EDITORIAL ESDEG

Revista
Ensayos sobre Estrategia Marítima
Volumen 6, número 16, julio-diciembre 2022
Bogotá, D.C., Colombia
ISSN: 2500-4735 • eISSN: 2981-3026
Página web: https://esdegrevistas.edu.co/index.php/rema

El ciberespacio: una variable determinante dentro del Poder Marítimo del país en la era digital

Cyberspace: a determining variable within the country's Maritime Power in the digital age

Jorge Ricardo Espinel Bermúdez

CITACIÓN APA:

Espinel Bermúdez, J. R. (2022). El ciberespacio: una variable determinante dentro del Poder Marítimo del país en la era digital. *Ensayos sobre Estrategia Marítima, 6*(16), 79-95. https://doi.org/10.25062/2500-4735.3125

Publicado en línea: **Diciembre 30 de 2022**

Enviar un artículo a la Revista

Revista **Ensayos sobre Estrategia Marítima**
Volumen 6, número 16, julio-diciembre 2022 (pp. 79-95)
Bogotá, D.C., Colombia

EDITORIAL ESDEG

El ciberespacio: una variable determinante dentro del Poder Marítimo del país en la era digital

Cyberspace: a determining variable within the country's Maritime Power in the digital age

DOI: https://doi.org/10.25062/2500-4735.3125

Jorge Ricardo Espinel Bermúdez
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D.C., Colombia

Resumen

El presente escrito pretende acercarse hacía cómo el Poder Marítimo de un país, en una era digital, requiere del uso del ciberespacio de una manera efectiva. De modo, que a través de éste pueda alcanzar una ventaja sobre otros Estados. Para lo cual, mediante la revisión bibliográfica se buscó entender el concepto de Poder Marítimo, el de Ciberespacio, cuál es la relación entre estos dos conceptos, para mostrar cómo a través de la superioridad de la información se puede encontrar una ventaja competitiva. Por lo tanto, se pudo concluir que a través del uso sistemas centrados en redes se alcanza una conciencia situacional de todo el dominio marítimo, el cual permite mejorar sus operaciones, y ser más efectivos en este mundo globalizado. De igual manera, se concluye que el uso efectivo del ciberespacio por parte del Poder Marítimo trae consigo beneficios en el bienestar y desarrollo de la nación.

Palabras Clave: Ciberespacio; Poder Marítimo; Superioridad de la Información; Sistema de Transporte Marítimo; Tecnologías de la Información y la Comunicación.

Abstract

This paper aims to approach how the Maritime Power of a country, in a digital age, requires the use of cyberspace in an effective way. So, that through it you can achieve an advantage over other states. For which, through the bibliographic review, we sought to understand the concept of Maritime Power, that of Cyberspace, what is the relationship between these two concepts, to show how through the superiority of information a competitive advantage can be found. Therefore, it was possible to conclude that through the use of network-focused systems, a situational awareness of the entire maritime domain is achieved, which allows improving its operations, and being more effective in this globalized world. In the same way, it is concluded that the effective use of cyberspace by the Maritime Power brings benefits in the well-being and development of the nation.

Key words: Cyberspace; Maritime Power; Information Superiority; Maritime Transportation System; Technology of the information and communication.

Artículo de reflexión
Recibido: 1 de agosto de 2022 • **Aceptado:** 7 de noviembre de 2022
Contacto: Jorge Ricardo Espinel Bermúdez jorge.bermudez@esdeg.edu.co

Introducción

La globalización es un fenómeno que ha fomentado la aceleración de la interdependencia entre los Estados, al ser un mundo más compacto. El desarrollo tecnológico y de las comunicaciones son dos aspectos claves para la globalización, los cuales han traído como consecuencia la compresión de los factores tiempo y espacio. Además, existen otros conceptos que se han visto afectados por la globalización, entre los cuales están; la integración global, el reordenamiento de las relaciones de poder, la conciencia de la condición global, el aumento de la conectividad interregional (Kenna, 2008). Asimismo, el Almirante Mike G. Mullen (Comandante de la Armada de los Estados Unidos para el 2015) y el Vicealmirante John G. Morgan de la Marina de los Estados Unidos, manifestaron que la globalización ha cambiado los cálculos de seguridad, porque ésta hace un mayor énfasis en lo económico, siendo éste el elemento central según el cual se debe organizar la estrategia marítima de cualquier país. De igual manera, la globalización ha estado dirigida por la revolución de las tecnologías de computación y de las telecomunicaciones; para la expansión del pensamiento occidental, sus normas, cultura en un movimiento de carácter mundial hacia una economía de libre comercio (Haynes, 2015).

De igual manera, hay que notar que mucho de ese libre comercio se hace a través del medio marítimo. Como se expone en el informe sobre el transporte marítimo emitido por la Conferencia de la Naciones Unidas sobre el Comercio y el Desarrollo (UNCTAD por sus siglas en inglés), en el mundo se transportaron un total de 11 mil millones de toneladas en el 2019 (Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, 2019), en contraste con lo transportado por vía aérea de acuerdo con datos del Banco Mundial y la Organización de Aviación Civil Internacional (OACI), 215 millones de toneladas (Banco Internacional de Reconstrucción y Fomento, 2021). En Colombia, el 97.8% de la carga que llega al país es por vía marítima (Dirección de Impuestos y Aduanas Nacionales, 2018), y para los Estados Unidos de América, los puertos marítimos manejan el 99. 4% de la carga (Twist et al., 2017). Lo cual indica que la vía marítima es el principal medio para el transporte a nivel mundial. Y el que está asociado directamente al poder marítimo de cada nación.

Asimismo, el sector marítimo ha sido impactado por la revolución de las tecnologías de la información de las telecomunicaciones. De manera tal, que el medio marítimo ha tenido una creciente dependencia de esas tecnologías como se puede observar en la electrónica a bordo de las unidades, la informatización de sus sistemas o la puesta de redes en las naves, armadores y los puertos (Centre d›études stratégiques de la Marine, 2015).

