PUBLICACIÓN MENSUAL DE FORMACIÓN CONTINUA : ABRIL 2021

ANAVE
ASOCIACIÓN DE NAVIEROS ESPAÑOLES

Cuaderno Profesional Marítimo

no. 446

contenidos

Crece la preocupación en el sector por los ataques piratas en el golfo de Guinea

La seguridad marítima en el golfo de Guinea está siendo amenazada. Alrededor del 40% de los ataques piratas notificados en todo el mundo se producen en esa zona.

A escala mundial, 135 tripulantes fueron secuestrados de sus buques en 2020, siendo el golfo de Guinea la zona en la que se produjeron más del 95% de los casos, con un total de 130 tripulantes secuestrados (cifra récord) en 22 incidentes independientes.

Desde 2019, el golfo de Guinea ha experimentado un aumento sin precedentes en el número de secuestros múltiples de marinos. Los incidentes que tienen lugar en esta zona son especialmente peligrosos, ya que más del 80% de los atacantes iban armados. Los incidentes de los 3 buques secuestrados en 2020, y 9 de los 11 buques contra los que se disparó, se produjeron en esta región. El 25% de los ataques a buques en el golfo de Guinea culminó con el secuestro de marinos, más que en ninguna otra parte del mundo.

El Consejo de Ministros de la UE aprobó, el pasado 25 de enero, las conclusiones para la puesta en marcha del primer programa piloto para la 'Presencia Marítima Coordinada (PMC)' en la zona del golfo de Guinea. Muchos Estados miembros ya tienen una amplia presencia propia en el mar en zonas que son de interés para toda la Unión Europea.

Desde el pasado 4 de marzo la armada española tiene desplegado en la zona el buque de acción marítima (BAM) 'Furor'. Dinamarca se unirá a la lucha contra la piratería en el golfo de Guinea, a partir de noviembre, con el despliegue de una fragata.

Crece la preocupación en el sector por los ataques piratas en el golfo de Guinea

El Consejo de Ministros de la UE aprobó, el pasado 25 de enero, las conclusiones para la puesta en marcha del primer programa piloto para la 'Presencia Marítima Coordinada (PMC)' en la zona del golfo de Guinea. A través de las PMC la UE podrá utilizar estos medios navales y aéreos ya desplegados por los Estados miembros para aumentar su capacidad de actuar.

Alrededor del 40% de los ataques piratas notificados en todo el mundo se producen en el golfo de Guinea.

La seguridad marítima en el golfo de Guinea está siendo amenazada. Alrededor del 40% de los ataques piratas notificados en todo el mundo se producen en esa zona.

A escala mundial, 135 tripulantes fueron secuestrados de sus buques durante 2020, siendo el golfo de Guinea la zona en la que se produjeron más del 95% de los casos, con un total de 130 tripulantes secuestrados (cifra récord) en 22 incidentes independientes.

Desde 2019, el golfo de Guinea ha experimentado un aumento sin precedentes en el número de secuestros múltiples de marinos.

Los incidentes que tienen lugar en esta zona son especialmente peligrosos, ya que más del 80% de los atacantes iban armados. Los incidentes de los 3 buques secuestrados en 2020, y 9 de los 11 buques contra los que se disparó, se produjeron en esta región.

El 25% de los ataques a buques en el golfo de Guinea culminó con el secuestro de marinos, más que en ninguna otra parte del mundo.

En el golfo de Guinea, cualquier tipo de buque puede ser atacado. En los últimos meses, los casos en los que los piratas consiguieron embarcar con éxito incluyen incluso buques que estaban navegando y cuyo francobordo resultaba considerable. Además, aunque es más probable que los ataques se produzcan cerca del delta del Níger, la amenaza se ha extendido y afecta a diversos países desde Ghana hasta Gabón.

Un reciente informe de *Risk Intelligence*, empresa especializada en evaluación y planificación de riesgos en la mar, en puerto y en tierra, analiza tres aspectos que los armadores deben tener en cuenta en cualquier tipo de operación que se lleve a cabo en el golfo de Guinea: la propagación de los ataques por toda la zona; las diferencias entre los ataques diurnos y nocturnos; y la creciente preocupación entre la gente de mar.

Según *Risk Intelligence*, entre 2016 y mediados de 2019, casi todos los incidentes, con éxito y fallidos, se produjeron relativamente cerca del Sur y Oeste del delta del Níger. Durante el último trimestre de 2019, la distancia media de los ataques desde el delta del Níger aumentó significativamente, mientras que, en 2020, los ataques tuvieron lugar tanto cerca de Nigeria como a distancias significativas de la costa del delta del Níger, afectando a varios países desde Togo hasta Gabón. El informe señala que «*la tendencia más preocupante para los buques mercantes en el golfo de Guinea ha sido la propagación de ataques a una zona más amplia*».

Además, no es la primera vez que grupos criminales de Nigeria llevan a cabo operaciones en todo el golfo de Guinea. Se han observado patrones similares entre 2010 y 2016. Al mismo tiempo, los grupos de piratas asentados en el delta del Níger siguen perpetrando ataques contra buques con el objetivo de secuestrar marinos.

ATAQUES NOCTURNOS

Los ataques con el objetivo de secuestrar a marinos pueden ocurrir en cualquier momento, aunque es mucho más probable que tengan éxito durante las horas de oscuridad.

Además, se sospecha que al menos algunos de los ataques que tuvieron éxito durante el día estuvieran vinculados con otras actividades ilícitas y que los respectivos buques no fueran seleccionados de forma aleatoria.

El mayor índice de éxito durante la noche se puede atribuir, en gran medida, al hecho de que durante el día es más probable detectar el ataque con tiempo suficiente y reaccionar a posibles lanchas rápidas hostiles, dando margen a los buques para aumentar la velocidad y efectuar maniobras de evasión,

o a los miembros de la tripulación reunirse en la ciudadela a la espera de una respuesta militar naval.

LA GENTE DE MAR ESTÁ PREOCUPADA

En los últimos dos años, ha aumentado significativamente el número de informes sobre actividades que se han considerado como sospechosas.

«*Esto es un indicio claro de que las tripulaciones de los buques mercantes que operan en la región están cada vez más preocupadas por posibles ataques*», dice *Risk Intelligence.*

Muchos de los incidentes denunciados estaban relacionados con patrones normales de vida en la región, por ejemplo, con actividades habituales de pesca.

Estos casos no se registraron como incidentes en el sistema de *Risk Intelligence* y, por lo tanto, no se incluyen en el gráfico 'Incidentes sospechosos'. Sin embargo, incluso esos informes ponen de relieve la ansiedad entre la gente de mar, especialmente entre aquellos que pueden no estar familiarizados con las operaciones en el golfo de Guinea.

ESPAÑA FORMA PARTE DE LA PRESENCIA MARÍTIMA COORDINADA (PMC) EN EL GOLFO DE GUINEA

El Consejo de Ministros de la UE aprobó, el pasado 25 de enero, las conclusiones para la puesta en marcha del primer programa piloto para la 'Presencia Marítima Coordinada (PMC)' en la zona del golfo de Guinea. El concepto de PMC se ha estado desarrollando durante más de un año y busca promover el intercambio de información sobre seguridad marítima en la región y coordinar la acción de los activos de los Estados miembros de la UE (navales u otros).

