Revista de Marina Nº 970, pp. 15-23
ISSN 0034-8511

CIBERATAQUE AL TRANSPORTE MARÍTIMO. ¿UNA AMENZA REAL O CIENCIA FICCIÓN?

James Crawford Crawford*

Resumen

Se exponen los riesgos de ciberataques a la industria marítima, con una clasificación y los sistemas que pueden ser intervenidos. Se analizan varios casos de ciberataques y las medidas que se han adoptado a nivel global y en Chile.

Palabras clave: Ciberataque, industria marítima, seguridad, hackers.

Durante el mes de julio del 2018, una importante entidad bancaria nacional, fue víctima de un ataque internacional sofisticado, de bandas a nivel mundial, previsiblemente de Europa del Este o Asia, que trajo como consecuencia, el robo aproximado de 10 millones de dólares, la paralización de ciertos servicios y el daño a la imagen del banco. Asimismo, el secretario general de la O.N.U.[1], Antonio Guterres, reconoció durante una actividad celebrada en Lisboa en febrero de 2018, la existencia de "episodios de guerra cibernética entre Estados. Y lo peor es que no hay un esquema reglamentario para este tipo de guerra, no está claro si ahí se aplica la Convención de Ginebra o el Derecho Internacional". En este mismo contexto, un informe presentado a la O.T.A.N.[2], preparado por un grupo de expertos independientes en derecho militar, conocido como *Tallin manual* afirma que "los países tienen justificación legal para usar la fuerza militar contra todo aquel que ayude a un país enemigo a lanzar un ciberataque", lo que justificaría su asesinato bajo determinadas circunstancias.

Considerando los argumentos del párrafo anterior y reconociendo que más del 90% del transporte de carga mundial se realiza por mar, del cual su seguridad y estabilidad depende el desarrollo, bienestar y libre tránsito de las importaciones y exportaciones de una serie de naciones del mundo, ¿podría considerarse el ámbito marítimo y portuario, libre de la amenaza de ciberataques? La respuesta es, sencillamente, no.

Durante los últimos años, ha surgido un tipo de amenaza, la cual hasta el momento ha sido subvalorada en el ámbito de la seguridad marítima, y es aquella constituida por los ataques

* Capitán de fragata LT. MSc Asuntos Marítimos, Universidad Marítima Mundial, Malmö, Suecia. (jcrawford@dgtm.cl).
1. ONU: Acrónimo de Organización de las Naciones Unidas.
2. OTAN: Acrónimo de Organización del Tratado del Atlántico Norte.

cibernéticos, que están llevando a varios países, instituciones y empresas del globo, a adoptar acciones preventivas al respecto. Un ejemplo de lo anterior, lo constituye la estrategia nacional de seguridad cibernética del Reino Unido, en la cual se asigna a la infraestructura marítima portuaria y a los buques, la clasificación de sistemas ciberfísicos, potencialmente vulnerables a las interferencias de amenazas cibernéticas, debido a la combinación de una serie de factores como son la mayor conectividad/dependencia de los componentes digitales, mayores niveles de control autónomo y sistemas de navegación accesibles a nivel mundial.

Si bien es cierto, la evidencia publicada sobre el panorama de amenazas marítimas es escasa, el análisis de los ataques reportados a la fecha deja en evidencia un aumento de la criticidad en términos de motivación de la amenaza, competencia técnica de los atacantes y complejidad de los ataques empleados. Lo anterior, ha sido ratificado por la estimación de inteligencia nacional de los Estados Unidos, en la cual se ha señalado la probabilidad de que el próximo ataque sobre la infraestructura critica de ese país, podría desarrollarse a través de un ciberataque en forma de un ataque cinético,[3] vale decir, desde el espacio.