Prácticamente casi todos los sistemas de los buques, aviones, submarinos y vehículos no tripulados cuentan con algún grado de interconexión (Secretary of Defense, 2012). El transporte marítimo se apoya cada vez más de soluciones digitales para el

cumplimiento de sus tareas, optimización operacional, ahorro en costos, y seguridad, lo cual lleva a la industria marítima a ser un negocio más sustentable (BIMCO et al., 2020). También la manera en que se controla y gerencia el comercio marítimo ha evolucionado, es por eso que cada vez más los puertos dependen de redes de computadores, en las cuales a través de sistemas de monitoreo de carga se puede seguir el estado de un contenedor, el cual puede estar en tránsito en un buque mercante o guardado en una bodega del puerto (Kramek, 2013). Por lo tanto, se puede afirmar que las tecnologías de la información y de la comunicación se encuentran inmersas dentro de todo el sector marítimo.

Si bien el aumento y la implementación de los desarrollos en tecnologías de la información y de la operación traen consigo una amplia gama de beneficios al sector marítimo, también traen unas potenciales vulnerabilidades y riesgos (BIMCO et al., 2020). Ese crecimiento masivo en la interconexión y conexión de dispositivos en el ambiente marítimo aumenta la superficie de ataques, la cual permite unos efectos físicos, e impacta sobre todo los costos en seguridad (Ablon, 2017). Como ejemplo, están los casos de los puertos de Barcelona y San Diego que durante septiembre de 2020, fueron objeto de ataques cibernéticos, los cuales no fueron ampliamente difundidos y cuya naturaleza tampoco es clara (Cimpanu, 2020). De manera que este tipo de ataques no sólo pueden afectar a la industria marítima en lo operacional, sino en campos como el económico, en su imagen y confiabilidad. Lo que hace necesario de un uso adecuado y eficaz del ciberespacio.

En relación con lo anteriormente expuesto, se puede observar que los componentes del Poder Marítimo tienen una alta dependencia de las tecnologías de la información, la operación y la comunicación, y que, a través del uso adecuado de éstas, los Estados obtienen una ventaja competitiva. De manera que, este artículo pretende acercarse a responder a la pregunta: ¿Cómo un país puede potencializar su Poder Marítimo a través de desarrollar la capacidad de operar efectivamente en el ciberespacio? Para lo cual, se ha desarrollado el presente escrito a través de una metodología cualitativa. Mediante la revisión bibliográfica de fuentes primarias y secundarias, se busca tener una perspectiva interpretativa de las acciones que se van captando durante el desarrollo de la investigación. Por ello, se ha divido el presente escrito varias partes. Primera, entender el concepto de Poder Marítimo, cuáles son sus componentes y cómo las tecnologías influyen en este hoy en día. Segunda, comprender qué es el ciberespacio, cuál es su alcance y componentes. Tercera, ver la relación que existe entre el ciberespacio y el sector marítimo, cómo ese sector se ve influenciado y qué amenazas le trae ese ciberespacio. Por último, presentar un concepto que está relacionado con el uso efectivo del ciberespacio y cómo se aplica no sólo a al sector a la competitividad desde lo militar sino desde el sector marítimo, el concepto de superioridad de la información

. ¿Qué se entiende por poder marítimo?

Geofrey Till (2013) define al Poder Marítimo desde dos perspectivas. Una primera, que él llama aportes, entre los cuales están las marinas militares y civiles, los guardacostas, la industria del sector marítimo, y que está asociado a las actividades del mar (Till, 2013). Asimismo, Till (2013) afirma que además de los anteriores aportes, están la contribución que hacen las fuerzas terrestres y aéreas. Estos constituyentes del Poder Marítimo se encuentran dentro del Poder Nacional, la manera en la que estos interactúan es cómo se alcanza ese Poder Marítimo (Till, 2013). La siguiente figura da una ilustración de esa perspectiva propuesta por Till (2013) en la que muestra los constituyentes del Poder Marítimo y su puesto dentro de Poder Nacional.

Gráfica 1. El Poder Marítimo y su entorno
Fuente: Elaboración propia, basado en el libro Seapower (Till, 2013)

La segunda perspectiva sobre el Poder Marítimo que plantea Till (2013) es desde el resultado. El poder marítimo no es simplemente quién usa el mar, sino también quién tiene la capacidad para influenciar a otras personas o cosas, sobre lo que se hace en o desde el mar. Esta parte del Poder Marítimo está definido por sus consecuencias y los fines, no por los medios (Till, 2013).

Además, Andrew Lambert (2018), considera que el Poder Marítimo (*Seapower*) está relacionado al concepto de la antigua Grecia - Talasocracia, que son Estados marítimos cuya relación con el mar va desde lo político, el desarrollo económico, el arte y la identidad, y que va más allá de la simple adquisición de una marina (Lambert, 2018). Es por

eso que el Poder Maritimo *Seapower* está constituido a través de una identidad nacional (Lambert, 2018). De igual manera Lambert (2018) diferencia el *Seapower* del concepto de *Sea Power*, la cual se una estrategia del Poder Naval. En tal sentido se puede decir que el *Seapower* es cuando un Estado dirige su atención hacia el mar, para asegurar la economía y las ventajas estratégicas de tener el control de mar para actuar como una gran potencia, a través de la construcción de manera deliberada de una cultura e identidad marítima.

De tal manera que es necesario tener el control de las líneas de comunicación marítimas para la cohesión entre el Estado y el mar, mantener el comercio con otros y el control de esa área para proteger esos intereses en el mar.

