INSTITUTO DE INVESTIGACIONES ESTRATÉGICAS
DE LA ARMADA DE MÉXICO

DI 01/24
01/10/2024

Maestro
Juan Manuel Ávalos Ochoa

Ciberseguridad marítima y sus implicaciones al Desarrollo

RESUMEN

Las naciones se enfrentan a retos en el uso y aprovechamiento de las tecnologías en entornos digitales para mejorar el desempeño del transporte y comercio marítimo. Estas pueden representar oportunidades para mejorar las operaciones y servicios portuarios, pero también representan riesgos y amenazas en la convergencia de entornos físicos y digitales. Estos retos no sólo implican un entendimiento técnico también implican el análisis holístico y la ciberseguridad marítima, en busca de la construcción de capacidades cibernéticas para la toma de decisiones, la anticipación y la respuesta. Por ello, deben de analizarse las implicaciones sistémicas al Desarrollo Marítimo y Nacional.

Palabras clave: Resiliencia portuaria, Control de Tráfico Marítimo, Gestión de riesgos.

ABSTRACT

Nations face challenges in the use and exploitation of technologies in digital environments to improve the performance of maritime transport and trade. These may represent opportunities to improve port operations and services, but they also represent risks and threats in the convergence of physical and digital environments. These challenges not only imply a technical understanding, they also imply holistic analysis and maritime cybersecurity, in search of the construction of cybernetic capacities for decision-making, anticipation and response. For this reason, the systemic implications for Maritime and National Development must be analyzed.

Keywords: Port resilience, Maritime Traffic Control, Risk management.

INTRODUCCIÓN

El Art. 25 de la Constitución Política de los Estados unidos afirma que corresponde al Estado Mexicano la rectoría del desarrollo nacional a fin de garantizar que esta sea integral y sustentable. Dentro de los sectores que contribuyen al desarrollo nacional, el comercio marítimo es una base fundamental en el desarrollo económico y social, por lo que los puertos a través de sus instalaciones, operaciones y servicios, son un pilar

fundamental para el desarrollo de las naciones. En especial, en los países en vías de desarrollo como en México. El puerto es también un polo de desarrollo desde el punto de vista económico y social, pues en éste y sus respectivas ciudades, se realizan actividades que impulsan el desarrollo, más allá de las costas mexicanas.