Mientras la ingeniería tradicional se ha centrado en el diseño y desarrollo de condiciones de seguridad a bordo de las naves, como la duplicidad de los sistemas de control y comunicaciones, diseño de cascos más seguros, etc., no ha considerado la aplicación de conceptos o estrategias asociadas a la ciberseguridad. Por lo anterior, se hace necesario, el trabajo en conjunto de los *stakeholders* del ámbito marítimo, que permita la protección global de las componentes de este sector - sistemas electrónicos y de control para buques, embarcaciones, unidades *offshore* y sistemas portuarios -, considerándolas en la totalidad del ciclo de vida de la ingeniería, con el propósito de evitar accidentes, protegerse de amenazas deliberadas y resguardar los intereses marítimos nacionales.

Definición de ciberseguridad

La Unión Internacional de Telecomunicaciones (UIT), ha definido, en la resolución UIT-Tx 1205, el concepto ciberseguridad como:

> ...el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno.

De esta forma, la definición considera a redes interconectadas de información y su hardware asociado, basadas en computadores y redes inalámbricas, incluyendo las informaciones, bases de datos, servicios y gestiones de trabajo, exclusivas al ciberespacio.

En la misma línea, el Instituto Nacional de Estándares y Tecnología del departamento de Comercio de los Estados Unidos (Conocido por su sigla NIST del inglés: National Institute of Standards and Technology), en su definición de ciberseguridad, reconoce la existencia de un escenario no físico como es el ciberespacio que requiere de habilidades que aseguren su protección.

Motivaciones de los ataques

Las motivaciones tras los ataques cibernéticos pueden ser muy variadas, por lo que ninguno de los componentes del ámbito marítimo-administración, logístico, seguridad, etc.- puede ser excluido. De acuerdo al Instituto de Ingeniería y Tecnología del Reino Unido[4], estas pueden ser clasificadas de la siguiente forma:

- **Espionaje**: búsqueda de acceso no autorizado a información sensible, sujeta a propiedad intelectual, asociada a gestiones comerciales, estrategias corporativas, entre otras, con el fin de interrumpir el normal funcionamiento o causar pérdidas comerciales.
- **Grupos de activismo o hacktivismo** (de hackeo por intereses del grupo) que buscan publicidad o generar presión en representación de una causa u objetivo.

3. Según Wikipedia, un bombardeo cinético, corresponde al acto de atacar desde el espacio una parte de la superficie planetaria con un proyectil no explosivo donde la fuerza destructiva proviene de la energía cinética liberada durante impacto del proyectil.
4. De su nombre en idioma inglés: *Institution of Engineering and Technology*.

- **Criminal**: con el propósito de obtener beneficios económicos, daño a bienes materiales, robo, tráfico de especies o personas y/o con el propósito de evadir impuestos o deberes.
- **Terrorismo**: acciones orientadas a producir temor y causar interrupciones físicas y económicas.
- **Bélicas**: en el contexto de conflictos entre Estados, con el propósito de interrumpir los sistemas y vías de comunicación, con el propósito de negar su acceso.

Clasificación de los ataques

Debido a que el tema de la ciberseguridad es relativamente nuevo, no existe un consenso generalizado respecto de los conceptos asociados a la problemática. No obstante lo anterior, se puede señalar, que existen dos categorías de ciberataques que afectan a las empresas navieras/portuarias y a los buques/plataformas:

- Ataques no focalizados, donde una empresa o los sistemas y datos de un buque son uno de muchos objetivos potenciales y
- Ataques dirigidos, donde los sistemas y datos de una compañía o de un buque son el objetivo deseado.

Respecto de la motivación, la Oficina Gubernamental para la Ciencia del Reino Unido, ha identificado tres categorías de ciberataques en relación a los objetivos de los mismos; ataques a: a) activos de empresa, b) sistemas de información y c) G.P.S. y sistemas de navegación o control crítico. En estos tres tipos de ataques, se ha observado un aumento de la criticidad en términos de motivación de la amenaza, competencia técnica de los atacantes y complejidad de los ataques empleados.