Por otra parte, Mahan (1890) define los elementos del poder marítimo *Sea Power* entendiendo este concepto como una estrategia para que una nación alcance ese Poder Marítimo *Seapower* y llegue a ser una nación marítima. No hay que olvidar ese contexto histórico en el que se encontraba Mahan, quien pretendía cambiar la mentalidad de los Estados Unidos en el momento en el que el escribió su libro, quien ha logrado que su pensamiento perdure hasta nuestros días. De tal modo, Mahan (1890) plantea que toda nación que desee alcanzar ese Poder Marítimo debe tener los siguientes elementos: Posición geográfica, Conformación física, Extensión del territorio, Cantidad de población, Carácter nacional y Carácter del Gobierno (Mahan, 1890)

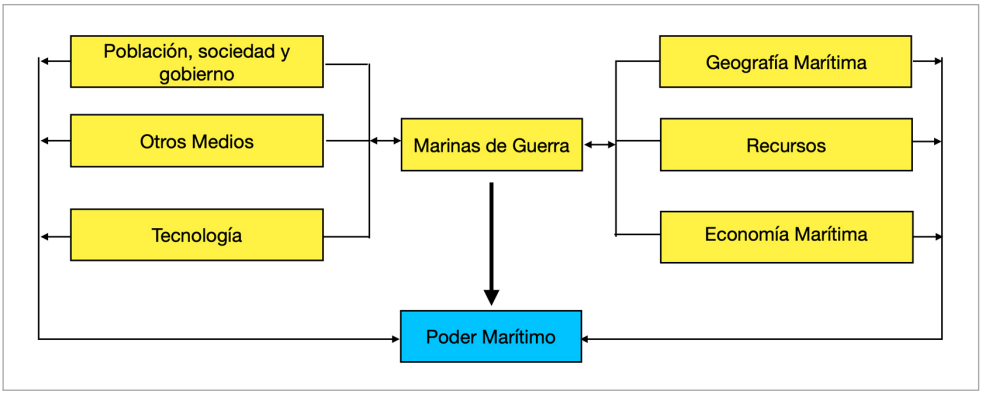
Estos elementos, permiten que la nación vislumbre hacia dónde debe enfocar sus esfuerzos si quiere llegar a tener o alcanzar ese Poder Marítimo. Lo cual lleva a preguntarse si esos elementos se encuentran vinculados hoy en día a las tecnologías de la información y la cuarta revolución industrial.

De acuerdo con el Almirante James Stavridis en su libro *Sea Power*, la visión de Mahan sigue siendo vigente y se adapta a los cambios que ha traído el siglo XXI como son los avances tecnológicos, las nuevas normas internacionales, entre otros. Asimismo, Stavridis (2018) planteó que, para el caso de los Estados Unidos, esta continua el planteamiento de Mahan al seguirse representándose como una nación marítima, a través de una amplia flota mercante, una poderosa y capaz marina, una robusta industria de astilleros, una flota pesquera competitiva, puertos e infraestructura marítima eficientes, la capacidad de rompehielos en el Ártico y la amplia capacidad de vigilar el océano en las aproximaciones de la nación. Todo los anterior con el apoyo de la tecnología (Stavridis, 2018).

De la misma manera, Till (2013) menciona que el Poder Marítimo (Seapower) es el producto de una combinación e interconexión de componentes que son difíciles de identificar. Estos componentes son atributos de los países que hacen que alcanzar esa fortaleza en el mar sea más fácil o difícil (Till, 2013). Si se toma al Poder Marítimo

(Seapower) como esa capacidad para influenciar el comportamiento de otras personas con respecto a lo que hacen en o desde el mar, entonces esos atributos pueden ser aceptados como parte de esa mezcla de elementos como la que planteó Mahan.

De hecho, esos componentes están en constante cambio de acuerdo con una variedad de desarrollos sociales, económicos, tecnológicos y políticos. De manera que esos componentes contribuyen de una manera particular al Poder Marítimo, unos de manera directa, como mantener una amplia flota comercial. Y otros, de una forma indirecta, que influyen en ese Poder Marítimo al contribuir a la efectividad de uno o más componentes del poder marítimo, como son sus marinas de guerra y en cierta medida también las tecnologías. Entre los principales componentes expuestos por Till (2013), están: Población, sociedad y gobierno asociado a lo marítimo, Tecnología, Geografía Marítima, Recursos, Economía Marítima, Marinas de Guerra (Till, 2013), los cuales se pueden ver representados en la gráfica 2.

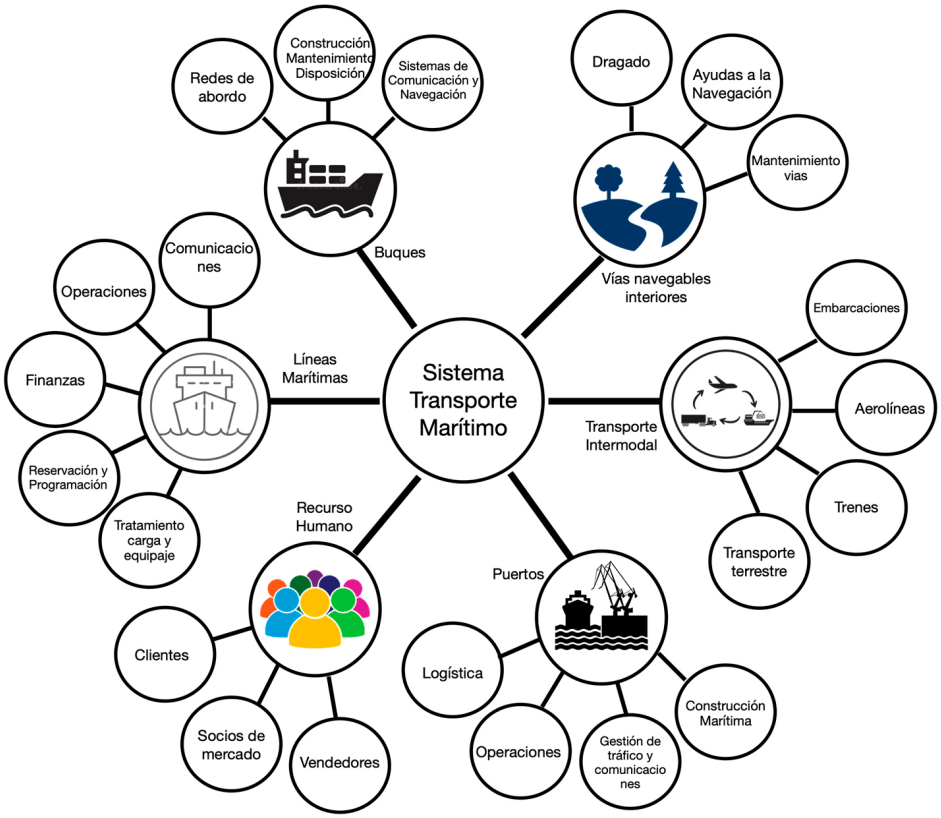


Gráfica 2. Componentes del Poder Marítimo
Fuente: elaboración propia. Basado en el Libro Seapower. (Till, 2013)