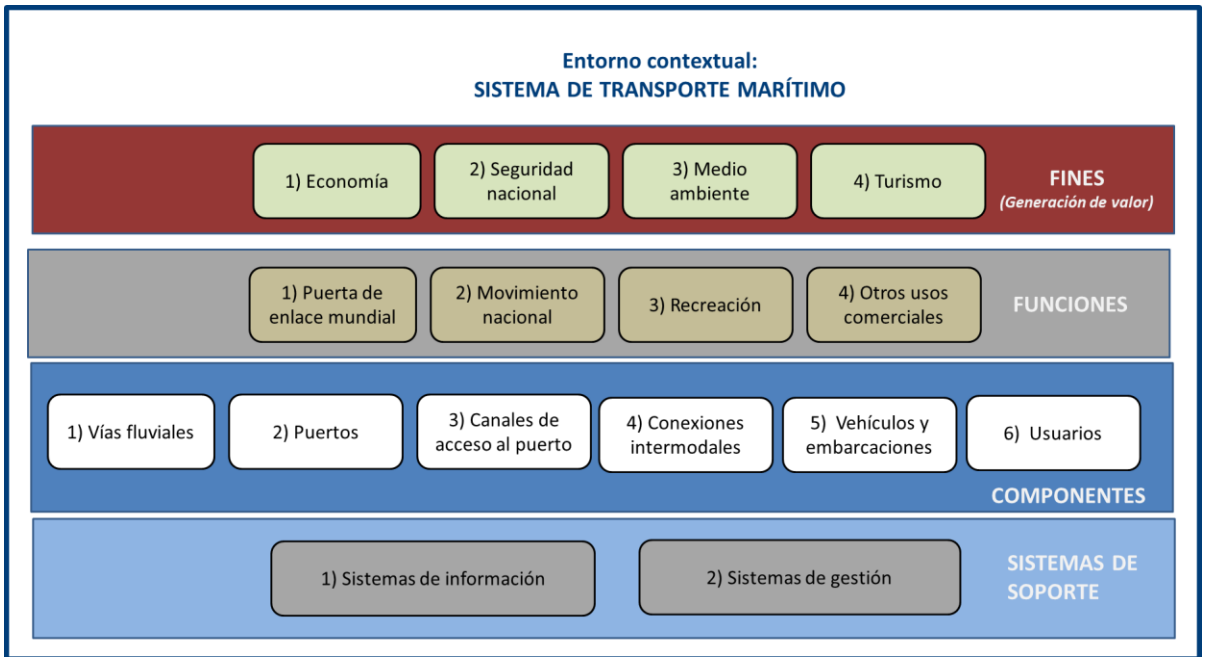
Por consiguiente, preservar la protección como condición para el desarrollo nacional significa el fortalecimiento de la seguridad en el sector marítimo. Con referencia a la evolución de las amenazas a la protección marítima, estás han ido evolucionando, utilizando herramientas y tecnologías de la información, las cuales están identificadas por parte de la OMI como amenazas potenciales en constante evolución tanto para los buques y los puertos, con afectaciones sistémicas hacia el *foreland* y *hinterland* portuario. El sector marítimo a través de los puertos se encuentra inmerso en un proceso de adaptación al nuevo entorno tecnológico, lo que deriva que los puertos deban de protegerse ante amenazas y ataques cibernéticos, ya que un ataque podría conducir a un desastre ambiental o económico (Alcaide & García Llave, 2019). Un ataque cibernético se considera un evento desestabilizador intencional causado por un individuo o un grupo, a partir de la vulnerabilidad de los sistemas ciber-físicos. Aguilar Antonio (2019) define el concepto de sistema ciber-físico, como una categoría de análisis para delimitar eventos, casos o unidades de estudio, en que las dinámicas o procesos sociales tienen repercusiones, o impactos que vinculan al internet y el espacio físico. El argumento de los hechos ciber-físicos, es exponer que existen eventos en el ciberespacio que tienen efectos tanto en el mundo físico, cómo en el virtual. Asimismo, estos al manifestarse al interior de un espacio sin fronteras como el ciberespacio, pueden tener implicaciones en los procesos, métodos y múltiples actores gubernamentales que contribuyen al Desarrollo Nacional.

DESARROLLO

En los Estados Unidos, el Sistema de Transporte Marítimo (MTS por sus siglas en inglés) es uno de los siete subsectores clave del sector de sistemas de transporte, sistema que forma parte de las 16 infraestructuras críticas nacionales de este país norteamericano, cuyos activos, sistemas y redes, ya sean físicos o virtuales, se consideran vitales para el país, tal que la incapacidad o destrucción tendrían un efecto adverso en la seguridad, la economía, la salud pública o cualquier combinación de estas. De acuerdo al US Department of Transportation (1999), el MTS se encuentra definido por cinco componentes principales, cuatro funciones y dos sistemas de soporte. Los componentes son: 1) las vías fluviales, 2) los puertos; 3) los canales de acceso al puerto, 4) las conexiones intermodales, 5) los vehículos y embarcaciones, y 6) los usuarios. Se considera que cada componente es un sistema complejo en sí mismo, donde cada uno tiene interrelación con los demás componentes. Las funciones son como puerta de enlace mundial, movimiento nacional, y recreación, y otros usos comerciales. Asimismo, el MTS considera como sistemas de soporte a los sistemas información y gestión, respectivamente. Asimismo, como sistema de transporte marítimo de los EUA, se tiene una

contribución a la generación de valor para la economía, la seguridad nacional, el medio ambiente y la recreación.

Figura 1 Sistema de Transporte Marítimo



Fuente: Elaboración propia

Los puertos, suelen entenderse como instalaciones que permiten el manejo de bienes y personas provenientes de rutas marítimas, que pueden conectarse a modos de transporte terrestres. La acepción de los puertos ha cambiado de la dimensión espacial o física a sus implicaciones económicas, en concordancia con el impacto de la tecnología en la infraestructura y operaciones portuarias, lo que implica riesgo y amenaza del uso integrado de la tecnología.