Conforme los resultados obtenidos en la encuesta realizada por el IHS Markit[5] y BIMCO[6] el año 2016 a *stakeholders* marítimos, el 21% de los encuestados reportó haber sufrido algún tipo de ciberataque (un 22% no respondió), 77% de los ataques perpetrados, respondía a *malware*, y cerca de un 20% a robo de credenciales. Se estima que el costo anual probable para la economía mundial del tipo de acciones señaladas precedentemente, se espera que alcance los dos trillones (2.000.000.000.000) de dólares americanos al año 2019.

Objetivos tecnológicos de los ataques

Si bien es cierto que los ataques en el ámbito marítimo pueden afectar el comercio global, existen ciertas acciones que podrían afectar directamente a la seguridad de la vida humana en el mar, o a la protección del medio ambiente, mediante la violación o alteración de sistemas críticos de seguridad a bordo de las naves. En este sentido, existen algunas experiencias de ataques sobre algunos sistemas como los que se señalan a continuación, agrupados según el tipo de tecnología intervenida.

- **ECDIS**[7]

La vulneración del sistema cartas electrónicas de navegación - conocidas como ECDIS-, que reemplazan a las cartas náuticas de papel a bordo de los buques, podría permitir el acceso de un atacante y la modificación de archivos y tablas a bordo o en tierra, lo que podría causar graves daños ambientales y financieros, incluso la pérdida de vidas humanas.

En enero de 2014, el Grupo NCC[8] intentó penetrar un sistema ECDIS de un importante fabricante. En el proceso se detectaron varias debilidades de seguridad tales como: capacidad de leer, descargar, reemplazar o eliminar cualquier archivo almacenado en la máquina que alojaba al sistema. Una vez conseguido el acceso, los atacantes, podrían haber tenido la capacidad de interactuar con la red a bordo y todo a lo que estaba conectado, solo a través de la inserción de dispositivo USB o a través de una descarga de internet.

- **AIS**[9]

Los A.I.S. básicamente, permiten a los buques comunicarse con otras naves e intercambiar su posición y otros datos de interés, con el propósito de evitar colisiones. Existen experiencias que

5. HS Markit Ltd.: es un proveedor global de información, basado en Londres.
6. BIMCO: Consejo Marítimo Internacional y del Báltico. IHS Markit: empresa proveedora de información global basada en Londres, Inglaterra.
7. E.C.D.I.S.: *Electronic Chart Display and Information System.* Sistema de información geográfica utilizado para la navegación náutica.
8. Grupo de expertos a nivel global, que ofrecen servicios en el ámbito de la ciberseguridad.
9. A.I.S.: *Automatic Identification System*, Sistema de identificación automático de naves, utilizado en el ámbito marítimo.

demuestran que un atacante con una radio V.H.F. de $100 dólares, podría utilizar las debilidades en el sistema de identificación automática, para modificar datos tales como: identidad, tipo, posición, rumbo y velocidad a las estaciones costeras. Asimismo, el atacante también podría alterar los datos, haciéndose pasar por autoridades portuarias, comunicarse con los buques y/o bloquear las comunicaciones entre las naves y los puertos.

En octubre de 2013 la empresa *Trend Micro* demostró la facilidad con la que se podían crear buques fantasmas en cualquier ubicación del mundo, los que serían reconocidos por los receptores como naves reales, o activar una alerta de colisión falsa, lo que obligaría a cambiar el rumbo de una nave. En la misma oportunidad se demostró que se podía enviar información meteorológica falsa, lo que obligaría a la nave a modificar su track, causar el aumento de la frecuencia de transmisión de datos A.I.S., saturando a los receptores en otros buques y/o autoridades.

- **GPS**

Los Sistemas de Posicionamiento Global (GPS), pueden ser atacados, causando graves problemas al transporte marítimo y poniendo en riesgo a miles de vidas humanas. La vulneración de este sistema fue demostrado con el ataque a la *White Rose of Drax*, que se analizará mas adelante.

