# Boletín de Lecturas Seleccionadas

**Publicación de la Escuela de Guerra Naval de la Armada Nacional**
**República Oriental del Uruguay**

**Segunda Época - Número 3**
**Agosto 2019**

## Indice





## Editorial

Hemos dejado atrás el punto al medidodía de nuestra singladura anual y nos comenzamos a preparar para las tareas vespertinas previas al crepúsculo del año lectivo. Seguimos en el rumbo y con timón firme, brindando nuevas perspectivas de las temáticas que nos ocupan.

En esta edición de nuestro boletín traemos el relato anecdótico de como, utilizando conocimientos teóricos en el área de matemáticas y estadística, se diseñó y experimentó con éxito una solución a un problema práctico de índole táctico en el conflicto del Atlántico Sur de 1982; un interesante punto de vista sobre la gestión económica de las fuerzas armadas, cuyo autor tendremos el placer de recibir en el mes de setiembre en nuestra casa; una metodología de medición del poder naval en Latinoamérica, que entre sus fuentes de referencia tiene un trabajo de investigación profesional realizado en nuestro instituto sobre la cuantificación de los intereses marítimos; la confluencia de la guerra cibernética, electrónica y cinética en el ámbito marítimo; y la redefinición de la cultura del oficial de superficie entre las demás especialidades que conviven en las armadas.

Al igual que en la edición anterior, a efectos de estimular a nuestros lectores en la práctica de otros lenguajes, presentamos un artículo en portugués, y otro en inglés.

En la sección sobre libros recomendados les acercamos una reseña de, "Tras la estela del Graf Spee", un clásico que continúa ofreciendo nuevos gráficos y fotografías inéditas.

Les deseamos una excelente lectura.

**CN (CG) José Manuel Ruiz Tocci**
**Director de la Escuela de Guerra Naval**

# Escuela de Guerra Naval

## Instituto de Postgrados de la Armada Nacional

# GESTIÓN ECONÓMICA DE LAS FUERZAS ARMADAS: UNA ORIENTACIÓN EN LA POLÍTICA MILITAR

## Ariel S. Pfurr

Ariel Pfurr es Doctorando en Ciencias Sociales por la Facultad Latinoamericana de Ciencias Sociales; Magister en Defensa Nacional por la Escuela de Defensa Nacional (Argentina) ; Licenciado y Profesor en Relaciones Internacionales por la Universidad Católica de Salta; Asesor de la Comisión Permanente de Defensa Nacional de la Honorable Cámara de Diputados de la Nación de la República Argentina; Docente de la Maestría en Administración Pública, en Economía y Política Económica de la Universidad Maimónides y en el Instituto de Capacitación Parlamentaria (ICAP) en el Modulo de Defensa Nacional. Sus líneas de investigación son: Defensa, Economía de Defensa, Intereses Marítimos y Geopolítica.

**12 de Setiembre** **08:45 hs. Acreditaciones**
**09:00 hs. Comienzo conferencia**

**Salón de Conferencias del**
**Área Naval Miramar (Escuela Naval)**
**Rambla Tomás Berreta S/N esq. Lido**

**Militares:** Uniforme N° 6 (Servicio de Invierno o equivalente)
**Civiles:** Sport Formal

# Los apuntes de la UNS[1] que permitieron hundir un buque inglés en Malvinas

La sorprendente historia de un libro que permitió a los pilotos de la Aviación Naval asestar un duro golpe a la marina británica en la guerra de 1982.

Adrián Luciani / aluciani@lanueva.com Publicado en Diario La Nueva, de Bahía Blanca el 30/06/19



A medida que pasan los años, cada vez más hechos demuestran no sólo el valor y el profesionalismo con el que combatieron nuestros pilotos de la Aviación Naval en Malvinas, sino también doctrinas de combate propias utilizadas, en inferioridad de medios, para sorprender la abrumadora cantidad de tecnología disponible en el bando enemigo.

El caso de la Tercera Escuadrilla de Caza y Ataque, unidad nacida en la Base Espora a comienzos de los 70`s, que para 1981 había alcanzado el límite de vida útil en sus jets monoplazas reactores Skyhawk A4Q, es uno de estos ejemplos.

Ocho aviones se encontraban con posibilidad de vuelo, pero varios presentaban fisuras a consecuencia de la operación en portaaviones y requerían el recambio de las alas para seguir volando. Los cañones no funcionaban, salían dos o tres disparos y se trababan dejando al caza indefenso ante un hipotético combate aéreo contra otro caza enemigo. A esto había que agregarle que los cohetes en los asientos eyectables estaban vencidos, poniendo en peligro la vida del piloto al quedar atrapado dentro de la cabina. Sin embargo, los pilotos conocían cada avión, cada uno de ellos volaba diferente y cada uno tenía un A4Q preferido.

El 21 de mayo de 1982 no fue un día más para los aviadores navales y mucho menos para los británicos. Esa jornada la Tercera Escuadrilla de Ataque iba a entrar en la historia al hundir a la fragata clase 21 “HMS Ardent” en la bahía de San Carlos.

1 Universidad Nacional del Sur. *Nota de la Redacción.*

Eso forma parte de una historia ampliamente difundida. Sin embargo, detrás de la escena, hubo otra historia desconocida y no menos apasionante: la de los apuntes de la UNS que permitieron semejante proeza militar cargada de alto profesionalismo.