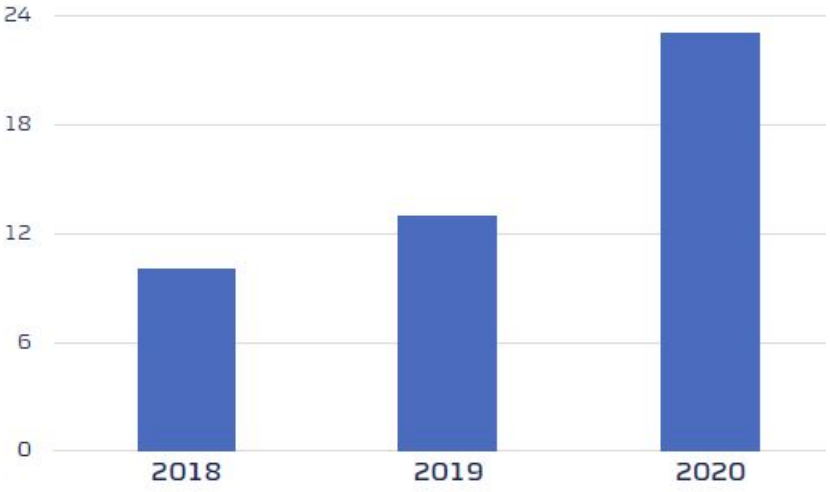
¿En qué consiste este nuevo concepto de PMC? Según informa el Servicio Europeo de Acción Exterior (SEAE) en su página *web*, dependiendo de la situación, el despliegue de una nueva operación naval de la UE desde cero puede no ser la única opción para solucionar un problema concreto, y a veces tampoco es necesariamente la más adecuada.

Muchos Estados miembros ya tienen una amplia presencia propia en el mar en zonas que son de interés para toda la Unión Europea. Estos medios navales de los Estados miembros de la UE están presentes todo el año en todas las zonas marítimas del mundo.

A través de las PMC la UE podrá utilizar estos medios navales y aéreos ya desplegados por los Estados miembros para aumentar su capacidad de actuar. La coordinación tendrá lugar de forma voluntaria, y los medios quedarán bajo las respectivas cadenas de mando nacionales.

Los Estados miembros de la UE que ya están presentes en la zona, entre ellos España (también Francia, Italia y Portugal), proporcionarán los medios navales y aéreos para apoyar el proyecto.

Desde el pasado 5 de marzo la armada española tiene desplegado en la zona el buque de acción marítima (BAM) 'Furor', cuya imagen se ve en la parte inferior de la página.



Incidentes sospechosos registrados en África Occidental. Fuente: Risk Intellingence.

DINAMARCA DESPLEGARÁ EL PRÓXIMO NOVIEMBRE UNA FRAGATA EN EL GOLFO DE GUINEA PARA LUCHAR CONTRA LA PIRATERÍA

El 18 de marzo, el Ministro de Defensa danés, Trine Bramsen anunció que Dinamarca se unirá a la lucha contra la piratería en el golfo de Guinea, a partir de principios de noviembre, con el despliegue de una fragata equipada con un helicóptero *Seahawk* que será capaz de desplegar Fuerzas de Operación Especiales, si es necesario. Las Fuerzas de Operación están especialmente entrenadas para ejecutar operaciones de rescate en buques que capturan a otros buques, entre otras.

Bramsen ha declarado que «*ni podemos ni debemos subestimar la gravedad de la situación. Debemos defender el derecho a la libre navegación*».

DIRECTRICES SOBRE EL USO DE LAS FUERZAS DE PROTECCIÓN MARÍTIMAS DESPLEGADAS POR EL GOBIERNO DE NIGERIA

El 18 de febrero de 2021, *Risk Intelligence*, publicó un conjunto de pautas sobre el uso de las fuerzas de protección privadas contratadas por el gobierno en Nigeria. El objetivo de estas directrices es aclarar el uso de la seguridad armada (buques escolta armados) en aguas de Nigeria.

El uso de guardias armados en buques mercantes, según la compañía de seguros marítimos *Skuld Club*, está prohibido en Nigeria desde el 6 de junio de 2016.

Desde 2012, la Armada de este país mantiene relaciones contractuales con empresas de seguridad privada, que se han regido por un *Memorandum of Understanding* (MoU) que ha sido revisado completa-

La información incluida en la presente publicación procede de las mejores fuentes disponibles. No obstante, ANAVE declina cualquier responsabilidad por los errores u omisiones que las mismas puedan tener.

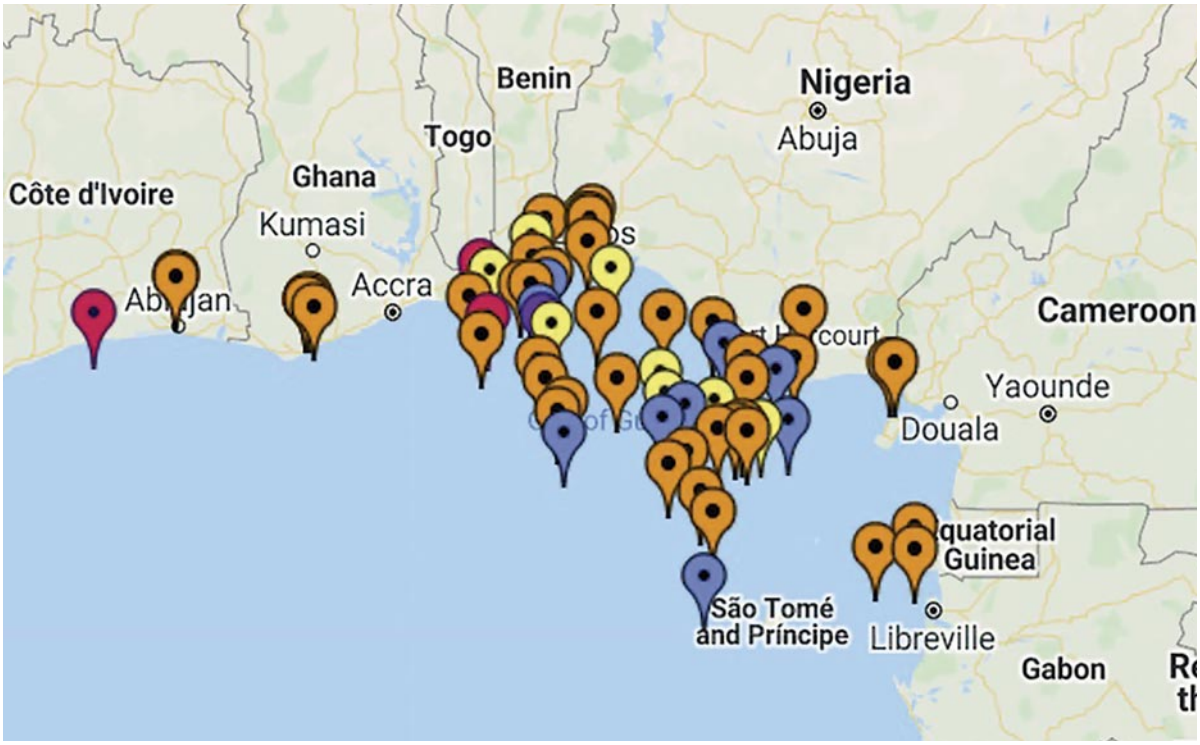
mente en dos ocasiones dureante los años 2016 y 2019. El número de empresas de seguridad marítima privada que actúan bajo este MoU asciende a unas 30. Las directrices destacan las siguientes cuestiones:

1. La armada nigeriana y la Agencia de Administración y Seguridad Marítima de Nigeria (*Nigerian Maritime Administration and Safety Agency*, NIMASA) son las únicas organizaciones que están facultadas para mantener la seguridad y protección en las aguas territoriales y en la Zona Económica Exclusiva (ZEE) de Nigeria.
2. La jurisdicción de la Policía Marítima de Nigeria está restringida a la protección de los puertos y vías navegables (zona interior de las boyas de señalización de los canales navegables).
3. La Ley NIMASA (NIMASA *Act*) faculta a dicho organismo a contratar empresas privadas o llegar a otros acuerdos con ellas para prestar servicios específicos relacionados con la seguridad y protección de buques en las aguas territoriales y la ZEE de Nigeria.
4. Salvo los acuerdos firmados entre la propia armada nigeriana y las empresas de seguridad privada en virtud del MoU, NIMASA considera una infracción que un buque navegue por las aguas territoriales de Nigeria con cualquier persona a bordo (ya sea ciudadano nigeriano o extranjero) descrita como guardia de seguridad con funciones de experto en seguridad o asesor del equipo del puente (esté o no armado).
5. El buque infractor podría ser objeto de una investigación y puede ser detenido por las autoridades nigerianas.
6. Las sanciones por incumplimiento incluyen la confiscación de cualquier artículo o propiedad y, en caso de ser condenado, el infractor será responsable del pago de una multa de 1 millón de nairas (unos 2.600 $) o podrá ser encarcelado durante un periodo de hasta 12 meses, o ambas.