Dentro de los componentes del poder marítimo descritos en la gráfica 2, la tecnología sería el componente en el cual se centra el presente artículo. Ya que es el componente en el cual se ven influenciados tanto el Poder Marítimo como la Marina de Guerra, se podría decir que ese componente en la actual era de la información es transversal a muchos de los otros componentes. Sin embargo, para el caso de una marina de guerra latinoamericana, que está asociada a las limitaciones de su presupuesto, el cual determina no solo la obtención de sus unidades de guerra, si no de la capacidad tecnológica. De manera que, estas marinas pretender tener un Poder Naval representativo, el cual se ve reflejado en su flota, y está asociado a la Jeune École, en la cual se contempla que los buques deben tenerse de una manera desagregada e individual, los cuales deben ser de menor tamaño a los antiguos destructores de la Segunda Guerra Mundial. Pero, hoy en día, además se

habla que estas unidades deben estar interconectadas para que puedan actuar de una manera cohesionada (Till, 2013). En ese mismo sentido, los buques de guerra son cada vez más dependientes de las Tecnologías de la Información y la Comunicación (TIC), y de las Tecnologías de la Operación (TO), lo cual incluye los sistemas de combate, comunicaciones, ingeniería, posición, navegación y sincronización.

Por otra parte, se encuentra el Sistema de Transporte Marítimo (STM), que es un sistema de sistemas. El STM está compuesto por seis sistemas interconectados; buques, líneas marítimas, puertos, recurso humano, vías navegables interiores y transporte intermodal (Kessler y Shepard, 2020). Estos subsistemas del STM logran su interconexión gracias a las Tecnologías de la Información y la Operación. La gráfica 3 muestra la configuración del STM. Muchos de esos componentes están directamente ligados a las TI, por lo tanto, se puede decir que el desarrollo del Poder Marítimo de una nación está vinculado con el grado de tecnología que ésta aplique en todo el ecosistema del sector marítimo, tanto para la defensa en la marina de guerra como en el resto del sector, el cual incluye el sistema de transporte marítimo.



Gráfica 3. El Sistema de Transporte Marítimo

Fuente: elaboración propia. Basado en el Capítulo de (Kessler & Shepard, 2020).

¿Qué se entiende por ciberespacio?

Es necesario entender qué es el ciberespacio, un término acuñado por William Gibson en una historia publicada en 1982, y que posteriormente fué tomado por la literatura de ciencia ficción como la película "*The Matrix*". El ciberespacio entra en el mundo real en los años 1990 con nacimiento de la Red Mundial (Word Wide Web) (Reveron, 2012). El Departamento de Estado de los Estados Unidos ha definido al ciberespacio como un dominio global dentro del ambiente de la información que consiste de la interdependencia de redes de infraestructura de tecnologías de la información, el Internet, las redes de telecomunicaciones, sistemas de computación, e incluye procesadores y controladores (Congressional Research Services, 2021).

De tal manera, el ciberespacio es algo que suena como de otra dimensión, pero es algo mucho más mundano. Éste se encuentra en el computador personal, o en ese portátil que lleva un niño a la escuela, en el computador del trabajo, está en un edificio monótono sin ventanas del centro, en una tubería que pasa por debajo de la calle, se puede decir que está en todas partes, en cualquier parte hay un computador, un procesador, y un cable que nos está conectando. (Clarke & Knake, 2011)

De modo que, el Ciberespacio son todas esas redes de computadores en el mundo, es todo lo que está conectado y controlado (Clarke & Knake, 2011). No es sólo Internet, éste hace parte del ciberespacio, porque es una red de redes, y desde cualquier red de Internet es posible comunicarse con cualquier computador que esté conectado a la red (SIPA, 2017). De igual manera, no sólo existen esas interconexiones entre computadores, sino que además hay unas relaciones entre los usuarios de este dominio, las cuales se asemejan a las que se realizan en el mundo físico, aunque estas por su volumen, cobertura y velocidad se consideran como instantáneas, colectivas y mundiales (Gómez A, 2013).

El ciberespacio incluye además del Internet otras redes que no están conectadas directamente a éste. Son redes privadas que teóricamente están separadas (Clarke & Knake, 2011). También hacen parte del ciberespacio las redes transaccionales desde la cuales se pueden hacer cosas como el flujo de dinero, mercado de valores, y transacciones de tarjetas de crédito. Adicionalmente, están las redes que son controladores de sistemas, las cuales permiten la comunicación entre máquinas, como los paneles de control que manejan bombas, elevadores y generadoras, como los sistemas de control industrial (ICS).

De igual manera, Eissa et al (2012), hace referencia a que el ciberespacio tiene un carácter global, en el cual existe una transferencia y producción de información. Este nuevo entorno de tráfico de información, el cual no se constituye como un espacio en sí mismo, sino como una superficie superpuesta, traspasa a las otras dimensiones físicas

conocidas (Eissa et al., 2012). Asimismo, Gómez (2012) considera al ciberespacio como un Global Common, entendiéndose como una figura del derecho británico que trata de aquellos espacios que, sin ser de propiedad de ningún vecino, son explotados por la comunidad para su beneficio. De manera que esos Commons globales son aquellos dominios que no cuentan con alguna soberanía, pero son utilizados por las naciones para transportar bienes o servicios o transmitir datos.