El año 2008, la Autoridad de faros del Reino Unido e Irlanda realizó, para efectos de prueba, el *jameo*[10] de un área oceánica dentro de la cual se encontraba uno de sus buques boyeros, el cual reportó fallas en el transpondedor A.I.S., sistema de posicionamiento dinámico, descalibración del giroscopio, sistema de llamada selectiva digital y no actualización de la cartografía electrónica.

- **GNSS**

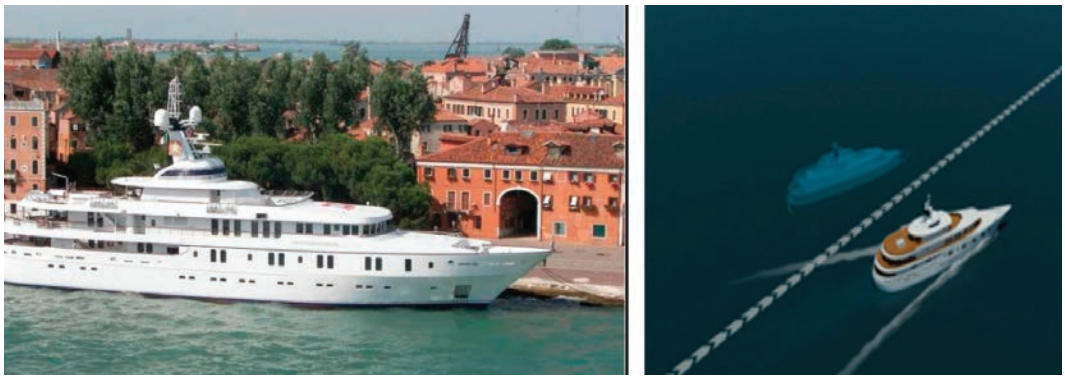
Conforme a lo publicado por la reconocida corporación transnacional de ciberseguridad y de servicios satelitales GMV, los sistemas mundiales de navegación por satélite, GNSS[11] se están convirtiendo en la quinta utilidad pública después del agua, la electricidad, petróleo/gas y telecomunicaciones. Sin embargo, la falta de seguridad de éstos en el dominio civil, se estima preocupante, por lo que se encuentran desarrollando servicios con esquemas de autenticación de la data y contacto.

Los sistemas mundiales de navegación por satélite, GNSS, civiles en uso son mucho más vulnerables al ataque que los GPS militares. Lo anterior, debido a que estos sistemas no están encriptados ni autenticados.

Casos de ciberataques

- ***White Rose of Drax***

El año 2013 un equipo de investigación de la Universidad de Texas-Austin demostró cómo un potencial atacante podría tomar control remoto de un buque, a través de la manipulación de su GPS El yate *White Rose of Drax* fue exitosamente penetrado mientras navegaba en el Mediterráneo, en solo 30 minutos. Mediante la transmisión de señales falsas de G.P.S. civil, el equipo de



Fotografía del yate *White Rose of Drax* y la representación de la alteración obtenida en su rumbo de navegación.

10. De *Jamming*, que se refiere en este caso, a efectuar interferencias electrónicas a los sistemas de ayuda a la navegación de un buque.
11. Un sistema global de navegación por satélite (*Global Navigation Satellite System*, G.N.S.S.).

investigación fue capaz de dominar lentamente las señales reales del G.P.S. del yate, obteniendo el control de su sistema de navegación. Cuando el equipo de hackeo transmitió una señal falsa a la antena del GPS del yate, el sistema de navegación del buque acusó una desviación del rumbo establecido, por lo que el equipo de navegación de puente tomó las acciones necesarias para volver a rumbo, sin saber que lo estaban haciendo a un rumbo equivocado y definido por los hackers. De acuerdo a lo señalado por el profesor a cargo de la investigación, Todd Humphreys, "el yate comenzó a alterar su rumbo, pero en la pantalla del radar solo se apreciaba una línea recta".