Los hechos, que se remontan al conflicto con Chile, fueron rescatados del olvido por el escritor bahiense Claudio Meunier y formarán parte de un nuevo libro.

"Gerardo Agustín Sylvester, matemático estadístico bahiense y profesor titular del Departamento de Matemática en la UNS, escribió una obra de estudio y consulta que se llamó Montecarlo, aplicación en las Empresas y las Fuerzas Armadas, que se editó en 1970. Copias de esta obra se pueden encontrar en el Conicet o hasta en Mercado libre. Durante la guerra las fotocopias de esa obra estaban en el kiosquito de apuntes del departamento de Matemáticas de la universidad a disposición de los alumnos y son

esas mismas páginas las que el MI5 del servicio británico de Inteligencia debió haber rastreado pues en el final del libro se publica un ejercicio de estadística clave.

Allí se detalla un supuesto ataque a un buque de guerra con una clase específica de avión en cuanto a sus características, con uso de determinado armamento, formas de atacarlo y se precisan también, a través de la estadística, los resultados del ataque. “Por ejemplo, mencionaba que dos grupos de tres aviones cada uno, seis en total con un total de 24 bombas (cuatro cada uno), lanzadas en reguero (una tras otra separadas por fracciones de milisegundos) y cruzando el objetivo desde diferentes ángulos, podían impactar de lleno al buque hundiéndolo u horquillándolo, es decir haciendo explotar las bombas a sus costados y ocasionándole serias averías.

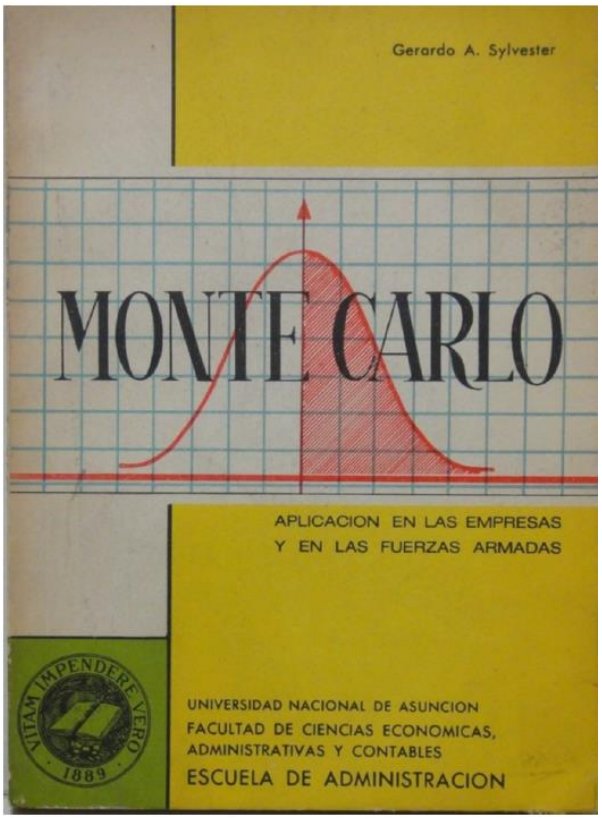
“También precisaba que en la acción se iba a perder el 50% del grupo de atacante. Esa es la estadística a la que habían llegado en el departamento de Matemática de la UNS el Profesor Sylvester con un núcleo de docentes muy capacitados que lo acompañaron en este trabajo único”, señala Meunier.

“El ataque del 21 de mayo de 1982, con la misión de los Skyhawk de la Aviación Naval Argentina, estuvo basado en las fotocopias de un libro de la UNS. Es decir que si los británicos querían saber cómo los iban a atacar sólo tenían que ir al kiosco y fotocopiarlo”, agrega.

Para llevar a la práctica la teoría del matemático local, la escuadrilla adquirió bombas americanas Mk 82 con cola retardada. El personal terrestre, clave en el mantenimiento de los Skyhawks a través de su departamento de armas, conocía el manejo de ellas por el alto grado de adiestramiento. De esta forma la escuadrilla entraba en la historia de la aviación mundial al ser la única en el mundo preparada para combatir a buques de guerra enemigos con doctrina propia y armamento especial para este cometido.

No fue ninguna sorpresa cuando el 21 de mayo seis Skyhawks partieron con sus cuatro bombas para producir daños en el desembarco ingles. Sin embargo, el primer vuelo de la mañana retornó con su armamento al desviarse de la zona de ataque por un problema en el sistema de navegación instalado días antes, el cual no permitió que los pilotos lograran, bajo la presión del combate, la preparación correcta.

En el segundo vuelo participaron seis aviones divididos en dos grupos de tres. El líder del primer grupo era el del capitán de corbeta y vecino bahiense Alberto Philippi, quien solicitó que le dieran un avión sin ese equipo de navegación ya que lo haría como siempre había volado. El segundo grupo tuvo dos aviones con navegador provisto de los valores correctos, en tanto el restante debía volar a la vista de los otros dos para no perderse en el retorno.



"La escuadrilla se preparó para atacar a los buques. No era como el Super Etendard, que lanzaba el misil fuera del horizonte del enemigo y se volvía. Los Skyhawks navales debían llegar hasta el blanco volando rasante, bajo fuego antiaéreo, esquivando misiles, sin poder disparar sus cañones, elevarse a 50 metros de altura exponiéndose aun más al fuego enemigo y lanzar las bombas pasando por encima del buque", refiere Meunier.