En el contexto marítimo y portuario nacional, se distingue la aplicación de tecnologías enfocadas principalmente a la digitalización de información, la automatización de procesos operativos, la conectividad entre el buque y el puerto, el análisis de grandes volúmenes de información de las operaciones marítimas, el mantenimiento remoto de sistemas, y el control en tierra de las operaciones portuarias autónomas, por mencionar algunas. Por ello, se distinguen dos grandes categorías de tecnologías utilizadas por los buques, puertos e instalaciones portuarias, que sostienen sus procesos: 1) tecnologías de información; y 2) tecnologías de operación. Las tecnologías de información, son aquellas que tienen la capacidad de adquirir, almacenar, analizar, evaluar, manipular, gestionar, mover, controlar, visualizar, conmutar, intercambiar, trasmitir o recibir cualquier dato de información (National Institute of Standards and Technology, 2017).

Ejemplos de estas, se encuentran aplicadas en los sistemas de navegación de los buques y sistemas de control, monitoreo y vigilancia de los puertos.

Asimismo, las tecnologías de operación aplicadas a los dispositivos programables detectan o provocan un cambio directo en un dispositivo a través del monitoreo y control (National Institute of Standards and Technology, 2018) . Ejemplos de estas tecnologías en el sector marítimo y portuario, se pueden presentar en el sistema de control de máquinas de los buques, los sistemas de monitoreo y control de carga en los puertos, así como en los procesos de revisión y gestión que llevan a cabo las aduanas.

La ciberseguridad marítima se conceptualiza como el conjunto de acciones tomadas por la comunidad marítima y portuaria para proteger, prevenir y reaccionar ante un ataque cibernético en los buques y terminales portuarias. En ese mismo sentido, la OMI considera a la gestión de riesgos cibernéticos como el proceso de identificación, análisis, evaluación y comunicación de riesgos de que involucra la 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 Comité de Seguridad Marítima, en su 98º período de sesiones, en junio de 2017, adoptó la Resolución MSC. 428 (98), Gestión de los Riesgos Cibernéticos Marítimos en los Sistemas de Gestión de la Seguridad. El riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posible, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas. La gestión de los riesgos es fundamental para la seguridad y la protección de las operaciones del transporte marítimo.

Anand & Grainger (2018) desde un enfoque de análisis de los riesgos a la infraestructura marítima y portuaria proponen que para mejorar la protección y seguridad de esta, debe considerarse como elementos críticos de la infraestructura nacional, es necesario primeramente entender el concepto operacional de un puerto, más allá de una integración de modos de transporte terrestre y marítimo, el cual debe considerar la combinación de tres perspectivas: 1) como instalaciones económicas; 2) como nodos en la cadena de suministro; y 3) como áreas de actividad humana y económica. Si bien en México no se tiene la definición “infraestructura crítica nacional”, a nivel global, es un término que se utiliza para describir aquellos activos físicos y cibernéticos para la prestación de servicios esenciales para mantener la seguridad y el desarrollo nacional de un país.

Por ejemplo, el ataque a la línea naviera Maersk en 2017 le costó a la empresa aproximadamente USD 300 millones. El reciente bloqueo del Canal de Suez, aunque no está relacionado con un ataque de seguridad cibernética, tuvo afectaciones del 12% del comercio mundial, lo que permite reflexionar sobre si el origen hubiera sido un fenómeno cibernético desestabilizador, se tendrían pérdidas económicas similares. A partir

de 2017, los principales puertos del mundo fueron objeto de aproximadamente 12 ataques por día. Además, en promedio, los armadores pagan aproximadamente USD 3,1 millones en rescate debido a ciberataques marítimos (Afenyo & César, 2023).

En el caso de México, los puertos mexicanos no son considerados dentro de la categoría de instalaciones estratégicas, ya que alguna afectación a debido a la interrelación existente entre buques, mercancías y transporte terrestre su existencia, permanencia y continuidad de sus operaciones ocasionaría afectaciones al desarrollo social y económico del país (Valenzuela, 2020).