Entre estos Commons están las aguas internacionales, el espacio aéreo, y el espacio exterior. Y, actualmente, se habla del Ciberespacio como otro de los Commons, por donde transitan datos e información (Feliu Ortega, 2012).

En ese mismo sentido, Feliu (2012) afirma que ese Common Global del ciberespacio cuenta con unas características que lo diferencian de los otros dominios (Terrestre, Marítimo, Aéreo, y Espacial):

1. El ciberespacio no tiene fronteras geográficas, los que desarrollan ataques pueden hacerlo desde cualquier lugar del planeta y son difícilmente localizados.
2. La defensa de este espacio se hace muy compleja debido a la variedad de factores que en éste intervienen, ya que no solo existen elementos de carácter estatal sino privados, lo que conlleva a una cercana coordinación entre ellos.
3. El enfrentamiento que se sucede en el ciberespacio tiene la particularidad de un conflicto irregular, debido a que muchas veces alguno de los bandos puede ser inferior en medios tecnológicos. Con muy pocos medios y baratos se pueden obtener resultados catastróficos. Además, normalmente son anónimos y clandestinos, lo cual atrae no sólo al gobierno sino también a organizaciones al margen de la ley.
4. El ciberespacio debe considerarse en una estrecha relación a los otros dominios.
5. El uso del ciberespacio permite que se obtenga información sobre un objetivo sin que éste sea destruido o neutralizado un sistema, inclusive sin llegar a ser detectado.
6. Puede ser utilizado para ejercer presión y disuasión.
7. Es un dominio que evoluciona de una manera rápida y sigue la misma velocidad con que están evolucionando las tecnologías de la información y la comunicación. (Feliu, 2012, p 45)

Así mismo, Clark (2012) afirma que el ciberespacio no es sólo un computador, que éste lo hacen las interconexiones, las cuales hoy se asocian al Internet, pero existen muchas otras alternativas de interconexión. Por lo tanto, Clark (2012) plantea un modelo para poder caracterizar el ciberespacio y lo llama modelo de capas. Las cuales las ha definido de la siguiente manera:

1. La capa compuesta por las personas, que son los que participan de esa experiencia cibernética, las que comunican, trabajan con la información, toman decisiones y llevan a cabo planes, y son ellas mismas las que transforman la naturaleza del ciberespacio mediante el trabajo con los servicios de los componentes cibernéticos y sus capacidades.
2. La capa en donde la información es guardada, transmitida, y transformada en el ciberespacio.
3. La capa compuesta por los componentes básicos lógicos que conforman los servicios y soporte a la plataforma de la naturaleza del ciberespacio.
4. La capa de las fundamentaciones físicas que suministran los elementos lógicos (Clark, 2010)

En conclusión, se puede decir que ese espacio en el cual se producen una cantidad de interacciones de carácter físico y lógico, a través del intercambio de datos e información, en el cual participan personas, computadores, redes como Internet y las redes de telecomunicaciones, las infraestructuras de la tecnología de la información y la operación, entre muchos otros actores, se denomina ciberespacio. Además, que éste tiene una relación estrecha y directa con otros los dominios ya existentes, entre los que se destaca el Marítimo como objeto de este artículo.

Relación entre el sector marítimo y el ciberespacio

El dominio marítimo no ha sido ajeno a ese mundo digital, a través de la interconexión, cada día más dispositivos están conectados a redes y al Internet (Ablon Lily, 2017). Prácticamente casi todos los sistemas en los buques, aeronaves, submarinos y vehículos no tripulados están conectados en algún grado. Lo que incluye no sólo a los sistemas de combate, sino a las comunicaciones, ingeniería, y sistemas de navegación, posicionamiento y sincronización (Secretary of Defence, 2012). Asimismo, dentro de ese ambiente marítimo se encuentran otros dispositivos conectados al ciberespacio como son: los sistemas computarizados de gestión de cargas y terminales marítimas, los puentes grúas intercomunicados, capacidades de seguimiento de buques y cargas, cámaras de seguridad, almacenamiento de combustible, sistemas de gestión logística, sistemas de conciencia situacional, y muchos otros sistemas y dispositivos (Ablon, 2017). De manera que, el Sistema de Transporte Marítimo, la Industria Marítima y sus fuerzas navales como componentes del Poder Marítimo del país se encuentran estrechamente ligadas y dependientes de Ciberespacio para su operación.

De igual manera, el desarrollo de las Tecnologías de la Información (IT) y la operación (OT), traen consigo una mayor disponibilidad de datos, mayor velocidad de procesamiento y de transferencia de éstos entre los involucrados de toda la industria marítima,

lo cual hace que se incrementen las posibilidades para una óptima operación, ahorro de costos, incremento de la seguridad, y un negocio más sustentable y rentable (BIMCO, 2020). Asimismo, el uso de las capacidades que brindan esas tecnologías tanto IT como OT a través del ciberespacio, le proporcionan una ventaja continua en el ambiente operacional al Poder Naval, lo cual contribuye de manera relevante a la seguridad física y económica de la nación (Joint Chiefs of Staff, 2018). Por lo tanto, esa interacción con el ciberespacio entre el sector marítimo y su Poder Naval le permite al Poder Marítimo del país tener una ventaja competitiva con respecto a los países que no cuentan con esas capacidades tecnológicas.

Sin embargo, estos desarrollos traen consigo un riesgo crítico a los sistemas y procesadores vinculados a los sistemas de operación del ambiente marítimo. Existen diferentes tipos de actores cibernéticos maliciosos que desean tomar ventaja tanto de las vulnerabilidades del software como de las humanas (Robinson et al., 2013). Estos actores, los cuales provienen de múltiples fuentes desde los patrocinados por un Estado, criminales cibernéticos, hacktivistas, hasta terroristas cibernéticos, los cuales tienen diferentes motivaciones, pero que pueden causar estragos sobre la tecnología conectada en el ambiente marítimo (Ablon, 2017). De manera que pueden llevar a cabo ataques sobre sistemas como los de posicionamiento (GPS) de los buques para producir interferencia o bloqueos de sus señales, o producir una suplantación de señal conocida como Spoofing (Goward, 2017). Lo que trae consecuencias graves para la seguridad de la navegación, la vida de los tripulantes y la economía del sector marítimo.