"Como los Skyhawks no tenían intervalómetro para lanzar las bombas unas detrás de otra, emplearon un método criollo local: utilizaron los lanzadores de sonoboyas que tenían los aviones Grumman Tracker de lucha antisubmarina. Fue realmente una obra maestra lo que hicieron para lanzar en reguero esas bombas americanas de 250 kilos con cola retardada. Estas se frenaban en el aire permitiendo que el avión pudiese escapar y no ser alcanzado por la onda expansiva".

Pero esa historia tuvo un capítulo más, no exento de dramatismo, ya que el hijo del profesor Gerardo Agustín Sylvester, el teniente de navío Roberto Gerardo Sylvester, era uno de los seis pilotos que ese 21 de mayo se preparó para atacar al desembarco británico en San Carlos.

"El padre lo llamó la noche anterior, estaba preocupado, su hijo se encontraba en esa lotería del 50 por ciento de pérdidas. Es decir, un ejercicio que él fabricó le toco vivirlo a su hijo, lo que resultó algo terrible para él", comenta Meunier.

La mañana del día del ataque –agregó-- Sylvester se subió a su automóvil Opel K 180 y se fue a la Base Espora a escuchar en los equipos de radio el ataque a los buques. Seguramente escuchó al capitán Philippi decir: 'Soy Mingo, me eyecto, me dieron, estoy bien' y también el grito de alerta del teniente de fragata Marcelo Marquez diciendo 'Harrier, Harrier'. Segundos más tarde su voz se apagaba cuando uno de los Sea Harrier piloteado por John Leeming lo alcanzaba con una salva de cañones esparciendo su Skyhawk en el firmamento luego de explotar su turbina.

"Luego escuchó al teniente de navío José César Arca, con su avión averiado, informando que se trababa en combate con un Harrier para luego eyectarse en Puerto Argentino. Así. una de las máximas del libro del profesor Sylvester, se cumplía: la mitad del grupo atacante era derribado. Márquez murió y Philippi y Arca lograron eyectarse. El primero fue tomado prisionero y el segundo fue rescatado por un helicóptero del Ejército Argentino.

El matemático vivió momentos muy difíciles, escuchar a su hijo yendo al combate volando en el segundo grupo. Los tenientes de navío Benito

Rotolo, Sylvester y Carlos Lecour, alertados por las voces de los primeros tres pilotos que estaban siendo atacados, emplearon lo practicado una y mil veces: acercarse al blanco volando bajo estricto silencio de radio.

Uno detrás de otro, en fila india, los tres Skyhawks se acercaron a una velocidad de casi mil kilometros por hora llevando un regalo impensado para los británicos, practicar con ellos la parte final del ejercicio de ataque incluido en el libro, que algunos poseían en fotocopias. Al llegar a la bahía de San Carlos, Rotolo observó a la fragata "Ardent" humeando profusamente, una bomba del capitán Philippi y una del teniente Arca habían dado de lleno en la popa ocasionándole incendios de magnitud. Rotolo la señaló y los tres pilotos fueron tras la castigada fragata que en horas de la mañana había sido blanco de los Dagger de la Fuerza Aerea Argentina basados en Río Grande. Las bombas de Rotolo explotaron a cada lado del buque, Lecour la alcanzó con una de nuevo en la popa, destrozándola por completo. Esa fue la estocada, el golpe de gracia. Sylvester, impresionado por la explosión delante suyo, apuntó a la "Ardent" y lanza su carga con resultados dantescos para el buque británico que pocas horas después se hundía producto de las averías. En la base Espora, Gerardo Agustín Sylvester, respiró profundo y hondo, volviendo a la vida cuando escuchó la voz de su hijo y sus compañeros llamándose entre ellos e iniciando el retorno a Río Grande. Los tres pilotos sobrevivientes formaron parte de la estadística Montecarlo, lograban retornar a su base y ser el otro 50% que salía con vida. "Es decir que se cumplieron los parámetros de hundimiento, uso de bombas, lanzamiento y pérdidas, fue a mi entender el ejercicio de estadística mas peligroso que creó este notable matemático de nuestro medio", concluyó Meunier.

# TEORÍA DE LA GESTIÓN ECONÓMICA DE LAS FUERZAS ARMADAS

Una contribución a las bases conceptuales para la orientación de la política militar

**Resúmen**

El presente trabajo explora los conceptos generales acerca la Teoría de Gestión Económica de las Fuerzas Armadas, la cual toma como referente a Países Medianos[1], desde el marco conceptual de la Economía de Defensa. Para ello, se ofrece una visión sobre el análisis de la política militar, el Gasto Militar (GAMIL) y, por último, cómo puede ser evaluada con el fin de generar capacidad operativa genuina. En este sentido, se abordan los ejes centrales que pueden contribuir a producir bienes públicos de calidad y sostenibles en el tiempo.

**Palabras Clave**

Gasto Militar (GAMIL)- Países Medianos- Factores de Producción-Amenazas-Misiones-FFAA-Política Militar

## Consideraciones Iniciales

La política de Defensa y la política militar de los Países Medianos no es voluntarista, ni tampoco es la consecuencia de incrementales erogaciones fiscales. Esta no se puede crear de la nada. De hecho, estas dos políticas deben "cerrar" simultáneamente en tres aspectos. **Política y diplomáticamente** viables y sostenibles, **militarmente** factible y eficiente, y **económicamente** posible y aceptable. Si dichos elementos no cierran simultáneamente, se construye un instrumento militar inútil para la Nación en detrimento de otros sectores de la economía. (Posen, 1984: 24-25, citado en: Scheetz, et al., 2015:16).

