Siria. La Universidad de Texas ve indicios en que gran parte de este tipo de ciberataques pudieran estar vinculados a Rusia por las semejanzas en las tácticas de desinformación, pero también admiten no tener prueba alguna que apoye sus teorías y lo certifique fehacientemente.

Aún está por resolver en gran medida el enigma, pero los expertos apuntan a una posible guerra cibernética silenciosa, que afectaría tanto a buques civiles como militares, y que veremos en el futuro qué dimensiones llegaría a tomar y si habría manera de frenarla.

Conclusiones

Según los analistas en seguridad, la previsión es que las amenazas y ataques cibernéticos se vayan incrementado con el tiempo y con mayor violencia. Expertos internacionales apuntan a una posible guerra cibernética silenciosa, que afectaría a buques civiles y militares y a infraestructuras y servicios marítimo-portuarios, tanto públicos como privados.

Existe una gran cantidad de sistemas marítimos o náuticos que son críticos y vulnerables y que deben ser protegidos en buques y empresas navieras, así como en terminales marítimas y puertos. La tecnología marítima portuaria de la información y los sistemas técnicos de tecnología operacional son parte integral del transporte marítimo.

Un ataque cibernético en el sector marítimo-portuario no solo presenta implicaciones para la protección y la confidencialidad y la integridad y la disponibilidad de la información desde el punto de vista empresarial o comercial, sino que también puede ocasionar otras mucho más graves que afecten a la seguridad marítima y de la navegación de los buques y a la integridad de las infraestructuras portuarias.

Entre las opciones de control de la gestión de los riesgos cibernéticos, hay que destacar los controles operacionales o de procedimiento y los controles técnicos.

La Organización Marítima Internacional (OMI) ha reconocido la necesidad urgente de crear una cultura de seguridad y protección del transporte marítimo frente a la amenaza real de los riesgos cibernéticos, y las administraciones públicas y las autoridades de los Estados deberían disponer lo necesario para

salvaguardarlo frente a este tipo de amenazas. Las directrices que publica la OMI para la gestión de riesgos cibernéticos facilitan recomendaciones técnicas de alto nivel para alcanzar el objetivo deseado.

Desde el 2 de enero de 2021, la OMI exige mediante la aplicación del Código Internacional de Gestión de la Seguridad Operacional (IGS) que los buques y las compañías navieras lleven a cabo prácticas y ejercicios dentro del ámbito de la seguridad cibernética y que los incluyan dentro de sus prácticas habituales de gestión de la seguridad y de la protección marítimo-portuaria. Las administraciones marítimas deberán garantizar que los riesgos cibernéticos se aborden debidamente en los sistemas de gestión de la seguridad aprobados a más tardar en la primera verificación anual del Documento de Cumplimiento de la compañía naviera (DoC) después del 1 de enero de 2021.

La gestión eficaz de los riesgos cibernéticos debería garantizar un nivel de concienciación adecuado sobre estos en todos los niveles de una organización. El grado de concienciación y preparación debe ser el adecuado para las funciones y responsabilidades del sistema de gestión de los riesgos cibernéticos.

En España, el transporte marítimo y su cadena logística asociada (empresas navieras, buques, agentes consignatarios, etc.), es decir, la Marina Mercante y el sector marítimo-portuario en su conjunto, son considerados operadores esenciales (servicios esenciales), y por imperativo legal (Real Decreto 43/2021, de 26 de enero) están obligados a llevar a cabo una gestión de incidentes de seguridad y su notificación a la autoridad competente: MITMA y CSIRT de referencia que corresponda.

La velocidad de los cambios de las tecnologías y de las amenazas dificulta el tratamiento de estos riesgos solamente mediante normas técnicas. En el sector del transporte marítimo no hay dos organizaciones que sean iguales. En el caso de los buques con sistemas de índole cibernética limitados, la simple aplicación de un sistema de gestión de procedimientos básicos de seguridad cibernética puede ser suficiente; sin embargo, los buques y compañías marítimas o grandes empresas navieras con sistemas cibernéticos complejos requerirán un mayor nivel de atención y deberían encontrar recursos adicionales a través de socios del sector reputados y del Gobierno mediante sus administraciones públicas. En este sentido, el Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Dirección General de la Marina Mercante como autoridad marítima nacional, y el Ministerio de Defensa a través de la Armada española pueden jugar un papel de vital importancia en la cooperación con la industria marítima española y, en definitiva, en la seguridad y protección de los intereses nacionales y del servicio esencial que representa la Marina Mercante y la logística e infraestructuras críticas del transporte marítimo y logística portuaria nacional.

Ataques cibernéticos «sencillos», como el GPS/AIS Spoofing, dirigidos a buques mercantes y/o militares, así como a centros de control del tráfico marítimo estatales, generan señales GPS y AIS equívocas y pueden falsear la

posición y demás información de seguridad marítima y de navegación asociadas a los buques en numerosos escenarios, pudiendo desencadenar tensiones muy graves entre países, fronteras y Estados ribereños por numerosas circunstancias. En los últimos años, se han visto afectados buques militares tanto de la OTAN como de la Unión Europea, así como diversos mercantes. España no ha permanecido al margen de este tipo de «ataques» y existen casos documentados en los que incluso se ha interesado en su investigación la propia US Coast Guard, si bien es cierto que tampoco se hace publicidad sobre ello y se trata como asuntos confidenciales, ya que evidencian que sistemas de radiocomunicaciones y navegación como el GPS y el AIS, ampliamente utilizados de forma generalizada por los buques de todo el mundo tanto civiles como militares, han sido en numerosas ocasiones vulnerados con gran facilidad y que por tanto precisan modernizarse de algún modo y corregir los fallos detectados.

Los ejercicios MARSEC de ciberseguridad marítima que lleva a cabo anualmente el Centro de Operaciones y Vigilancia de Acción Marítima (COVAM) de la Armada en colaboración con la flota civil española y la industria marítimo-portuaria en general, representan una magnífica ocasión de poner a prueba nuestros sistemas informáticos y equipos electrónicos y demás tecnologías asociadas y detectar posibles vulnerabilidades. Estos escenarios no solo deberían centrarse en la colaboración con la flota mercante y compañías navieras, sino que también deberían incluir cada vez con mayor frecuencia a la propia Administración Marítima y también a la Portuaria por el servicio esencial que prestan en España, asegurando la logística del transporte marítimo y la prestación del servicio de salvamento marítimo, etc. No podemos olvidar además que desde hace ya un tiempo hemos entrado en una nueva era, la de la Administración Electrónica, y un ataque cibernético a la misma puede ocasionar grandes perjuicios.

BIBLIOGRAFÍA

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016. Directiva NIS (*Directive on Security of Network and Information Systems*).

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Directrices OMI sobre la gestión de los riesgos cibernéticos marítimos. MSC-FAL.1/Circ. 3, 5 julio 2017.

www.imo.org

www.boe.es

www.armada.mde.es

https://encomar.covam.es

Interoperabilidad en el *Juan Carlos I*. Patrón de aeronaves tomando un helicóptero *Chinook*. (Foto: Andrés Díaz-Ripoll Marzol)