Casos de ataques cibernéticos, como el sucedido a la empresa Maersk en el 2017, uno de los gigantes del transporte marítimo que sufrió un ataque mediante el uso de un software malicioso de nombre NoPetya, de tipo Ramsonware que imitaba al software Wannacry, tuvo como consecuencia que el sistema de reservas quedó paralizado, y el sistema de seguimiento de contenedores se puso más lento, haciendo que las operaciones en los 80 puertos alrededor del mundo donde tiene operaciones estuvieran suspendidas alrededor de tres días, lo cual llevó a que tuvieran una pérdida cercana a los 26 millones de dólares (Marta, 2020).

De igual manera, la naviera CMA CGM, la tercera del mundo por volumen de negocio, sufrió un ataque cibernético en el año 2020, el cual afectó al sistema de comunicaciones internas de la compañía, teniendo que interrumpir todos los accesos a su red para poder aislar al software malicioso (EuropaSur, 2020). Este tipo de ataque afecta las navieras al detener no solo su operación sino su proceso administrativo, con consecuencias económicas y sobre todo reputacionales.

De igual forma, está la alerta lanzada por el cuerpo de Guardacostas de los Estados Unidos a todos los buques comerciales sobre las vulnerabilidades a ataques cibernéticos, la cual fue lanzada debido a un incidente ocurrido en febrero de 2019 en un buque de transporte de pasajeros que iba de Nueva York a Nueva Jersey, y que fue impactado por

un ataque cibernético mediante un software malicioso, el cual perturbó gravemente los sistemas de control del buque. Afortunadamente la acción de la tripulación logró mitigar el riesgo a tiempo y que éste no se convirtiera en el mayor accidente por pérdida de control de un buque (Goud, 2019). Esto lleva a pensar en la importancia de la ciberseguridad, y el impacto que pueden tener estos ataques en toda la industria marítima y la forma de manejar de una manera adecuada y efectiva el ciberespacio.

Superioridad de la Información un medio para un uso efectivo del ciberespacio

Una vez entendidos los conceptos de Poder Marítimo y Ciberespacio, surge la pregunta ¿Cómo podemos usar el Ciberespacio de una manera adecuada y eficaz, para propender por el Poder Marítimo? Para poder utilizar el Ciberespacio de una forma adecuada y eficaz, es necesario tener la libertad de acción en él, de modo que la información que transite, esté disponible, sea íntegra, auténtica y mantenga su confidencialidad (Joint Chiefs of Staff, 2018). Para alcanzar esa libertad de acción en el Ciberespacio se requiere de la habilidad de recolectar, procesar y diseminar de una manera ininterrumpida el flujo de la información, mientras se explota o se niega al adversario ésta habilidad (Joint Chiefs of Staff, 2014). Esto se entiende por superioridad de la Información.

La superioridad de la información es un estado de desequilibrio en el cual alguien cuenta con una ventaja sobre otro en el dominio de la información (Alberts et al., 2004). De igual manera, Alberts (2004) afirma que para alcanzar ésta superioridad es necesario tener la información correcta, para las personas correctas, en el tiempo indicado, de la manera correcta negándole a un adversario la capacidad de hacer lo mismo (Alberts et al., 2004). Esto con una mirada militar, en la cual se cuenta con un Estado antagónico que busca hacer lo mismo en las propias tropas y las de los aliados. Sin embargo, éste mismo enfoque puede ser aplicado no sólo al militar sino a cualquier otro campo, como al sistema de transporte marítimo, al Poder Naval, la industria marítima, en definitiva, a cualquier componente del Poder Marítimo del país.

De igual manera, se puede llegar a decir que la superioridad de la información es un concepto comparativo y relativo, cuyo valor está en los resultados que de ésta se obtengan (Espinel-Bermúdez, 2020). En tal sentido, este concepto puede ser análogo a los conceptos de control de mar y superioridad aérea. Vego (2016) considera el control del mar desde una perspectiva sencilla, como la habilidad para usar una parte determinada del océano o el mar, en la cual se debe incluir el espacio aéreo, para propósitos militares y no militares y negarle esa habilidad al enemigo en momentos de hostilidades (Vego, 2016). De modo que, para obtener éste concepto de superioridad de la información según Alberts (2003), es necesario que se adopte la idea de centrado en redes (network-centric), la cual surgió en la empresa privada, como una forma de obtener una conciencia compartida y auto sincronizada (Alberts et al., 2003).

En ese mismo sentido, Alberts (2003) afirma adquirir esa superioridad de la información incrementa la velocidad del comandante para anteponerse a las opciones del enemigo, crea nuevas opciones e incrementa la efectividad de las opciones seleccionadas, lo cual lleva a que las operaciones culminen de manera satisfactoria, más rápida y a un menor costo (Alberts et al., 2003). Y siguiendo la idea presentada por Alberts (2003) sobre centrado en redes, desde el punto de vista de la Fuerzas Militares, Cebrowski y Gartska (1998) exponen que las operaciones centradas en redes suministran una poderosa dinámica a las operaciones militares. En el nivel estratégico, como un elemento esencial tanto para entender de una manera apropiada el espacio competitivo como todos los elementos de espacio de la batalla y el tiempo de ésta. En el nivel operacional, permite cerrar los vínculos e interacciones que suceden entre las unidades y el ambiente operacional, y en el nivel táctico, en donde la velocidad es fundamental (Cebrowski & Garstka, 1998).