Los elementos mencionados son el producto de la identidad de cada país. De esta manera, el Estado se convierte en un campo de discusión fragmentado por un dilema estratégico fundamental dado por la ejecución de políticas públicas donde cada bien público lucha por una porción del presupuesto nacional, y por otro lado, poseer un instrumento militar que posea capacidad operativa genuina tendiente a la generación de efectos militares en pos del cumplimiento de misiones. Donde, en muchas ocasiones, las demandas de la sociedad están más allá de las posibilidades que tiene el Estado para poder cumplirlas.

1 La definición de "estados de poder mediano" se encuentra en Hill (1986:26).Se emplea la frase "países medianos" en este sentido: "Por consiguiente, dado un determinado mínimo de recursos básicos, territorio, población, educación y desarrollo industrial, que un Estado sea incluido en la categoría de mediano depende fundamentalmente de la percepción que tenga de sí mismo... Lo que caracteriza a la potencia mediana es su deseo de satisfacer por sí misma los requisitos para mantener su existencia como entidad. Tiene que ser capaz de desencadenar las acciones requeridas, aunque otros Estados u organizaciones acudan en su auxilio en algún momento. Debe asegurarse el control siempre que sea posible, mientras sus intereses permanezcan bajo amenaza".

2 "Las estrategias grande desinteresadas, en las cuales los objetivos políticos y la doctrina militar son pobremente reconciliados, pueden llevar a la guerra y a la derrota, poniendo en peligro así la supervivencia propia del Estado. En tiempos de paz, la doctrina debería permitirle al Estado asegurar su seguridad con costos económicos, políticos y humanos que estén dentro de su alcance" (Posen, 1984:24-25).

Con el fin de abordar dicha dinámica, el presente artículo se centra en abordar tres aspectos fundamentales, a saber: la asociación de una serie de conceptos de la economía neoclásica al análisis de la defensa nacional. El segundo, cómo los conceptos relacionados con la economía de defensa pueden contribuir a responder a las necesidades o demandas del instrumento militar de países medianos. El tercer aspecto, cómo puede ser evaluada la política militar con el fin de generar capacidad operativa genuina. Finalmente, se desarrollarán las conclusiones pertinentes del artículo.

## Fundamentos económicos de la Gestión pública de la Defensa

La economía de defensa otorga una serie de herramientas que permiten encuadrar y analizar la gestión pública de la política militar. Todos los países se encuentran en una puja casi constante entre la promoción de niveles óptimos de su sistema de defensa nacional, bajo un contexto de limitación cada vez más importante de recursos en un medio caracterizado por crecientes riesgos-amenazas del sistema internacional. A esta dinámica se le suma un factor más, que el Estado asume la responsabilidad de cubrir una serie de demandas públicas en el ejercicio de la gestión de gobierno. Básicamente, esta cuestión se focaliza en el rol económico que juega el Estado en la promoción de bienes públicos y paralelamente a ello, como agente ejerciendo control sobre el mercado privado (Stiglitz, 2000).

En estas condiciones se requiere de guías teóricas, que contrasten de manera permanente el "ser" (la realidad, en este caso, los datos económicos) con el "deber ser" (la teoría económica), cuyos postulados conceptuales ayuden a orientar con eficiencia la gestión gubernamental de la defensa.

Esencialmente, se trata de responder tres cuestiones puntuales: 1) Quién y para quién produce defensa externa, 2) cuánta defensa externa se debe producir, 3) cómo se puede producir defensa externa.

Considerando los tres interrogantes planteados, el primer aspecto para su abordaje es a partir de la definición de la Defensa como un Bien Público Puro cuyo consumo afecta a todos los habitantes del país por igual, teniendo como rasgos distintivos que son bienes "no rivales" y "no excluyentes" (Scheetz, et al., 2015: 36-37; Krugman, 2006:479; Hartley, 2015:37) a diferencia de los bienes privados que sí son rivales y excluyentes.

El rol de Estado es proveer bienes y servicios públicos de calidad[3] financiados por el gobierno a partir de una serie de prioridades y responsabilidades que asumió por mandato de sus votantes y/o contribuyentes. Sin embargo, la decisión que el gobierno adopte en la dirección de la Defensa Nacional provocará costos y beneficios, no solo en materia de gestión de recursos, sino también en la promoción de otros bienes y servicios públicos tales como educación, salud, seguridad interior, entre otros (Cusack, Fuchs, 2003 & Lindert, 2004). El punto crucial de esta elección es que a mayores niveles de defensa no se asegura necesariamente mayor seguridad[4]. De hecho, un excesivo, o mal orientado, GAMIL termina siendo perjudicial para el desarrollo económico de la nación.

La determinación de qué bienes públicos se producen y en qué cantidad encierra de manera implícita "un equilibrio marshalliano" [5] (Scheetz, et al., 2015), es decir, que las decisiones colectivas (Stiglitz, 2000: 23) determinarán las prioridades y las cantidades de cada bien público y estos, a su vez, "competirán" por una porción

[3] En muchas ocasiones se pueden asignar muchos recursos públicos a financiar bienes cuyo resultado no necesariamente es de calidad.

[4] El Estado no puede financiar todos los riesgos que pueden llegar a afectarlo. Desde este punto de vista el Estado"compra" una "póliza de seguro" concreta, dado que debe priorizar que riesgos puede enfrentar y cuáles no.