Risk Intelligence aconseja que cuando se contraten Empresas Privadas de Apoyo Logístico Marítimo (*Private Maritime Logistics Support Companies*, PMLSCs) en el marco del MoU para la prestación de servicios de seguridad marítima, las empresas confirmen:

- El cumplimiento de la PMLSC con el MoU publicado en 2019.
- El cumplimiento de la PMLSC con otras normas (según lo estipulado en el MoU), especialmente la normativa de la empresa, laboral, de inmigración (para el personal extranjero) y la legislación sobre cabotaje (para los buques de escolta contratados).
- Buques de escolta adecuados y debidamente armados, capaces de disuadir a los atacantes nigerianos en alta mar (en particular, con armas montadas en los buques de seguridad).
- Los certificados de la armada nigeriana para el buque(s) de seguridad.
- Si un no titular del MoU forma parte de la operación, es necesaria una aprobación por escrito de la armada nigeriana.
- Que las PMLSC cuenta con procedimientos operativos estándar para tratar la compleja cuestión del mando y control táctico/operacional compartido con la armada nigeriana, así como la resolución de conflictos entre las Reglas de las PMLSC sobre el Uso de la fuerza (*Rules for the Use of Force*, RUF) y las Reglas de intervención de la armada nigeriana (que siempre prevalecen sobre las RUF).
- Plan de contingencia en caso de avería del buque escolta o reasignación de personal por la armada nigeriana.
- Cobertura de seguro adecuada.

La armada nigeriana ha informado de que hará pruebas de COVID-19 a sus guardas armados.



Mapa del centro de información IMB de piratería y robos a mano armada de 2020 que muestra los intentos de ataque, buques disparados, secuestros, abordajes e incidentes sospechosos en el golfo de Guinea

Cuarta versión de las Directrices sobre ciberseguridad a bordo de buques

Como principal novedad, esta versión incluye una sección con orientaciones revisadas sobre el concepto y la gestión del riesgo.

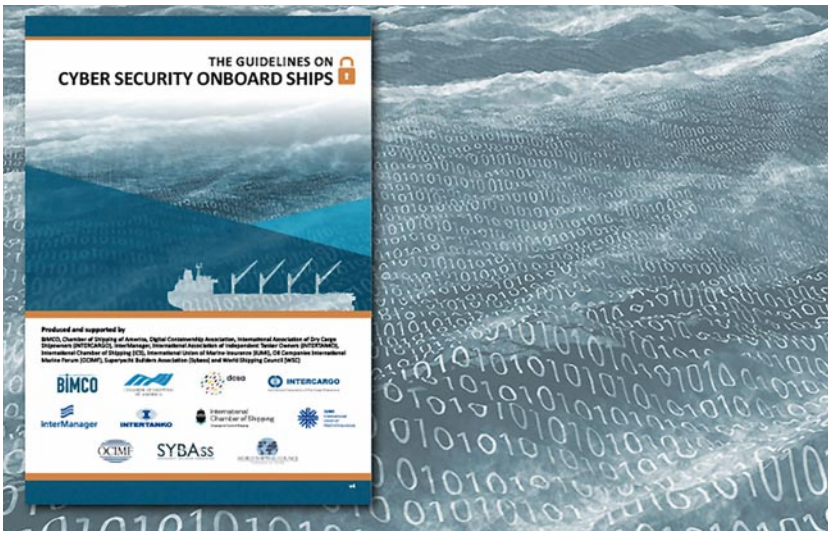
A finales de enero las principales organizaciones marítimas internacionales (entre ellas, ICS, BIMCO, INTERTANKO, INTERCARGO, OCIMF, et.) publicaron la 4ª versión de las Directrices sobre ciberseguridad a bordo de los buques. El texto completo de 64 páginas se puede descargar en el siguiente enlace:
https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Esta 4ª versión contiene actualizaciones generales de las mejores prácticas en la gestión del riesgo cibernético y, como principal novedad, incluye una sección con orientaciones revisadas sobre el concepto y la gestión del riesgo. Se resumen a continuación las principales novedades.

CARACTERÍSTICAS DE CIBERSEGURIDAD DEL SECTOR MARÍTIMO

El sector marítimo presenta una amplia gama de características que afectan a su vulnerabilidad frente a los ciberataques, entre las que se incluyen:

— La existencia de múltiples actores involucrados en la explotación y fletamento de un buque, lo que podría dar lugar a una falta de concreción y definición de la responsabilidad sobre los sistemas de tecnologías de la información (IT) y de la operación (OT) y las redes del buque.
— Uso de sistemas de IT y OT que ya no son compatibles y/o que dependen de sistemas operativos obsoletos.
— Uso de sistemas de OT que no pueden ser actualizados o funcionar con un antivirus debido a problemas de homologación.
— Buques que interrelacionan de forma virtual con tierra y otras partes interesadas en la cadena de suministro mundial.
— Equipos del buque que se controlan y a los que se accede a distancia, por ejemplo, por los fabricantes o los proveedores de asistencia.
— El intercambio de información crítica de la empresa, datos e información comercialmente sensible con los proveedores de servicios en tierra, incluidas las terminales marítimas, estibadores y autoridades.
— La disponibilidad y el uso de sistemas críticos para la seguridad del buque y protección del medio ambiente controlados por ordenador, sistemas que pueden no tener instaladas las últimas actualizaciones o estar adecuadamente protegidos.
— Una cultura de gestión del riesgo cibernético que aún tiene potencial de mejora, por ejemplo, mediante una formación más reglada, ejercicios, funciones y responsabilidades más claras.



Cuarta versión de las Directrices sobre Ciberseguridad

— Con frecuencia, el sistema de automatización comprende múltiples subsistemas de numerosos proveedores que han sido integrados en los astilleros sin dar importancia a las cuestiones de ciberseguridad.

Estos elementos deben tenerse en cuenta e incorporarse en las políticas de ciberseguridad de la empresa y en el Sistema de Gestión de la Seguridad (SGS).

El creciente uso de análisis de datos exhaustivos, buques inteligentes y el 'Internet industrial de las cosas' (*Industrial Internet of Things*, IIoT) aumentará la cantidad de información disponible y la capacidad potencial de ataque de los cibercriminales.

La gestión del riesgo cibernético debe ser parte inherente de la cultura de seguridad y protección de la compañía, favorecer la operación segura y eficiente del buque y aplicarse a diferentes niveles, incluidos los altos directivos en tierra y el personal a bordo.

PARTICIPACIÓN DEL PERSONAL DE DIRECCIÓN DE LA COMPAÑÍA EN LA CIBERSEGURIDAD

La gestión del riesgo cibernético debe implicar de forma permanente al personal de dirección de una compañía, en lugar de, por ejemplo, sólo al oficial de protección del buque o al responsable de la gestión de tecnologías de la información. Hay varias razones para ello:

— Algunos riesgos cibernéticos tienen gran potencial destructivo, y amenazan la seguridad del personal y el medio ambiente, así como el funcionamiento y reputación de la empresa. Los

riesgos cibernéticos son un desafío empresarial que requiere de la implicación de la dirección.
— Las iniciativas para mejorar la seguridad y protección cibernética pueden afectar a los procedimientos y operaciones comerciales estándar, haciéndolas más lentas y/o costosas. Por lo tanto, es una decisión de la dirección evaluar y asignar los recursos necesarios para establecer una reducción del riesgo hasta un nivel aceptable de riesgo residual.
— Las iniciativas que aumentan la conciencia cibernética pueden cambiar la forma en que la compañía interactúa con los sindicatos, clientes, proveedores y autoridades, e imponer nuevos requisitos a la cooperación entre las partes. Es una decisión de la dirección impulsar estos cambios e implementarlos de la mejor forma.