■ Ataque a Maersk

El año 2017, la empresa Maersk sufrió un ataque informático del tipo *Ransomware*, impidiendo o limitando el acceso de los usuarios de sus sistemas de administración y control, a su propio sistema informático, causando entre $250 millones y $300 millones de dólares en pérdidas. Si bien es cierto que algunas fuentes señalan que lo sucedido correspondió a un daño colateral producto del ataque de *hackers* a Ucrania, la situación afectó a una de las principales compañías navieras del mundo. Durante los 10 días del proceso de levantamiento de los sistemas posterior al ataque, los empleados de la empresa no pudieron administrar solo un 20% de las demandas de transporte, gracias al esfuerzo y compromiso de los mismos. El presidente de Maersk, señaló que producto del ataque, se tuvieron que reemplazar 45.000 computadores, 4.000 servidores e instalar 2.500 aplicaciones.

■ Ataque a plataformas petroleras

El año 2010, durante el proceso de traslado de una plataforma de perforación petrolera, desde Corea del Sur a Brazil, la estructura se inclinó hacia una banda, produciendo una serie de heridos. Tras 19 días de investigación, el personal a cargo pudo identificar la falla, confirmando que se trataría de un ataque computacional, producido por el alojamiento de una plaga de virus en las computadoras y los sistemas de control de la plataforma.

Otro ciberataque a una plataforma petrolera, la *Noble Regina*, fue reportado el 3 de diciembre de 2012, en circunstancias que se encontraba en su proceso de construcción. Los ciberatacantes lograron tomar el control de sus sistema de bombas, lo que les permitió producir una escora de 17º, ocasionando un accidente que afectó a 89 trabajadores, estructura de apoyo y perdidas económicas al astillero.

Finalmente, en abril de 2014 por la compañía ThetaRay en las afueras de las costas de África, que también produjo que se escorara, obligando a detener sus operaciones durante una semana.

■ Plataforma petrolera *Noble Regina*, escorada posterior al ataque.

■ Ataque a compañía naviera iraní

En agosto del año 2011, piratas informáticos penetraron en los servidores de IRISL[12], la mayor línea naviera iraní, dañando datos con tarifas, cargando números de carga, fechas de entrega y lugares. Lo anterior, trajo como consecuencia, el descontrol sobre la ubicación de un gran número de contenedores. Asimismo, una cantidad considerable de carga se entregó a los destinos equivocados o incluso se perdió.

12. IRISL acronismo de *Islamic Republic of Iran Shipping Lines* (IRISL Group), que cuenta con al menos 115 buques de trafico internacional con una capacidad aproximada de 3.3 millones de toneladas.

■ **Ataque a sistemas aduaneros y/o portuarios**

El año 2012, piratas informáticos pusieron en peligro el sistema de carga controlado por la agencia del Servicio de Aduanas y Protección Fronteriza de Australia. Los ciberdelincuentes querían saber qué contenedores se encontraban bajo sospecha por la policía o las autoridades aduaneras. Con esta información sabrían si necesitaban abandonar contenedores particulares con carga de contrabando.

Asimismo, entre los años 2011 y 2013, ataques similares al señalado precedentemente, se desarrollaron en el puerto de Antwerp, Bélgica, logrando la pérdida de información acerca del paradero de contenedores, cambio de las fechas y lugares de entrega y ocultamiento de números de seguridad, entre otras acciones. Cuando la brecha de seguridad fue expuesta, el puerto instaló un *firewall*. Sin embargo, los criminales ingresaron al puerto e instalaron puentes inalámbricos en las computadoras en funcionamiento, abriendo un acceso directo al sistema operativo. A la administración del puerto, le tomó cerca de dos años el encontrar la razón de la desaparición de los contenedores en sus recintos.