[5] "El equilibrio marshalliano" se define como aquella situación caracterizada por la elección que realizan los agentes económicos ante la oferta y demanda de un conjunto de bienes en un contexto de escasez de recursos. En el caso específico de la defensa nacional, como un bien público puro, el trade-off implica que el Estado se enfrenta ante una disyuntiva donde la promoción de un determinado bien afecta no solo sus cantidades, sino también las cantidades de otros bienes públicos. Por ejemplo, si medidas políticas adoptadas por un gobierno tienden a mejorar la calidad educativa, esta decisión puede impactar (reducir) las cantidades ofrecidas de defensa (partiendo del supuesto de que en la economía presupuestaria se encuentran compitiendo estos dos bienes). Esto ocurre porque los recursos fiscales son finitos. Por lo tanto, la política pública "elige racionalmente" cuáles son los bienes que mayor prioridad requieren, de acuerdo a las demandas sociales. Para mayor información al respecto se puede consultar: (Scheetz, et al., 2015: 44-48).

del presupuesto nacional. Esta situación implica que, a mayores porciones presupuestarias destinadas a un bien se "debe" renunciar a cantidades de otros bienes[6]. El ejemplo característico de dicha reasignación presupuestaria se observa en las "transferencias" o "desplazamientos"[7] de recursos públicos fiscales en el periodo posterior a la guerra fría cuando los países redujeron sustancialmente el presupuesto de defensa y "trasladaron-desplazaron" paulatinamente dichos recursos a otros bienes públicos, principalmente a gastos sociales tales como educación y salud (Cusack, 2003).

Como contrapartida de esta situación, en muchas ocasiones el Estado realiza asignaciones presupuestarias a bienes públicos cuya promoción y resultado es ineficiente. En tales ocasiones se los puede denominar como "males públicos", ya que los efectos pueden ser el aumento de la inseguridad, de la pobreza, de la contaminación, o la pérdida de calidad educativa, por ejemplo. Estos son el producto del fracaso de la gestión pública del Estado.

Es un hecho que los niveles de Producto Bruto Interno (PBI)[8] varían sustancialmente en cada país, en base a lo cual cada Estado determinará cuál es la porción presupuestaria destinada a la defensa. La clave está en que no será la misma porción presupuestaria la que asigne un país que se encuentra atravesando un conflicto bélico a otro país que se encuentra en un escenario caracterizado por el binomio paz-cooperación. También será diferente la porción asignada por un país que elige un diseño del instrumento militar basado en una actitud estratégica ofensiva o defensiva[9]. En consecuencia, las porciones de PBI muestran el nivel de amenazas que enfrenta un país, dado que, el 1% puede ser suficiente mientras que en otro el 10 % del PBI puede ser muy poco. Este dato es muy útil cuando se quiere estudiar el impacto del GAMIL en el crecimiento de los países.

Al mismo tiempo, es importante señalar que esta "porción" destinada a la defensa será definida en términos del beneficio marginal (BMa) que tiende a identificar los efectos deseados de la defensa dados los niveles de gasto, ya que se financian misiones específicas en base a un tamaño, magnitud, cantidad y diseño de fuerza determinado políticamente. Es decir, que los contribuyentes pagan la valoración marginal de cada misión adicional y cuando esta valoración (BMa) se iguala al costo marginal (CMa) de su provisión es el punto óptimo donde se encuentra su equilibrio presupuestario (GAMIL). Si bien este punto de equilibrio no es empíricamente identificable, su importancia reside en su impacto didáctico y en el planeamiento que se describe abajo.

***De acuerdo con esta visión, para el caso puntual de la defensa se puede citar el ejemplo de las acciones realizadas para el control de los espacios marítimos adyacentes, como un activo estratégico vital para el Estado.*** Para ello, el diseño de la flota naval debe poseer los medios adecuados, tendientes para a la protección de los recursos en lo que respecta la Zona Económica Exclusiva (CONVEMAR), en este sentido tener la capacidad para realizar operaciones militares autónomas, con personal alistado y adiestrado con el fin de cumplir con dicha misión. Pero además, la flota debe tener la capacidad de cooperar con países de la región en base a la gestión de riesgos/amenazas comunes, ya sea en la participación de organizaciones multilaterales o bilaterales, poder realizar las operaciones de búsqueda y rescate (SAR) y tener la capacidad de proyectar "fuerza" a distintos puntos dentro de su territorio[10] y de ser necesario utilizar dicha

[6] El principio subyacente de esta afirmación es que cada nación tiene una dotación limitada de recursos para poder producir, es decir, mano de obra, capital fijo y variable, conocimiento (tecnología) y recursos naturales, a partir de la cual, debe elegir qué bienes y en qué cantidad producir eficientemente.

[7] Concepto conocido en inglés como *crowd-out,* hace referencia al efecto de desplazamiento, donde todo gasto público tiene su correlato en el costo de oportunidad para el consumo e inversión de otros bienes públicos y privados.

[8] Está demás aclarar que estos niveles varían según el tamaño de la economía, la inversión directa, etc.

[9] Dado que se trata de medios militares, todos tienen un potencial ofensivo y de letalidad máxima por su característica de material de combate. La diferencia radica en el diseño y despliegue de una estructura de fuerza con capacidad de proyección y de capacidad para retener territorio enemigo.