Las respuestas a las siguientes preguntas se pueden usar como base para informar e implicar a la dirección sobre la importancia de abordar los riesgos cibernéticos a bordo de los buques:
— ¿Qué activos están en riesgo?
— ¿Cuál es el impacto potencial de un incidente cibernético para la compañía, clientes, socios y partes interesadas?
— ¿Quién tiene la responsabilidad final de la gestión del riesgo cibernético?
— ¿Están protegidos los sistemas OT frente a accesos no autorizados y modificaciones?
— ¿Hay acceso remoto a los sistemas OT? Y si es así, ¿cómo se vigila y protege?
— ¿Están protegidos los sistemas IT y se gestiona el acceso a ellos?
— ¿Cuáles son las mejores prácticas de gestión del riesgo cibernético que se están aplicando?
— ¿Cuál es el nivel de formación sobre riesgos cibernéticos del personal que opera los sistemas IT y OT?

Sobre la base de las respuestas obtenidas, la compañía debe describir y delegar la autoridad según corresponda y asignar los recursos necesarios para desarrollar y mantener soluciones adecuadas basadas en los resultados obtenidos en la evaluación de riesgos.

PLANES Y PROCEDIMIENTOS

En la reunión 101º del Comité de Seguridad Marítima de la OMI, celebrada en julio de 2019, se «*acordó que las cuestiones relacionadas con la gestión de los riesgos cibernéticos, incluidos los aspectos referidos a la protección física de la ciberseguridad, deberían incluirse en los planes de protección de los buques previstos en el Código PBIP; no obstante, no debería considerarse que se exige con ello que las compañías establezcan un sistema de gestión de la ciberseguridad aparte que funcione en paralelo con el SGS de la compañía*».

En la misma reunión, la OMI también «*...confirmó que en la Resolución MSC.428(98) sobre 'Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad' se establecen las prescripciones de la OMI por las que las Administraciones deben asegurarse que los riesgos cibernéticos se abordan debidamente en los SGS vigentes, verificándolo mediante el refrendo del Documento de Cumplimiento y un Certificado de Gestión de la Seguridad de la compañía, y que en los planes de protección del buque se debería hacer referencia a los procedimientos de gestión de los riesgos cibernéticos de los SGS*».

Para una compañía, una forma sencilla de organizar los procedimientos exigidos por la OMI podría ser reflejar en el SSP lo siguiente:
— Procedimientos relacionados con el acceso físico a zonas con sistemas IT y OT.
— Una referencia a los procedimientos sobre ciberseguridad del SGS. Debe tenerse en cuenta la redacción de la referencia de manera que no haya que actualizarla cada vez que se modifique, añada o suprima un procedimiento relacionado con la seguridad cibernética en el SGS, ya que los cambios en el SPS normalmente requieren la aprobación del Estado de bandera o de la Organización Reconocida autorizada para ello por el Estado de bandera.

Por tanto, los procedimientos restantes sobre la gestión de los riesgos cibernéticos deben reflejarse en el SGS, excluyendo al mismo tiempo la información sensible, por ejemplo, la documentación del sistema descrita en la sección 3.2 de las directrices (documentación de los sistemas IT y OT) que podría ser aprovechada por agentes maliciosos ajenos a la compañía.

CUANTIFICAR LA AMENAZA

La amenaza es el resultado de la capacidad, oportunidad e intención de causar daño. El propósito de cuantificar la amenaza es ayudar a medir probabilidad y el impacto, lo que forma parte de la evaluación del riesgo. En otras palabras, si la capacidad, oportunidad o intención de un agente malicioso es cero o casi cero, la amenaza y por lo tanto el riesgo será pequeño.

Amenazas contra los sistemas OT

A diferencia de otros ámbitos de la seguridad y la protección, en los que se dispone de pruebas históricas, la gestión de los riesgos cibernéticos resulta más difícil debido a la escasez de estadísticas sobre incidentes y su impacto. Hay indicios de que los ataques dirigidos específicamente contra los sistemas OT son menos comunes y, en muchos casos, no se divulgan, debido a:
— La mayoría de los sistemas OT en el sector marítimo todavía no están conectados a redes con acceso externo, es decir, la exposición a amenazas es baja y los ciberdelincuentes no tienen oportunidad de atacar. No obstante, hay excepciones, por ejemplo, muchos dispositivos de control (por ejemplo, los de control de funcionamiento del motor) están conectados a internet y por lo general tienen instaladas medidas de protección cibernética mínimas, especialmente en comparación con los sistemas IT. Estos sistemas se conocen como el 'Internet Industrial de las Cosas' (*Industrial Internet of Things*, IIoT) y están cada vez más integrados a bordo para proporcionar control remoto y conexión de sistemas para permitir una mayor automatización y eficiencia en las operaciones. Los agentes maliciosos pueden escanear estos sistemas y usarlos como punto inicial de infiltración a una red del buque, desde la cual pueden acceder a otros sistemas. Por lo tanto, es importante evaluar este riesgo.

— Los sistemas OT normalmente no tienen potencial directo para recompensar económicamente al cibercriminal.
— Los ataques a los sistemas OT conllevan riesgos de seguridad para las víctimas, algo que puede constituir un factor que desincentive a algunos ciberdelincuentes.

A pesar de lo anterior, los riesgos de los sistemas OT no se deben subestimar. Las amenazas planteadas, por ejemplo, por el *malware* introducido a través de actualizaciones del *software* -ya sea online o a través de procesos manuales como por ejemplo memorias USB- o mediante el acceso no regulado o no autorizado por la tripulación todavía pueden materializarse y se sabe que causan interrupciones y retrasos operacionales.

Amenazas contra los sistemas IT

Las amenazas contra los sistemas IT son generalmente más fáciles de cuantificar porque hay muchas más pruebas en relación con los incidentes. Además, la interrupción de los sistemas IT no se considera que pueda dar lugar a un daño a personas, el medio ambiente, los bienes o la carga. Sin embargo, las amenazas contra los sistemas IT no deben subestimarse.

Ejemplos recientes de casos en líneas regulares han demostrado que los incidentes cibernéticos pueden causar estragos en las operaciones de los buques y en la gestión de la carga, causando importantes pérdidas económicas. Además, también pueden tener consecuencias en cascada para la seguridad de las personas, el medio ambiente, los bienes y la carga, por ejemplo, cuando las perturbaciones de los sistemas IT dan lugar a una falta de control de la carga perecedera o de las mercancías peligrosas.

IDENTIFICAR LOS PUNTOS DÉBILES

El objetivo de llevar a cabo una evaluación de la red del buque y de sus sistemas y dispositivos es identificar las vulnerabilidades que, en un momento dado, puedan comprometer o provocar la pérdida de confidencialidad, integridad o disponibilidad de los datos y sistemas necesarios para el funcionamiento de los equipos, sistemas, redes, o incluso del propio buque.

Estas vulnerabilidades y debilidades podrían clasificarse en una de las siguientes categorías:
— Exposiciones temporales debidas a defectos de software o sistemas desactualizados.
— Falta de gestión del acceso o interconexiones de red no gestionadas.
— Errores de implantación, por ejemplo, cortafuegos (*firewalls*) mal configurados.
— Errores de procedimiento o del usuario.

Los sistemas a bordo son equipos potencialmente vulnerables, que deben revisarse durante la evaluación. La evaluación de la vulnerabilidad puede ser apoyada contestando las siguientes preguntas para cada sistema:
— ¿El sistema es independiente o está conectado a otros sistemas?
— ¿El sistema está conectado al exterior, ya sea directamente o a través de otros sistemas?
— ¿Cuenta con medidas de mitigación de riesgos integradas y eficaces, como por ejemplo la codificación?
— ¿Requiere actualizaciones periódicas de *software*?
— ¿El funcionamiento del sistema implica conectar dispositivos extraíbles, por ejemplo, para obtener información de diagnóstico?
— ¿El sistema es de fácil acceso físico?