De lo anteriormente expuesto, se puede ver la importancia que tiene contar con un sistema centrado en redes, el cual le proporciona al tomador de decisión un poder combate, que se da a través de un efectivo vínculo e interconexión con toda la organización de combate. Además, cuenta con la característica de tener unas fuerzas geográficamente dispersas con un alto nivel de conciencia situacional compartida del espacio de la batalla, que puede ser explotada para alcanzar la intención del comandante. En consecuencia, tener ese sistema centrado en redes, le da la ventaja operacional sobre el enemigo, que está traducida en la superioridad de la información, todo esto se produce a través del ciberespacio. De manera que la superioridad de la información debe ser aplicada al Poder Naval que protege el Poder Marítimo de la Nación, pero también es posible aplicarla sobre todos los componentes del Poder Marítimo. Porque no es posible desarrollar y protegerlo desde una sola visión, esta debe ser integral a todos sus componentes.

Reflexiones Finales

Para Colombia es primordial entender el Poder Marítimo, desde la perspectiva de Lambert (2018) como nación marítima, que ha puesto sus ojos en el mar. De manera que el desarrollo, prosperidad y bienestar de la nación dependen en gran medida de la capacidad de usar el mar de una manera efectiva. En su comercio, el cual está vinculado con el Sistema de Transporte Marítimo, y que requiere de una infraestructura adecuada, para enfrentar un mundo globalizado y dependiente de las tecnologías de información y comunicación. Como, en la capacidad de defenderlo y protegerlo para garantizar la libertad de acción de todos los contribuyentes de ese Poder Marítimo.

El ciberespacio es un dominio, que juega un papel predominante en el desarrollo del Poder Marítimo de la nación. De manera que, en un mundo globalizado y competitivo se requiere del uso de las tecnologías de la información y la comunicación por parte de los constituyentes del Poder Marítimo para su óptimo desempeño. Asimismo, está

la necesidad de los tomadores de decisiones, de poder tomar acciones de una manera adecuada, efectiva y a un menor costo, para lo cual necesitan tener un panorama situacional amplio y compartido, mediante el uso del centrado de redes. Por otra parte, los diferentes componentes del Poder Marítimo buscan optimizar sus operaciones, ahorrar costos y mejorar la seguridad, esto lo pueden alcanzar mediante el uso de soluciones digitales que brinda el ciberespacio como son la Inteligencia Artificial, Machine Learning, entre muchas más. Por lo tanto, se puede decir que el uso del ciberespacio, así como la dependencia del Poder Marítimo de éste, hace que éste sea una variable fundamental en la era de la información.

De igual manera, el ciberespacio debe ser usado de una manera efectiva para que éste represente una ventaja sobre el enemigo, competidores de poder y amenazas al Poder Marítimo de la Nación. En ese mismo sentido, la superioridad de la información permite tener libertad de acción en el ciberespacio, para actuar en favor de los intereses del país. Para alcanzar esa superioridad, es necesario tener una infraestructura informacional, la cual debe orientarse al centrado en redes, que permita la creación de una conciencia compartida y conocimiento del ambiente operacional o del espacio de la batalla, que va a traer como consecuencia un aumento en la velocidad de las operaciones, la capacidad de reacción, disminuir los riesgos y costos, e incremento de la efectividad en el combate y de las operaciones. Sin embargo, esta superioridad debe ir acompañada con un componente más que pueda garantizar el flujo constante de la información, su integridad, y su confidencialidad, para evitar que sea explotada por diferentes amenazas, y esto se logra a través de un sistema de ciberseguridad.

El Sistema de Transporte Marítimo es uno de los componentes que aglutina gran parte del Poder Marítimo del País, y que está directamente involucrado con el ciberespacio, debido al incremento del uso de las tecnologías de la información, operación y de las comunicaciones. Está la relación de los buques con el ciberespacio, la cual se evidencia mediante la conexión de los sistemas de navegación, comunicación, ingeniería, posicionamiento y sistemas de combate de un buque a diferentes redes.

De igual manera, se encuentra la relación de otros componentes del Sistema de Transporte Marítimo con el ciberespacio mediante la conexión a Internet y otras redes de sistemas computarizados de gestión de cargas, las terminales marítimas, los puentes grúas, el seguimiento de buques y cargas, y la gestión logística, entre otros muchos más sistemas y dispositivos. Esta interconexión entre todo el Sistema Marítimo, ha traído una mayor disponibilidad de datos, un mayor procesamiento y transferencia de estos, lo que trae como resultado una operación más efectiva, ahorro en costos, un negocio más sustentable y rentable. Además, de un Poder Naval con mayores capacidades operativas y disuasivas. Todo esto trae consigo un mejor desarrollo del Poder Marítimo, que se traduce en un desarrollo económico para la nación.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con este artículo. Es resultado del proyecto de investigación "El Poder Marítimo como fundamento estratégico del desarrollo, la seguridad y la defensa de la Nación - II Fase" del grupo de investigación "Masa Crítica" adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (Minciencias) y registrado con el código COL0123247.

Sobre el autor

Jorge Ricardo Espinel Bermúdez. Capitán de Navío (Retirado) de la Armada Nacional de Colombia. Magister en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, Colombia. Especialista en Docencia Universitaria y Especialista en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra, Colombia. Ingeniero Naval Electrónico y Profesional en Ciencias Navales de la Escuela Naval de Cadetes "Almirante Padilla", Colombia.

ORCID: https://orcid.org/0000-0001-6073-0513
Contacto: jorge.espinel@esdeg.edu.co

Referencias

Ablon, L. (2017). *Cyber security considerations for the maritime enviorement.* En Issues in Maritime Cyber Security (Joseph Direnzo III, Nicole K. Drumhillerand Fred S. Roberts).

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2003). *Network Centric Warfare: Developing and Leveraging Information Superiority*. (5th ed.). Assistant Secretary of Defense (C3I/Command Control Research Program.

Alberts, D. S., Garstka, J. J., Hayes, R. E., & Signori, D. A. (2004). *Understanding information age warfare (3th ed.)*. Assistant Secretary of Defense (c3i/command control research program.