[10] Por ejemplo: el caso de la República Argentina donde su plataforma continental en distintos puntos llega a alcanzar las 350 millas, el Estado debería tener la capacidad para proyectar sus fuerzas hasta allí con el fin de proteger las especies bentónicas y los recursos naturales (ej: Petróleo). En este punto, se debe mencionar una segunda acepción, dado que al participar en misiones multilaterales de paz los Estados deben tener la capacidad de proyectar su fuerza en dicho marco.

fuerza. Esta combinación de recursos representa el BMa que permite el cumplimiento de misiones específicas, que en este caso particular componen el control del espacio marítimo que posee un Estado.

El BMa de estas acciones "incluye" a la sociedad, por lo tanto, no se pueden excluir a estos consumidores de este bien público (principio de no-exclusión). Aun si se sumaran consumidores, el CMa será el mismo, dado que el diseño de fuerza previsto cubre los riesgos identificados. Asimismo, no existe una empresa privada que goce del monopolio legítimo de la fuerza y que pueda proveer estos niveles de seguridad externa. Por esta razón el Estado es el principal oferente (monopolista) de este bien público y a su vez, la nación en su conjunto es el principal consumidor (monopsonista).

Finalmente, la teoría de los bienes públicos permite responder conceptualmente cuál es la cantidad de misiones que un país puede asumir en base a un determinado nivel de GAMIL y cuánto debería ser el gasto militar para obtener un nivel óptimo de Defensa Nacional, es decir, el punto que está determinado por medio de la igualdad entre CMa y BMa.

## Acerca del Gasto Militar

La asignación del GAMIL está determinada por dos "momentos" o escenarios posibles: el primero es la gestión de recursos en tiempos o escenarios de paz y el segundo en tiempos o escenarios de crisis y de guerra. Cuando un país transita **tiempos de crisis y guerra,** donde en el segundo caso de su esfuerzo depende su **supervivencia.** La idea general es minimizar los riesgos operacionales y maximizar la eficiencia en la utilización del instrumento militar y de los recursos para lograr el mayor provecho posible de las acciones militares. En esta situación extrema tiende a existir una transferencia de gastos de otros bienes públicos hacia la defensa. Aunque esta reorganización de recursos públicos no garantiza la victoria en el campo de batalla, dado que para ello las fuerzas deberían haberse preparado en tiempo de paz, esta lógica responde a una elección de misiones llevada al extremo de recursos, reduciendo las proporciones de gasto de otros bienes públicos.

En contraste, en los **tiempos de paz** se suele ver una asignación de recursos relativamente **constantes** en base a un criterio de asignación racional y neoclásica que se caracteriza por misiones relativamente sin cambio. Aun así, en este contexto se puede reorganizar la productividad del sector, re-evaluar las cantidades de gastos (para el mediano y largo plazo) destinadas a capital, mano de obra y tecnología, llevar a cabo políticas militares que sean conducentes al cumplimiento de estas misiones, y de los acuerdos cooperativos regionales, entre otros aspectos relevantes.

El **segundo punto** es un desprendimiento conceptual del anterior y se refiere a la manera de presupuestar en tiempos de paz. Las asignaciones presupuestarias se deben realizar por medio de **misiones**, es decir, aquella combinación de tecnología, capital y mano de obra necesaria para generar un determinado efecto militar. Pero en un sentido contrario, si se asignara una suma presupuestaria determinada y a partir de esa suma dada, se orientará todo el accionar del instrumento militar, este último enfoque no sería racional, ni se asociaría con los costos reales de los distintos factores de producción para cumplir misiones. De este enfoque poco sensato se establecería una política militar coyuntural y cortoplacista que aseguraría, en forma muy limitada, el cumplimiento de operaciones en curso. La única excepción a la regla es (asumiendo que el punto de partida fuera eficiente) que esta "porción" presupuestaria se vaya actualizando año tras año (en términos de inflación, precios relativos, *performance* relativa, etc.). ¡De no contar con dichos recursos se corre el riesgo de pérdida o disminución de capacidades militares!

La **tercera cuestión** a abordar es ¿qué porcentaje se debería asignar a cada factor de producción para generar capacidad operativa genuina? Reconociendo los desafíos planteados, una respuesta es que una proporción de gasto militar entre 40% a 60% debería ser asignados a costos laborales y entre un 15% a 25% a las adquisiciones bélicas y no bélicas del GAMIL en todos los años, destinando una porción restante para "operaciones y mantenimiento", es decir, capital variable y otras cuestiones menores (Scheetz, et al., 2015:57). La base de este análisis la representa el estudio de series de gastos de

países miembros de la OTAN[11] , los cuales representan una constante en su asignación presupuestaria en términos de capital y trabajo. Con respecto a la composición de los gastos en capital se pueden observar que se encuentran entre un 15 y 25%en adquisiciones todos los años, tal como se puede observar en el cuadro 1.