Las afectaciones derivadas de los ataques cibernéticos como eventos desestabilizadores al sector marítimo y portuario tienen implicaciones al Desarrollo Marítimo Nacional y sus intereses marítimos. Un ataque cibernético a la interfase puerto-buque genera una interrupción en el tráfico marítimo, lo que tendría como consecuencia retrasos, altos costos e impactos irreversibles, que se traducen en pérdidas económicas al comercio marítimo, que originaría la disminución de la eficiencia de las Cadenas Logísticas Marítimo y Portuarias. Por otro lado, una interrupción cibernética en la operación de las terminales portuarias generaría un riesgo a la conectividad del hinterland portuario y el transporte intermodal, lo que afectaría considerablemente a la reputación de las operaciones y servicios portuarios, lo que implicaría un aumento en los seguros para las líneas navieras para el transporte, almacenamiento y distribución de bienes. De igual manera, una afectación cibernética ya sea en la interfase del buque-puerto o en las terminales portuarias, podría interrumpir las actividades de la gente de mar y ocasionar daños al medio ambiente marino, con la dificultad de evaluar los daños y las pérdidas ocasionadas por este.

CONCLUSIONES

Las tecnologías de la información, las comunicaciones y las operaciones han contribuido al desarrollo de las organizaciones y las naciones. En el sector marítimo, estas tecnologías han servido como vehículo para mejorar la eficiencia en los servicios y las operaciones portuarias. Pero esta incorporación de tecnologías, suponen una exposición, donde son explotadas por delincuentes, terroristas y grupos del crimen organizado, lo que afecta no solamente el Desarrollo Marítimo Nacional, sino también el Desarrollo Nacional.

Las naciones y la comunidad portuaria están colaborando en el diseño, implementación y desarrollo de mejores prácticas de ciberseguridad adecuadas para proteger y mejorar la resistencia de los sistemas cibernéticos en los que se apoya el funcionamiento de los puertos, buques, instalaciones marinas y otros elementos del sistema del transporte marítimo. Hasta la fecha, se tiene una preferencia en la Comunidad Portuaria por adoptar medidas orientadas específicamente a la seguridad cibernética de los buques, más que las instalaciones portuarias.

Para el desarrollo de la ciberseguridad marítima deben de establecerse mecanismos de capacitación, colaboración y cooperación para hacer frente a los riesgos y amenazas en el ciberespacio. Se destacan cinco funciones principales para hacer frente ante posibles ataques en el ciberespacio: 1) identificar; 2) proteger; 3) detectar; 4) responder; y 5) recuperar. Para lo que en lo que respecta a las etapas uno y dos se basan en procesos de anticipación, análisis del entorno y generación de alertas temprana. Asimismo, para las etapas cuatro y cinco se involucran procesos de planeación y toma de decisiones, así como también la exploración de posibles escenarios y amenazas que podrían presentarse en el futuro.

BIBLIOGRAFÍA

Afenyo, M., & César, ,. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean and Coastal Management, 236*.

Aguilar Antonio , J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. (Flacso-Ecuador, Ed.) *URVIO Revista Latinoamericana de Estudios de Seguridad*, 24-40.

Alcaide, J. I., & García Llave, R. (2019). Critical infrastructures cybersecurity and the maritime sector. *AIIT 2nd International Congress on Transport Infrastructure and Systems in a changing world*.

Anand, N., & Grainger, A. (2018). The port as a critical piece of national infraestructure. *Safety and Reliability, 37*(2-3), 106-127.

National Institute of Standards and Technology. (2017). *An Introduction to Information Security.*

National Institute of Standards and Technology. (2018). *Risk Management Framework for Information Systems and Organizations.*

US Department of Transportation. (1999). *An Assesment of the U.S. Marine Transportation System.* A report to Congress.

Valenzuela, J. E. (2020). Los puertos nacionales: instalaciones estratégicas de México. *Revista del Centro de Estudios Superiores Navales*, 231-262.