Banco Internacional de Reconstrucción y Fomento. (2021). Transporte aéreo, carga (millones de toneladas-kilómetros). Banco Mundial - Datos. https://datos.bancomundial.org/indicator/IS.AIR.GOOD.MT.K1

BIMCO, Columbia Shipmanagment Cyprus, Chamber of shipping America, Digital containership Association, & Interferry. (2020). The Guidelines on Cyber Security Onboard Ships. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Cebrowski, A. K., & Garstka, J. J. (1998). Network-centric warfare: Its origin and future. Proceedings, 124(1).

Centre d'études stratégiques de la Marine -CESM-. (2015). La Marine Nationale, Acteur De La Cyberdéfense Maritime. *BRÉVES MARINES*, No 182. https://cesm.marine.defense.gouv.fr/index.php/component/cck/?task=download&file=fichier_pdf&id=169

Cimpanu, C. (2020). *Port of San Diego suffers cyber-attack, second port in a week after Barcelona*. ZDNet. https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/

Clark, D. (2010). Characterizing cyberspace: Past, present and future. *MIT CSAIL*, Version, 1, 2016–2028. https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf

Clarke, R. A., & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It.*

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. (2019). *Informe sobre el transporte marítimo-2019. United Nations Publications*. https://unctad.org/system/files/official-document/rmt2019_es.pdf

Congressional Research Services. (2021). *Defense Primer: Cyberspace Operations.* https://sgp.fas.org/crs/natsec/IF10537.pdf

Dirección de Impuestos y Aduanas Nacionales. (2018). *Estadísticas de Carga de las Importaciones y Exportaciones en Colombia.* DIAN. https://www.dian.gov.co/dian/cifras/CargaImpExp/Estad%C3%ADsticas%20de%20Carga%20de%20las%20Importaciones%20y%20Exportaciones%20en%20Colombia%20Enero%20-Jun%202018.pdf

Eissa, S. G., Gastaldi, S., & Poczynok, I. (2012). *El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino.* 19. http://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1&isAllowed=y

Espinel-Bermúdez, J. (2020). *Prospectiva de las Operaciones Navales*. En Arte Operacional Marítimo: Una perspectiva desde la Escuela Superior de Guerra (PHd Sergio Uribe Caceres, pp. 257–295). Imprenta Nacional de Colombia.

EuropaSur. (2020, octubre 2). *La naviera CMA CGM se recupera de un ciberataque que no afecta a los puertos [Noticias]. Europa Sur - Maritimas*. https://www.europasur.es/maritimas/naviera-CMA-CGM-ciberataque-puertos_0_1506749448.html

Feliu Ortega, L. (2012). *La Ciberseguridad y la ciberdefensa*. En El ciberespacio. Nuevo escenario de confrontación (Ministerio de Defensa, Instituto Superior de Estudios Estratégicos, Vol. 126, pp. 165–203). Instituto Español de Estudios Estratégicos. https://dialnet.unirioja.es/servlet/libro?codigo=547632

Gómez A, H. (2013). Ciberoperaciones. *Revista Marina*, 935(4), 362–367. https://independent.academia.edu/HéctorGómezArriagada

Goud, N. (2019, julio 11). *Cyber Attack on Ship disrupts the functionality of onboard Control Systems. Cybersecurity Insiders.* https://www.cybersecurity-insiders.com/cyber-attack-on-ship-disrupts-the-functionality-of-onboard-control-systems/

Goward, D. A. (2017). *GPS Jamming and spoofing Maritimes Biggest cyber threat.* En Issues in Maritime Cyber Security (Joseph Direnzo III, Nicole K. Drumhillerand Fred S. Roberts).

Haynes, P. (2015). *Toward a New Maritime Strategy: American Naval Thinking in the Post-Cold War Era.* Naval Institute Press.

Joint Chiefs of Staff. (2014). *Information Operations JP 3-13.* JCS. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Joint Chiefs of Staff. (2018). *Cyberspace Operations JP3-12.* United States Chiefs of Staff. https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

Kenna, P. (2008). Globalization and housing rights. *Indiana Journal of Global Legal Studies,* 15(2), 397. Gale OneFile: Criminal Justice. https://link.gale.com/apps/doc/A186436918/GPS?u=esdegue&sid=bookmark-GPS&xid=b02dffec

Kessler, G. C., & Shepard, S. D. (2020). *Maritime Cybersecurity: A Guide for Leaders and Managers.*

Kramek, C. J. (2013). *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities.* Center for 21 century security and intelligence at brookings.

Lambert, A. (2018). *Seapower States: Maritime Culture, Continental Empires and the Conflict That Made the Modern World.* Yale University Press.

Mahan, A. T. (1890). *The Influence of Sea Power Upon History,* 1660-1783 (12a ed.). Little, Brwn and company.

Marta. (2020, febrero 21). *Ciberataque contra Maersk: Nuevos piratas amenazan al comercio marítimo.* Cytomic. https://www.cytomic.ai/es/tendencias/ciberataque-contra-maersk/

Reveron, D. S. (Ed.). (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.*

Robinson, N., Gribbon, L., Horvath, V., & Robertson, K. (2013). *Cyber-security threat characterisation A rapid comparative analysis* (p. 74) [Research]. RAND Corporation.

Secretary of Defense. (2012). *Navy Cyber Power 2020*. https://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf

SIPA. (2017, febrero). *Securing Our Hyperconnected World* [Mp4]. https://isoc-ny.org/sipa/20180208_sipa_schneier.mp4

Stavridis, J. A. (2018). *Sea Power: The History and Geopolitics of the World's Oceans (Penguin Books)*. Penguin Books.

Till, G. (2013). *Seapower: A guide for the twenty-first century (Third edition)*. Routledge.

Twist, J., Rhodes, B., & Wong, E. (2017). *Navigatting the cyber threaths to the U.S. Maritime Transportation System. En Issue in Maritime Cyber Security*. Westphalia press.

Vego, M. (2016). *Maritime Strategy and Sea Control: Theory and Practice*. Routledge.