La OMI y la ciberseguridad

En mayo 2016 el Comité de Seguridad Marítima de la Organización Marítima Internacional (OMI) aprobó la guía de gestión de ciber riesgos marítimos,[13] reconociendo este tipo de amenazas en el ámbito marítimo y su posible impacto en las operaciones y la seguridad de las naves y sus tripulaciones. En este contexto y con el objetivo de proteger al sector marítimo de los ciber riesgos, la O.M.I. consideró necesaria la incorporación en la gestión de riesgos de las compañías y buques los riesgos de ciberseguridad.

La aproximación a la gestión de riesgos de ciberseguridad de la OMI, propone un enfoque basado en la implementación y mantenimiento de cinco elementos: identificación, protección, detección, respuesta y recuperación. Asimismo, plantea la adopción de ciertas buenas prácticas tales como:

- Marco de ciberseguridad del Instituto de Ingeniería y Tecnología del Reino Unido.
- Estándar de seguridad en tecnologías de la información ISO 27001.
- Guía de la ciberseguridad a bordo de buques del Consejo Marítimo Internacional y del Báltico.

Aunque la OMI ha otorgado a los propietarios y administradores de buques plazo hasta el año 2021 para incorporar la seguridad del riesgo cibernético a los sistemas de gestión de seguridad de los buques, los propietarios y operadores de tanqueros sujetos a verificación bajo el foro de Compañías Petroleras Marinas Internacionales (OCIMF)[14] deberían encontrarse abordando los riesgos de ciberseguridad en sus políticas y procedimientos desde el 1 de enero del presente año. La tercera versión del sistema de gestión de seguridad de este tipo de buques (2018) ya incluye la gestión del agua de lastre, del combustible y otros elementos, como asimismo, incluyó un nuevo capítulo (Nº13) titulado "seguridad marítima".

La guardia costera norteamericana y la ciberseguridad

Estados Unidos ha adoptado los niveles de seguridad del Instituto Nacional de Estándares y Tecnología para instalaciones portuarias, para el análisis de vulnerabilidades en el ámbito de la ciberseguridad, con el propósito de generar un plan de respuesta ante este tipo de incidentes.

Cabe señalar que Estados Unidos de Norteamérica, ya ha experimentado situaciones similares a lo que podría ser un ataque a sus instalaciones portuarias. El año 2012, durante la evolución del huracán *Sandy* sobre los puertos de Nueva York, se produjo la pérdida de un billón de dólares por día, por concepto de salarios, negocios no realizados, y el valor de carga que tuvo que ser derivada a otros puertos.

La guardia costera de Estados Unidos se encuentra desarrollando sus políticas de ciberseguridad en tres ámbitos:

➢ Defensa del ciberespacio: desarrollo de sistemas de tecnología de la información seguros y resistentes, que permitan el desarrollo de la totalidad de las capacidades de la organización, de la forma mas eficiente.

13. MSC.1/Circ.1526, 1 June 2016, *Interim Guidelines On maritime cyber risk management.*
14. OCIMF - *Oil Companies International Marine Forum*.

- Habilitación de operaciones: operar efectivamente dentro del ciberdominio, que permita desarrollar y potenciar las cibercapacidades de la infra estructura critica y autoridades relacionadas.
- Protección de la infraestructura: mediante la utilización de sistemas robustos, rápidos y eficientes, que permitan la protección de las infraestructura critica, en atención a la importancia que reviste para la nación.

El esfuerzo nacional

El día 7 de abril del año 2017, la presidenta Michelle Bachelet, participó en el lanzamiento de la política nacional de ciberseguridad nacional, constituyéndose en el primer instrumento de la política pública del Estado de Chile orientado a asegurar un ciberespacio libre, abierto, seguro y resiliente, protegiendo derechos humanos como la privacidad y la libertad de expresión.