**Cuadro 1: OTAN**

**Porcentaje de gastos en defensa por categoría (Factor)**

| % Adquisiciones (Equipos) | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Albania | | | | | | | | 11,3 | 15,7 | 13,4 | 14,4 | 16,3 | 16,7 | 8,9 | 8,0 |
| Bélgica | 7,1 | 5,3 | 5,5 | 6,4 | 5,9 | 4,8 | 8,1 | 8,2 | 6,8 | 6,3 | 3,6 | 2,8 | 3,5 | 3,4 | 4,7 |
| Bulgaria | | | 17,6 | 16,6 | 15,7 | 24,0 | 21,4 | 14,2 | 15,4 | 6,3 | 3,7 | 4,5 | 1,0 | 3,5 | 12,6 |
| **Canadá** | 13,9 | 13,6 | 13,7 | 11,8 | 11,8 | 14,8 | 13,0 | 12,8 | 13,8 | 9,7 | 8,3 | 11,2 | 13,0 | 13,1 | 18,1 |
| Croacia | | | | | | | | 10,2 | 8,1 | 15,8 | 14,7 | 10,7 | 7,4 | 10,6 | 7,4 |
| Rep. Checa | 17,5 | 19,5 | 15,4 | 9,3 | 14,6 | 10,1 | 12,9 | 22,4 | 12,4 | 13,3 | 14,8 | 9,5 | 6,5 | 11,8 | 7,2 |
| Dinamarca | 13,5 | 16,1 | 19,2 | 11,2 | 15,4 | 15,7 | 18,8 | 9,9 | 14,1 | 9,7 | 9,0 | 11,3 | 11,0 | 11,5 | 12,4 |
| Estonia | | | 12,6 | 11,9 | 14,5 | 23,7 | 10,1 | 17,9 | 11,9 | 10,1 | 13,7 | 14,5 | 22,2 | 13,9 | 13,5 |
| **Francia** | 19,1 | 20,5 | 20,9 | 21,3 | 23,2 | 21,4 | 21,0 | 27,0 | 30,2 | 28,2 | 30,6 | 28,6 | 24,7 | 25,0 | 24,5 |
| **Alemania** | 14,1 | 13,8 | 14,8 | 14,2 | 15,0 | 14,6 | 17,1 | 17,6 | 17,6 | 16,4 | 16,5 | 12,7 | 12,9 | 11,9 | 12,2 |
| Grecia | 13,1 | 10,7 | 7,3 | 15,3 | 14,9 | 10,5 | 16,4 | 27,8 | 18,0 | 5,9 | 7,5 | 12,1 | 8,2 | 12,8 | 14,9 |
| Hungría | 11,1 | 10,3 | 11,9 | 8,4 | 9,0 | 12,1 | 14,8 | 12,7 | 12,1 | 12,3 | 5,8 | 11,1 | 7,8 | 8,2 | 13,0 |
| Italia | 12,4 | 12,9 | 11,7 | 9,1 | 7,2 | 14,0 | 12,7 | 11,3 | 10,9 | 11,7 | 8,9 | 12,5 | 10,9 | 9,7 | 20,2 |
| Letonia | | | 7,4 | 8,7 | 12,3 | 9,6 | 14,9 | 5,4 | 15,6 | 10,8 | 10,5 | 12,1 | 7,6 | 13,6 | 17,9 |
| Lituania | | | 12,3 | 15,3 | 17,0 | 18,7 | 16,3 | 16,2 | 10,0 | 9,4 | 11,2 | 9,2 | 14,1 | 21,6 | 27,7 |
| Luxemburgo | 6,8 | 7,4 | 8,2 | 11,4 | 8,7 | 6,8 | 25,1 | 17,4 | 34,4 | 21,9 | 17,1 | 14,6 | 22,6 | 33,3 | 27,2 |
| **Países Bajos** | 15,9 | 14,9 | 16,7 | 16,0 | 16,8 | 19,1 | 17,2 | 17,6 | 15,7 | 14,4 | 13,4 | 12,6 | 10,7 | 11,2 | 14,1 |
| **Noruega** | 23,7 | 21,8 | 22,9 | 21,1 | 19,4 | 21,4 | 22,6 | 19,2 | 18,1 | 17,0 | 17,8 | 18,9 | 21,2 | 22,5 | 25,1 |
| Polonia | 11,1 | 12,4 | 14,6 | 14,6 | 18,2 | 18,6 | 13,9 | 15,9 | 18,1 | 16,1 | 15,2 | 13,9 | 18,8 | 33,1 | 25,8 |
| Portugal | 4,1 | 7,4 | 7,6 | 8,9 | 8,9 | 8,4 | 13,5 | 8,7 | 13,2 | 12,1 | 9,3 | 8,7 | 8,4 | 8,7 | 9,4 |
| Rumania | | | 25,6 | 20,0 | 24,0 | 13,3 | 16,7 | 8,7 | 8,8 | 7,6 | 4,1 | 10,7 | 15,8 | 19,7 | 20,4 |
| Eslovaquia | | | 10,4 | 14,8 | 12,7 | 16,2 | 14,6 | 13,2 | 9,8 | 7,1 | 9,6 | 7,4 | 11,1 | 18,3 | 15,3 |
| Eslovenia | | | 18,5 | 9,5 | 12,2 | 10,8 | 7,4 | 8,5 | 18,0 | 5,7 | 1,2 | 1,3 | 0,7 | 1,9 | 1,0 |
| **España** | 23,3 | 22,2 | 22,8 | 22,1 | 21,7 | 20,8 | 21,4 | 17,4 | 12,1 | 6,7 | 22,9 | 12,4 | 13,5 | 14,8 | 15,2 |
| **Turquía** | 31,5 | 38,3 | 32,9 | 29,8 | 34,4 | 24,5 | 29,3 | 25,6 | 28,0 | 24,6 | 21,2 | 26,9 | 25,1 | 25,1 | 22,4 |
| **Reino Unido** | 23,7 | 22,6 | 22,8 | 23,1 | 21,2 | 22,6 | 22,5 | 21,9 | 24,5 | 22,0 | 19,5 | 21,9 | 22,8 | 21,8 | 22,6 |
| **Estados Unidos** | 27,4 | 24,5 | 24,6 | 24,5 | 25,1 | 24,6 | 26,1 | 24,1 | 24,1 | 27,0 | 27,0 | 25,8 | 26,0 | 25,4 | 25,0 |
| **Promedio** | **16,1** | **16,3** | **15,9** | **15,0** | **16,0** | **16,0** | **17,1** | **15,7** | **16,2** | **13,4** | **13,0** | **13,1** | **14,0** | **16,0** | **16,8** |
| ***Promedio de los principales 9 países de la OTAN*** | ***21,4*** | ***21,4*** | ***21,3*** | ***20,4*** | ***21,0*** | ***20,4*** | ***21,1*** | ***20,4*** | ***20,5*** | ***18,4*** | ***19,7*** | ***19,0*** | ***18,9*** | ***19,0*** | ***19,9*** |