Interfaz buque-tierra

Los buques se están integrando cada vez más con las operaciones en tierra porque la comunicación digital se usa para llevar a cabo negocios, gestionar operaciones y mantener contacto con las oficinas centrales. Además, los sistemas críticos del buque, esenciales para la seguridad de la navegación, la energía eléctrica y la gestión de la carga, se han digitalizado y conectado cada vez más a internet para desempeñar una gran variedad de funciones legítimas, como:
— Supervisión del rendimiento del motor.
— Diagnósticos a distancia/remoto.
— Mantenimiento y gestión de piezas de repuesto.
— Seguimiento y gestión de la carga y de los contenedores, operaciones de carga y descarga, y planificación de la estiba.
— Manipulación de las grúas y bombas.
— Supervisión de los sistemas de cumplimiento de la normativa medioambiental y presentación de informes.
— Supervisión del desarrollo del viaje.

La lista anterior proporciona ejemplos de esta interfaz y no es exhaustiva. Los sistemas anteriores contienen, procesan e intercambian datos, que pueden ser de interés para que los ciberdelincuentes los exploten.

Las tecnologías modernas pueden añadir vulnerabilidades a los buques, especialmente si los diseños de las redes no son seguros y no se controla el acceso a internet. Además, el personal de tierra y a bordo puede no saber cómo los fabricantes y proveedores de *software* mantienen el acceso remoto a los equipos del buque y a su sistema de red. El acceso remoto a un buque en operación debe tenerse en cuenta como una parte importante de la evaluación de riesgo.

Se recomienda que las empresas comprendan y documenten plenamente, según proceda, los sistemas de OT e IT del buque y la forma en que estos sistemas se conectan e integran con tierra, incluidas las autoridades, las terminales marítimas y los estibadores. Esto requiere de una comprensión previa de todos los sistemas informáticos a bordo y cómo la seguridad, las operaciones y el negocio, incluyendo la gestión de la mercancía y carga, pueden verse comprometidos por un incidente cibernético.

Visitas al buque

Las visitas a buques por terceros que requieran una conexión a uno o más ordenadores también pueden dar lugar a la conexión del buque a tierra. Algunos técnicos pueden necesitar medios extraíbles para actualizar los ordenadores, descargar datos y/o efectuar otras tareas. A veces no hay control de quien tiene acceso a los sistemas de a bordo, por ejemplo, durante las varadas en dique seco, en buques inactivos o al hacerse cargo de un buque nuevo o existente. En tales casos, es difícil saber si se ha quedado algún *software* malicioso instalado en los sistemas de a bordo.

Se recomienda eliminar los datos sensibles y reestablecerlos al regresar al buque, y al menos debería haber una copia de seguridad de los mismos. Siempre que sea posible, los sistemas deben ser escaneados en busca de *malware* antes de su uso.

CUANTIFICAR LA PROBABILIDAD

Hay una tendencia a evaluar los riesgos por sí solos sobre la base de los posibles efectos y las vulnerabilidades existentes. Sin embargo, la probabilidad de que ocurra un incidente de ciberseguridad es el resultado de la amenaza y la vulnerabilidad. Esto también significa que, si alguno de estos dos factores es prácticamente inexistente, también lo será la probabilidad.

El SGS de una compañía normalmente contiene una matriz de evaluación del riesgo donde la probabilidad de un acontecimiento determinado se mide en una escala de 5 niveles. El uso de la escala de probabilidad existente del SGS permite usar un lenguaje y conceptos ya existentes y facilitará la comprensión en toda la compañía. Es fundamental contar con una estrategia y una comprensión armonizada de la gestión del riesgo de la compañía basada en los resultados de la evaluación del riesgo. Se muestra a continuación un ejemplo de dicha escala:

Nivel	Descripción de la probabilidad
1	Nunca se ha oído hablar de ellos en el sector. Cerca de ser algo inimaginable.
2	Se ha oído hablar de ello anteriormente en el sector, pero muy raramente y como resultado de una cadena de acontecimientos desafortunados.
3	El incidente ha ocurrido probablemente en la propia compañía, pero en el contexto de equipos defectuosos o por errores humanos inesperados.
4	Ocurre ocasionalmente en la propia compañía, normalmente por equipos defectuosos o por errores de las personas involucradas (el tipo de errores que suelen ocurrir a bordo de vez en cuando).
5	Sucede con frecuencia al llevar a cabo el trabajo en cuestión.

CUANTIFICAR EL IMPACTO

Asimismo, el impacto que tiene un determinado acontecimiento en la compañía también se mide en una escala de 5 niveles en función de su gravedad para, por ejemplo, la seguridad del personal, del medio ambiente, de la carga, los bienes, la continuidad del negocio, el impacto económico y la reputación de la compañía. Si esta escala no se ha usado para describir los impactos derivados de los riesgos cibernéticos, puede ser necesaria su modificación. El uso de dicha escala también permite a la compañía distinguir entre los distintos buques de la flota en función de su importancia crítica para el conjunto de actividades de la compañía. Se muestra a continuación un ejemplo de esa escala:

Nivel	Descripción del impacto
1	Ningún efecto/lesiones para la salud. Ningún daño al medio ambiente, bienes, economía o reputación de la compañía.
2	Efectos/lesiones muy leves en la salud. Daños muy leves en el medio ambiente, bienes, economía o reputación de la compañía.
3	Algún efecto para la salud/lesiones menores. Daños menores al medio ambiente, bienes, economía o reputación de la compañía.
4	Efectos importantes para la salud/lesiones relativamente graves. Daños locales pero importantes al medio ambiente, bienes, economía o reputación de la compañía.
5	Daños fatales o discapacidades permanentes. Daños generalizados y significativos al medio ambiente, bienes, economía o reputación de la compañía.

RESPONDER Y RECUPERARSE DE INCIDENTES DE SEGURIDAD CIBERNÉTICA

El punto de partida para una respuesta eficaz es el plan que abarca las contingencias pertinentes.

Para la mayoría de los buques, los planes de contingencia ya están incluidos en los procedimientos de emergencia exigidos en la sección 1.4.5 del Código ISM.

Los incidentes cibernéticos requerirán una respuesta activa para que el buque vuelva a estar operativo. Si, por ejemplo, el ECDIS ha sido infectado con un *malware*, iniciar la copia de seguridad del ECDIS puede causar otro incidente cibernético. Por lo tanto, se recomienda elaborar y ensayar un plan de respuesta a incidentes, detallando las funciones y responsabilidades, las vías de comunicación y las actividades principales. Puede haber ocasiones en que responder a un incidente cibernético puede requerir de expertos externos.

Pérdidas que conlleva un ciberataque

A medida que los riesgos cibernéticos aumentan, las aseguradoras marítimas también afrontan una demanda cada vez mayor de productos y servicios que protejan de las eventuales consecuencias de esos riesgos cibernéticos.Los incidentes cibernéticos pueden dar lugar a pérdidas económicas o costes en la reconstrucción de los datos perdidos que normalmente no están cubiertos por las pólizas generales.

Un incidente cibernético que se lleve a cabo con éxito puede tener varias implicaciones importantes para el seguro: pérdida de vidas humanas; daños personales; contaminación; pérdida/daños en la carga, equipo de manipulación de la carga o bienes; interrupción del negocio; incumplimientos de contrato; pérdida de producción; de datos; de reputación y muchos otros daños. .Un estudio elaborado por *Lloyd's* en 2017 muestra que los incidentes cibernéticos relacionados están evolucionando rápidamente y pueden convertirse en un riesgo sistémico, por lo que no existe necesariamente un enfoque único para su seguimiento y cuantificación.

Pasar del elemento humano a la red: por qué la formación marítima necesita redefinir su relación con la tecnología

Para reducir el número de accidentes mediante la concienciación y formación, debemos tener una comprensión más profunda de la interacción entre las personas y la tecnología.

La mar es un medio hostil y el transporte marítimo entraña siempre, de por sí, un cierto grado de riesgo. Partiendo de la base de que eliminar completamente dichos riesgos, es decir, 'garantizar una seguridad total' es imposible en toda actividad humana, para disminuirlos hasta un nivel aceptable, existe una amplísima normativa de seguridad, también relacionada con la formación. El examen de los resultados de la investigación de accidentes puede poner de manifiesto posibles lagunas en la formación y conocimientos. Investigaciones recientes han puesto de relieve que el enfoque del elemento humano en las prácticas marineras 'tradicionales', que coloca al marino en el centro de todas las operaciones, no aborda la causa de los accidentes y no prepara adecuadamente a los marinos para el futuro. Sólo analizando de forma crítica el papel de la tecnología en el puente de un buque y la forma interconectada en que se toman las decisiones podemos profundizar en las causas de estos accidentes. Se requiere un cambio en la relación a bordo entre la tecnología y las personas, así como un análisis de los métodos de enseñanza y formación para preparar a nuestros futuros marinos para el entorno en el que van a trabajar.