La política nacional, se encuentra diseñada bajo cinco ejes esenciales:

- Primero, contar con una infraestructura de la información capaz de resistir y recuperarse en caso de ataques e incidentes de ciberseguridad;
- Segundo, proteger los derechos de los ciudadanos en el ciberespacio;
- Tercero, generar una cultura de ciberseguridad en el país;
- Cuarto avanzar en conjunto con los organismos internacionales en los desafíos que se establezcan;
- Quinto, promover el desarrollo de una industria de la ciberseguridad, que permita posicionar a Chile de mejor manera en la región.

ENTIDAD	ROL	MISIÓN
PDI, Brigada Investigadora del ciber crimen	Preventivo e investigativo	Encargada de la investigación de los delitos de conformidad con instrucciones del Ministerio Público, como es el caso de los ciberdelitos.
Carabineros, departamento OS 9	Preventivo e investigativo	Encargados del orden público y la seguridad pública interior, su alteración debe ser prevenida e investigada, como es el caso de los ciberdelitos.
Agencia nacional de inteligencia	Preventivo	De acuerdo a la Ley 19.974 que regula su funcionamiento, entre sus tareas se encuentra: "proponer normas y procedimientos de protección de los sistemas de información crítica del Estado" Art 8, letra c)
Estado Mayor Conjunto y fuerzas armadas	Preventivo y reactivo	Las instituciones de las fuerzas armadas están a cargo de proteger su propia infraestructura de la información, además de colaborar en las tareas de ciberseguridad que correspondan en relación con la seguridad nacional y el sistema nacional de inteligencia. El Estado Mayor Conjunto es el organismo de trabajo y asesoría permanente del Ministro de Defensa Nacional en materias que tengan relación con la preparación y empleo conjunto de las fuerzas armadas, y está a cargo de elaborar y mantener actualizada la planificación secundaria de la defensa, junto con otras tareas relevantes para la ciberseguridad del país. Las fuerzas armadas, por su parte, están a cargo, acorde a la planificación realizada, de los planes institucionales y operativos que correspondan.

La Política Nacional de Ciberseguridad establece las siguientes misiones: Fuente: Política Nacional de Ciberseguridad.

En el ámbito marítimo, la Dirección General del Territorio Marítimo y de Marina Mercante (DIRECTEMAR), se encuentra evaluando la mejor forma de abordar este nuevo tipo de amenaza y la forma de enfrentar su fiscalización en su ámbito jurisdiccional.

Conclusiones y recomendaciones

Conforme a los antecedentes señalados precedentemente, puede concluirse que, los ataques al ciberespacio marítimo, son un hecho real, que se han registrado durante los últimos años, un aumento de la criticidad en términos de motivación de la amenaza, competencia técnica de los atacantes y complejidad de los mismos. Lo anterior, ha significado pérdidas económicas, materiales, daño a la vida humana y potencial beneficio para el tráfico ilegal de productos a través de recintos portuarios. Asimismo, podría entenderse, como un periodo de entrenamiento para ataques más grandes y de mayor impacto.

Afortunadamente, la comunidad liderada por la OMI ya se encuentra adoptando acciones que permitan la protección del transporte marítimo de ciberamenazas y vulnerabilidades, que protejan la vida humana y el medio ambiente marino. En ese contexto, y considerando que en nuestro país más del 90% del comercio exterior se moviliza a través del sector marítimo, ya se cuenta con una política nacional de ciberseguridad, orientada a la creación de una infraestructura de información que permita resistir y recuperarse de este tipo de ataques.

Asimismo, la autoridad marítima nacional, ya se encuentra evaluando la mejor aproximación para enfrentar este nuevo tipo de amenaza en forma holística que permita proteger la vida humana en el mar, protección del medio ambiente y la cautela de los intereses marítimos con el propósito de contribuir al desarrollo del poderío marítimo nacional. Se estima que, como primer elemento, debe considerarse la generación del marco legal que permita a la Dirección General del Territorio Marítimo y de Marina Mercante, proteger la estructura crítica de su ámbito jurisdiccional, mediante el desarrollo y aplicación de una ciber estrategia amplia y detallada, que promueva el éxito de sus misiones. Asimismo, y en base a otras estrategias en aplicación, DIRECTEMAR debiese considerar al menos dentro de sus acciones:

a) Monitoreo y detección de alta capacidad desplegadas para proteger y proporcionar alertas tempranas;

b) Sistemas críticos diseñados con medidas avanzadas para contrarrestar las infecciones de malware; junto con medidas que permitan minimizar el daño físico y la interrupción;

c) Generación de informes, respuesta y gestión de incidentes que permitan aumentar de manera eficiente el riesgo mitigación, forense y coordinación de la aplicación de la ley.

Por otro lado, el ámbito de la construcción naval, debería comenzar a reconocer la exposición de los buques y sistemas a amenazas cibernéticas, aplicando diseños con enfoques basados en el riesgo; desde la etapa de diseño de la seguridad cibernética, hasta la robustez de la misma al momento de la construcción, mediante la aplicación de múltiples capas de medidas de protección que consideren la función de las tripulaciones, los procedimientos que permitan aumentar la probabilidad de detección de ciberataques y la protección de sistemas sensibles a bordo.

* * *

BIBLIOGRAFÍA

1. Comité Interministerial sobre Ciberseguridad, Política Nacional de Ciberseguridad, Gobierno de Chile, 2016, http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf, obtenido de la red, agosto 2018.
2. CyberKeel, Maritime Cyber-Risks, Oct. 15, 2014, http://www.sfmx.org/support/amsc/cybersecurity/webdocs/Maritime%20Cyber%20Crime%2010-2014.pdf, accessed Jan. 1, 2015.

3. D. Ilesh, “A discussion on maritime Cybersecurity – A largelly US viewpoint”, Diginus Ltd: London. July 2015.
4. DiRenzo, Joseph & A. Goward, Dana & S. Roberts, Fred. (2015). The little-known challenge of maritime cyber security. 1-5. 10.1109/IISA.2015.7388071.
5. El Mercurio, “Banco de Chile confirma que ataque informático de mayo robó US$ 10 millones”, obtenido de internet, julio 2018, http://www.emol.com/noticias/Economia/2018/06/09/909234/Banco-de-Chile-confirma-que-ataque-informatico-de-mayo-robo-US-10-millones.html.
6. El País, El secretario general de la ONU dice que hay “ciberguerra entre Estados”, obtenido de la red agosto del 2018, https://elpais.com/internacional/2018/02/19/actualidad/1519058033_483850.html.
7. Forbes, “Cyber Crime Costs Projected To Reach $2 Trillion by 2019”, obtenido de internet agosto 2018, https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#677e5ff73a91.
8. Foresight – Future of the Sea Evidence Review Foresight, Government Office for Science, obtenido de la red, agosto 2018.https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf.
9. J. Wagstaff, “All at sea: Global shipping fleet exposed to hacking threat,” April 23, 2014, Reuters, http://www.reuters.com/article/2014/04/23/tech-cybersecurityshipping-idUSL3N0N402020140423, accessed Feb. 21, 2015.
10. Motherboard, Oct. 21, 2013, “To move drugs, traffickers are hacking shipping containers,” http://motherboard.vice.com/blog/how-traffickers-hackshipping-containers-to-move-drugs, accessed Feb. 21, 2015.
11. NIST - Glossary of Key Information Security Terms, obtenido de internet julio 2018, https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf.
12. S. Bell, “Cyber-attacks and underground activities in Port of Antwerp,” Bull Guard, Oct. 21, 2013, http://www.bullguard.com/ blog/2013/10/cyber-attacks-and-underground-activities-inport-of-antwerp.html, accessed Feb. 21, 2015.
13. The Guidelines on Cyber Security Onboard Ships Version 2.0, http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16, obtenido de la red, agosto 2018.