La estadística que señala que el 80% de los accidentes marítimos se deben a errores humanos es conocida. *Meifeng & Shin* (2019) estudió más de 572 informes de investigación de accidentes ocurridos a lo largo de 50 años y descubrió que había habido un cambio en las principales causas: de factores relacionados con la ingeniería naval a factores humanos. *Bielic, et al.* (2017) mencionaron una serie de elementos que contribuyeron a ello, entre ellos la ergonomía, el escaso conocimiento de los propios sistemas del buque y la autocomplacencia. En sus conclusiones, afirmaron que «*la dependencia y la confianza en la tecnología es cada vez mayor, dando lugar a nuevas fuentes de error y riesgos*». Esto se ve respaldado por las conclusiones de la Agencia Europea de Seguridad Marítima (2019), que clasificaron los tres principales factores humanos contribuyentes como: concienciación sobre la seguridad, métodos de trabajo inadecuados y falta de conocimientos.

SITUACIÓN ACTUAL

La ergonomía, el estudio de cómo podemos organizar al equipo y los objetos a nuestro alrededor para permitir un trabajo eficiente, es, según la OMI, uno de los factores que contribuyen al elemento humano en los accidentes e incidentes. El elemento humano, en este caso el Oficial de Guardia (*Officer Of the Watch, OOW*), es reconocido como el «*principal protector de la seguridad y protección marítimas*» (OMI 2006).

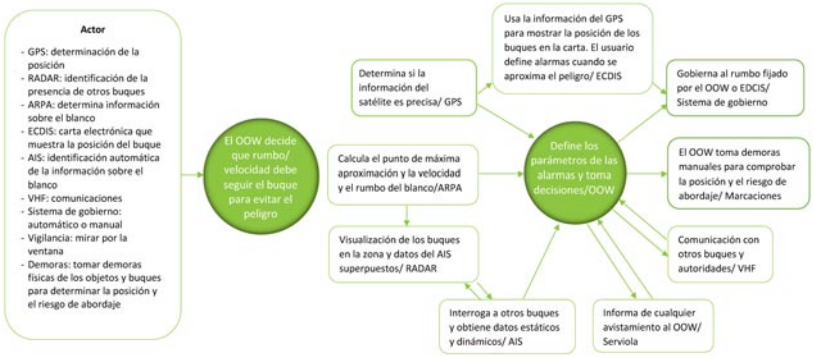


Figura 1: diagrama 'Acción única versus patrón de acción' adaptado. Elaborado por Pentland&Thorvald en 2015.

En los últimos años, sin embargo, hemos visto una reducción del número de tripulantes a bordo debido a que las nuevas tecnologías permiten automatizar cada vez más funciones. Al mismo tiempo, el volumen de datos recibidos y transmitidos desde los buques ha aumentado (*Mallam, et al.*, 2019). Esta información puede analizarse en los centros de gestión de la flota en tierra y los oficiales del buque aportan cada vez menos a las decisiones sobre la planificación de la ruta, velocidad y cuidados de la carga. Este cambio en la dinámica desafía la visión de la OMI del elemento humano como 'principal protector' del buque y sitúa a la tecnología en el centro de las operaciones. Ésta ya no es una 'herramienta' pasiva usada por el armador, sino que influye directamente y determina las decisiones operacionales.

Este cambio en el papel del oficial del buque aún no ha sido reconocido por los proveedores de formación marítima, que aún tienen una visión de las operaciones del buque centrada en el elemento humano y ven la tecnología como un medio para mejorar la forma de actuar de los marinos a bordo.

TECNOLOGÍA Y TAREAS RUTINARIAS

Es importante desarrollar un conocimiento más profundo de las tareas y rutinas cotidianas para detectar lo que se puede cambiar o mejorar. El uso de la tecnología digital puede ayudar a llevar a cabo tareas rutinarias y tomar consciencia de las cambiantes condiciones meteorológicas y de tráfico marítimo. Estos sucesos y compromisos cotidianos con las tecnologías digitales dan como resultado lo que *Pink et al* (2017) denomina 'datos cotidianos'. Reagruparlos puede dar una visión más profunda de nuestra relación con la tecnología y resaltar las lagunas en los conocimientos que se pueden abordar. Por ejemplo, *Whatpulse* es una aplicación de *software* que hace un seguimiento de las pulsaciones de teclas y los *clics* del ratón en una pieza del equipo. Si se

instala en el ECDIS y radar, puede rastrear el flujo de su uso cotidiano destacando si el usuario está usando la tecnología de la manera más provechosa.

OPERAR COMO PARTE DE UNA RED

La teoría del actor-red se puede usar para ilustrar la relación entre el OOW y la tecnología. Esta teoría busca entender el papel de la tecnología en la configuración de los procesos sociales.

Según esta teoría, el elemento humano es sólo uno de los actores involucrado en el proceso de toma de decisiones en el puente, formando parte de una red que incluye a la tecnología, y en la que la información fluye en ambas direcciones. La Figura 1 intenta mostrar la diferencia entre la visión de las operaciones del puente centrada en el elemento humano y la tomada por esta teoría. El cuadro de la derecha muestra las influencias que afectan a la toma de decisiones del OOW desde una visión de las operaciones del puente centrada en el elemento humano. La figura de la izquierda muestra cómo los diferentes actores de la red del puente influyen e interactúan entre sí y con otros actores externos.

Explicar la interacción entre el elemento humano y la tecnología desde esta teoríada una idea más precisa de lo que sucede en el puente que desde la visión centrada en el elemento humano, y nos permite analizar de forma crítica el intercambio de información y datos en red.

Es hora de replantearse lo que significa ser marino en la era digital y dejar atrás algunos de los conceptos obsoletos y estereotipos de lo que significa ser capitán de un buque, aislado de otras influencias y libre de tomar las decisiones que crea convenientes.

INTERACCIÓN DIGITAL Y 'DIGI-GRASPING'

La visión tradicional de la función del OOW es antropocéntrica, coloca la actividad humana en el centro de todas las operaciones (*Maritime and Coastguard Agency*, 2010). Sin embargo, las tecnologías digitales que son comunes y obligatorias en el puente crean y dan forma a nuestra comprensión del entorno exterior.

Dufva & Dufva (2019) analiza el papel de una mayor digitalización en nuestras vidas, desarrollando el concepto de '*digi-grasping*', que describe como «*tener sentido activo y empoderado y participación en un mundo cada vez más digitalizado*». El *digi-grasping* es más que un entendimiento teórico o técnico, refleja las cualidades y habilidades requeridas para operar en el entorno físico y digital, algo que la formación debe tener en cuenta.

Al 'captar' su papel en la interacción entre la toma de decisiones cognitivas, la manipulación física de las interfaces tecnológicas y la capacidad de la tecnología de adoptar e informar de las decisiones, los OOW pueden reforzar su relación con la tecnología, y un mejor conocimiento de la forma en que interactúan con ella. En vez de enseñar a los futuros oficiales que la seguridad del buque depende solo de su propia toma de decisiones, el *digi-grasping* permite un cambio de mentalidad donde el elemento humano y lo digital se convierten en colaboradores con retroalimentación entre las dos partes.

El *digi-grasping* está vinculado a la investigación sobre la Interacción-Persona-Ordenador (*Human – Computer – Interaction*, HCI) y la teoría de la cognición personificada (*theory of embodied cognition*), es decir, que nuestro cuerpo influye en la forma en que procesamos la información a nuestro alrededor, y diferentes cuerpos pueden interpretar la misma información de manera diferente. *Shapiro* (2010) y *Petit et al.* (2019) afirman que el uso de interfaces digitales afecta a nuestra cognición del entorno en el que operamos. Las interfaces usadas por el OOW para determinar los datos relacionados con la navegación y para evitar abordajes influyen en la forma en la que interpreta esa información.

CUESTIONES SOBRE LA FORMACIÓN EN EL FUTURO

¿Qué impacto deberían tener los 'datos cotidianos', el *digi-grasping* y la HCI en la forma en que impartimos formación a los profesionales de la mar? Tal como *Dufva & Dufva* destaca, las habilidades necesarias para operar en un entorno digital son «*difíciles de cuantificar o hacer visibles*». A menudo se deja que el individuo desarrolle estas habilidades por sí mismo en el lugar de trabajo o a través de la formación en cascada de sus compañeros.

Los métodos tradicionales de formación de la gente de mar no satisfacen las necesidades del lugar de trabajo actual. Esto se evidencia en el número de incidentes relacionados con el 'factor humano'. El problema de los Centros de Formación Marítima (*Maritime Educational Training,* MET) tradicionales es que las habilidades y experiencia de los profesores cualificados no reflejan las habilidades requeridas en el lugar de trabajo (*Emad, et al.*, 2020). Además, actualmente hay una falta de recursos para que aquellos que trabajan en el puente se involucren y entiendan las cuestiones digitales y tecnológicas que afectan a la forma en la que trabajan.

Es importante fomentar un análisis más crítico sobre el papel de la tecnología y cómo formamos a las personas para trabajar con ella. Esto nos permitirá definir más claramente el papel del elemento humano en los incidentes y accidentes de buques y alejarnos de términos confusos como 'complacencia' y 'falta de conocimiento'.

RETOS FUTUROS

Por el momento, el cambio en el sector marítimo lo están impulsado los especialistas en tecnología en lugar de las partes interesadas del sector marítimo (*Mallam, et al.*, 2019). El desafío para los educadores marítimos es intentar imaginar cómo será el futuro. Mientras que los organismos reguladores y otras agentes del sector tratan de configurar el futuro aplicando y adaptando los marcos y jerarquías existentes, la formación requerirá un enfoque diferente para definir las futuras pedagogías y formación.

Antes de mirar hacia el futuro, primero debemos entender y comprometernos con el 'presente denso' (*thick present*) (*Facer*, 2016). Este es un reconocimiento de que nuestra comprensión del entorno que nos rodea está formada por «*múltiples capas de realidad que son los materiales para crear futuros*». *Facer* (2019) describe la 'Pedagogía del Presente', que es el proceso de ser abierto y explorar la posibilidad de diferentes futuros.

Para hacer esto, sería conveniente crear una plataforma o un espacio donde la gente de mar pueda aprender más sobre la relación entre la tecnología y el elemento humano, que podría estructurarse como un espacio de Recursos Educativos Abiertos (*Open Educational Resource*, REA). Este recurso permitiría explorar una serie de futuros diferentes dentro del sector con la intención de desarrollar pedagogías que reflejen con mayor precisión el papel cambiante de la gente de mar hoy y en el futuro.

Investigación del abordaje y posterior hundimiento del granelero Oceania en el estrecho de Malaca

La causa del abordaje fue casi con toda seguridad el resultado de un conflicto en el intercambio de comunicaciones entre los dos buques.

El 29 de julio de 2011, se notificó a la Autoridad Marítima de Malta que el *Oceania*, un granelero abanderado en Malta, de 230 m de eslora y 38.377 GT, había sufrido daños graves en el casco tras un abordaje con el buque *Xin Tai Hai*, de bandera panameña, 295 m de eslora y 94.710 GT.

El *Oceania* navegaba por el estrecho de Malaca cuando sonó una alarma en la cámara de máquinas. El oficial de máquinas de guardia se dirigió a la sala de control y observó que se había activado una alarma de baja frecuencia. Inmediatamente después de silenciar y reconocer la alarma, el motor principal se ralentizó, sufrió una caída de planta (*black out*) y se quedó sin gobierno.

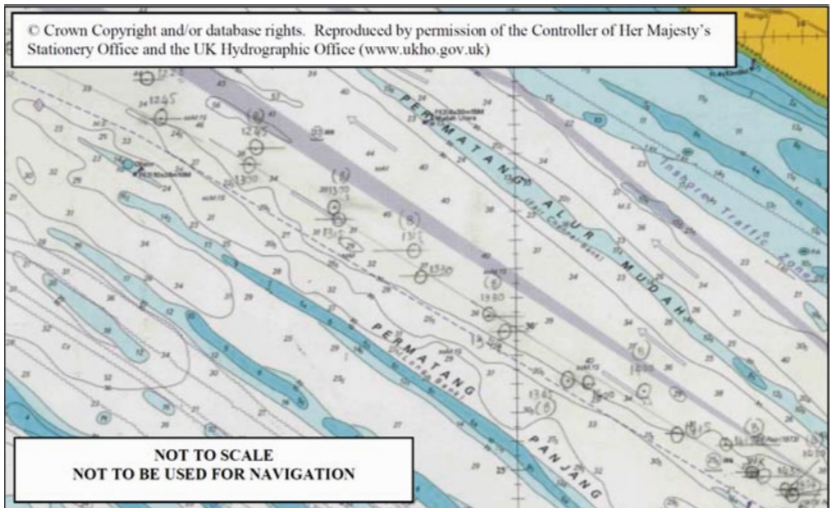
Mientras los oficiales de máquinas se ocupaban de solucionar el problema de la pérdida de energía eléctrica e intentaban arrancar los motores auxiliares, los Oficiales de Guardia en el puente (*Officers Of the Watch, OOWs*) se enfrentaban a una situación peligrosa en una de las zonas de navegación más transitadas del mundo. En concreto, al capitán y los OOWs del *Oceania* les preocupaba el buque *Xin Tai Hai*, que les estaba adelantando.

Ambos buques discutieron por VHF la situación y, en principio, parecía que habían llegado a un acuerdo sobre cómo el *Xin Tai Hai* iba a adelantar con seguridad al *Oceania*. Finalmente, el *Xin Tai Hai* mantuvo el rumbo y la velocidad, y el *Oceania* fue variando lentamente su rumbo a estribor, produciéndose el abordaje de ambos buques. En el momento de la colisión, el *Oceania* había efectuado un giro de casi 98° a estribor. El *Xin Tai Hai* sufrió graves daños en su amura. Los daños sufridos por el *Oceania* fueron mucho más importantes y extensos, y los tripulantes tuvieron que abandonar el buque, que se hundió unos 40 minutos después del abordaje.

La investigación del Departamento de Investigación de Seguridad Marítima (*Marine Safety Investigation Unit*, MSIU) concluyó que la causa más probable del *blackout* fue un fallo en la bomba de suministro de HFO o en la bomba auxiliar. El hecho de que la bomba auxiliar de HFO y/o la bomba de suministro de HFO de reserva (*'stand-by'*) estubiera funcionando en modo manual pudo agravar la situación. La investigación reveló que se produjo un conflicto en el intercambio de comunicación verbal por VHF y las acciones reales tomadas por el *Xin Tai Hai,* que el informe atribuye a la propia complejidad de la situación, agravada por la barrera del idioma.

NARRACIÓN DE LOS HECHOS

El 24 de julio, el *Oceania* completó el cargamento de unas 67.453 t de finos de mineral de hierro en Paradip (India). Tras los necesarios reconocimientos de los calados y carga, y la comprobación documental, el granelero abandonó el puerto de carga sobre las 18.00 h. El buque tenía un calado de 13 m (sin asiento). El combustible disponible a bordo era de 601 t de HFO (380 cST) y 131 t de MDO. Se había previsto que el buque llegaría a Singapur para tomar combustible el 30 de julio, sobre las 04:00 h.



Zona del estrecho de Malaca en la que tuvo lugar el abordaje.

Los miembros de la tripulación revisaron que todas las comprobaciones preceptivas previas a que el buque se hiciera a la mar se habían completado. Aunque esa época del año era época de monzones, las condiciones meteorológicas no se consideraron extremas; la fuerte marejada en la zona hizo que el buque se balanceara, aunque no en exceso.

Se mantuvieron los turnos de guardia habituales de 4 horas de servicio y 8 horas de descanso. De acuerdo con el programa de mantenimiento planificado del buque, los filtros de combustible se revisaban y limpiaban mensualmente. La última comprobación se había hecho 2 días antes del accidente y los filtros de combustible del motor auxiliar se limpiaron un día después. No se observó nada anormal y la presión diferencial en los filtros de combustible estaba dentro de los límites. Las señales de alarma (que indican un aumento en la presión diferencial antes y después del filtro) no se habían activado.

El 29 de julio, el *Oceania* entró en el estrecho de Malaca. El motor principal se mantuvo a 80 rpm. Los motores auxiliares 2 y 3 se mantuvieron funcionando en paralelo. El capitán permaneció en el puente la mayor parte del día. Por la noche, se encontraba en el puente en el cambio de guardia entre el 1er y 3er oficial, guardia que abarcaba el periodo de 20:00 a 00:00 horas. Se

quedó en el puente durante toda la guardia del 3er oficial, excepto unos 5 minutos, que se ausentó para revisar el correo electrónico.

El *Oceania* navegaba al rumbo 123° y a 12,5 nudos, con el piloto automático conectado y una bomba en funcionamiento para el gobierno. Aunque estaba oscuro, la visibilidad era buena, el viento soplaba del Sureste a 20 nudos y el estado de la mar con respecto a la altura de las olas era de grado 3 en la escala de Douglas (marejada). Tanto el radar de banda X como el de banda S estaban en funcionamiento y operaban en las escalas de 3 y/o 6 millas de alcance. El buque también tenía conectadas las luces de navegación reglamentarias. Un marinero estaba de guardia como vigía adicional y tenía asignada la tarea de permanecer a la escucha en los canales 16 y 88 (*Port Kelang VTIS*) de VHF.

De acuerdo con el plan de viaje, el *Oceania* tenía previsto entrar en el Dispositivo de Control de Tráfico durante la guardia del 3er oficial. También se había planificado que debía cambiar de rumbo a estribor unos 10°. Se llegaría al punto de referencia (*waypoint*) para efectuar dicho cambio sobre las 14:45 h. El *Oceania* tenía a 2 buques por su proa. Los controles de los radares mostraron que dichos buques estaban a 8 y 10 millas respectivamente.

Ambos buques navegaban con rumbos parecidos al del *Oceania*. Otros 2 blancos transitaban por el estrecho hacia el Noroeste en la dirección opuesta. El blanco más próximo al *Oceania*, sin embargo, se observó a popa, a unas 3 millas. Plenamente consciente de que se trataba de un buque que estaba adelantando, el 3er oficial consultó el AIS para averiguar su nombre. El buque fue identificado como el *Xin Tai Hai*, que también navegaba con rumbo Sureste pero a 13,8 nudos. El capitán del *Oceania* también era consciente de que el *Xin Tai Hai* estaba adelantando, dando por hecho que pasaría por el costado de estribor del *Oceania*. El 3er oficial estimó que el *Xin Tai Hai* tenía un Punto de Máxima Aproximación (*Closest Point of Approach*, CPA) de 5 a 6 cables. Se observó que, de vez en cuando, el vector del radar apuntaba hacia la popa del *Oceania* antes de volver a su rumbo anterior.

Cuando se produjo la caída de planta, el 3er oficial calculó que el *Xin Tai Hai* estaba a una distancia de entre 5 y 10 cables por el través de estribor y podía ver su luz de tope y la lateral roja de babor. Después de llamar al *Xin Tai Hai* 2 veces por su nombre en el canal 16 de VHF, este último reconoció la llamada a las 14:27:30 horas. El OOW del *Oceanía* pidió al del *Xin Tai Hai* que se mantuviera apartado de su trayectoria porque se encontraban sin gobierno. El OOW del *Xin Tai Hai* solicitó al del *Oceania* que le confirmara que su buque era el que estaba por su babor. Este último confirmó la posición del buque.

Unos 2 minutos más tarde, el OOW del *Xin Tai Hai* llamó al *Oceania* y acordaron cambiar de canal de VHF. Tras retomar la comunicación, el OOW del *Oceania* le pidió al del *Xin Tai Hai* que se mantuviera apartado de su derrota. El OOW del *Xin Tai Hai* pidió al del *Oceania* que le aclarase cuáles eran sus intenciones, ya que veía que estaba cayendo a estribor. El rumbo del Oceania era 130,6° y su velocidad 8,7 nudos.

El OOW del *Oceania* le volvió a aclarar que su buque estaba sin gobierno. Sin embargo, al acusar recibo de las advertencias del *Oceania*, el OOW del *Xin Tai Hai* le informó de que su AIS no mostraba que el *Oceania* fuera un buque sin gobierno. Entre las 14:31 h y las 14:33 h, no hubo más comunicaciones. El rumbo del *Oceania* continuó cayendo a estribor a pesar de tener todo el timón metido a babor. En este periodo de tiempo, el rumbo cambió del 148,6° al 195,8° y su velocidad se redujo de 7,7 a 5,6 nudos.

El ARPA del *Xin Tai Hai* mostró un aviso de abordaje y a las 14:32 h empezó a sonar una alarma acústica, que se hizo más fuerte 30 segundos después. Con su nuevo rumbo ahora al 201,8° y 5 nudos de velocidad, el OOW del *Oceania* llamó de nuevo al del *Xin Tai Hai* y le pidió que se mantuviera apartado y evitara caer a estribor. Poco después, el OOW del *Xin Tai Hai* preguntó al del *Oceania* si debía cambiar el rumbo a estribor. El *Oceania* pidió al *Xin Tai Hai* que se mantuviera apartado. A las 14:34 h, el OOW del *Xin Tai Hai* confirmó que estaba cayendo a estribor, pasando del rumbo 139,3° al 145,2°, manteniendo su velocidad en 13 nudos.

En la cámara de máquinas, el jefe de máquinas del *Oceania* estaba a punto de sincronizar los motores auxiliares, pero mientras se dirigía a la sala de control de máquinas junto con el electricista, sintieron dos impactos fuertes y consecutivos a las 14:34:48 h. La amura de babor del *Xin Tai Hai* había golpeado al *Oceania* por el costado de estribor de popa en la posición l: 01° 23,7' N; L: 103° 09,0' E.

CONCLUSIONES

- El Oceania sufrió un *blackout* mientras navegaba por el estrecho de Malaca. No hay indicios de que el buque hubiera tenido previamente algún fallo en el sistema de propulsión.
- La causa del abordaje fue casi con toda seguridad el resultado de un conflicto en el intercambio de comunicaciones entre los dos buques.
- Es posible que los motores auxiliares se bloquearan por falta de alimentación de combustible justo antes de pararse por completo.
- Es posible que en algún momento antes del día del *blackout* y el abordaje, el modo de funcionamiento automático de la bomba auxiliar de combustible en '*standby*' y/o la bomba de suministro de HFO del Oceania se hubieran desactivado e, inadvertidamente, el modo automático no se hubiera reactivado, comprometiendo así la redundancia del sistema de combustible.
- Quizá la causa principal de la parada de los auxiliares del *Oceania* fue la pérdida de presión de combustible en los motores principales debido a un fallo de una de las bombas de alimentación.
- No se descartó que días antes del abordaje uno de los oficiales de máquinas pudo 'sufrir' un lapsus de memoria mientras efectuaba el mantenimiento del sistema de combustible.
- No se descartó que la gasificación en el sistema de combustible de los auxiliares pudo provocar la falta de suministro de combustible y la eventual parada.
- El OOW del *Oceania* avisó en varias ocasiones de que su buque estaba sin gobierno. El OOW del *Xin Tai Hai* confirmó la recepción de los mensajes e indicó que entendía la situación, hasta el último momento, segundos antes del abordaje.
- El *Xin Tai Hai* mantuvo su rumbo y velocidad, lo que indica que la comprensión global del OOW de las señales que había recibido no requerían de ninguna acción diferente a las que ya había tomado.
- Todos los tripulantes del *Oceania* abandonaron el buque de forma segura y fueron trasladados a tierra.