**Fuente**:www.nato.int

**Notas**: Porcentajes dedicados a gastos de infraestructura no están incluidos en nuestro cuadro

Promedio simple de 9 incluye a Canadá, Francia, Alemania, Países Bajos, Noruega, España, Turquía, el Reino Unido y los Estados Unidos

Los gastos de personal incluyen los gastos militares y civiles y las pensiones.

El gasto en equipo incluye el gasto en equipo principal y la I + D dedicada a los equipos principales.

De igual manera, al focalizar el estudio en las asignaciones presupuestarias de mano de obra en términos generales, los valores en términos de porcentaje de gasto varían entre un 40 a 60%. En un sentido especifico, analizando los principales 9 países su evolución esta en dicho rango (ver cuadro 2).

[11] Lo singularmente relevante para este análisis es que no solo la OTAN presenta una relación de 40% - 60%, sino países como Chile, Sudáfrica, Australia y Nueva Zelanda, entre otros, poseen dicha asignación de gasto, lo cual de ninguna manera indica que no hacemos referencia a situaciones estratégicas o de formas de planeamiento, sino **solo proporción de gasto asignado**.

**Cuadro 2: OTAN**

**Porcentaje de gastos en defensa por categoría (Factor )**

| % Personal | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Albania | | | | | | | | 66,2 | 75,7 | 77,1 | 70,0 | 75,2 | 68,1 | 78,2 | 67,3 |
| Bélgica | 71,5 | 72,8 | 73,6 | 75,1 | 75,3 | 78,9 | 72,2 | 74,5 | 75,5 | 75,9 | 78,5 | 77,1 | 77,8 | 78,2 | 77,1 |
| Bulgaria | | | 53,4 | 50,2 | 49,3 | 44,8 | 44,9 | 59,2 | 64,3 | 67,4 | 64,7 | 65,4 | 72,8 | 73,7 | 64,3 |
| **Canadá** | 45,1 | 44,9 | 45,9 | 46,2 | 46,6 | 46,0 | 44,9 | 45,3 | 45,3 | 47,1 | 49,1 | 52,4 | 50,9 | 47,2 | 45,8 |
| Croacia | | | | | | | | 72,4 | 71,6 | 67,2 | 68,1 | 68,1 | 69,3 | 63,6 | 68,5 |
| Rep. Checa | 45,5 | 41,9 | 51,1 | 47,2 | 47,4 | 49,2 | 51,5 | 46,1 | 50,7 | 56,3 | 61,7 | 62,1 | 61,4 | 55,3 | 58,5 |
| Dinamarca | 52,0 | 51,5 | 53,4 | 54,9 | 48,5 | 50,6 | 51,5 | 56,3 | 50,8 | 52,2 | 49,0 | 51,7 | 51,3 | 52,0 | 50,3 |
| Estonia | | | 32,8 | 29,2 | 26,0 | 27,0 | 31,5 | 34,5 | 34,5 | 32,3 | 29,7 | 39,8 | 38,6 | 39,1 | 38,2 |
| **Francia** | 60,7 | 58,9 | 57,4 | 58,0 | 56,5 | 57,1 | 57,4 | 49,3 | 47,6 | 49,4 | 49,1 | 49,2 | 48,5 | 47,8 | 47,9 |
| **Alemania** | 59,4 | 60,1 | 59,3 | 58,3 | 57,1 | 54,9 | 53,9 | 53,2 | 52,7 | 52,3 | 50,6 | 49,9 | 50,7 | 49,9 | 48,4 |
| Grecia | 67,6 | 74,5 | 77,3 | 74,1 | 73,8 | 79,5 | 74,1 | 56,5 | 65,1 | 76,0 | 73,2 | 74,6 | 77,2 | 70,0 | 69,9 |
| Hungría | 49,3 | 48,8 | 49,4 | 48,1 | 51,2 | 46,4 | 48,1 | 50,4 | 56,4 | 50,6 | 47,7 | 49,3 | 49,8 | 48,3 | 50,2 |
| Italia | 74,0 | 72,7 | 75,3 | 77,1 | 81,9 | 72,8 | 70,8 | 73,9 | 75,1 | 74,8 | 77,1 | 75,0 | 76,4 | 77,6 | 69,2 |
| Letonia | | | 43,8 | 49,8 | 39,2 | 38,9 | 46,3 | 59,3 | 55,9 | 51,3 | 56,2 | 53,0 | 53,0 | 50,1 | 44,9 |
| Lituania | | | 51,1 | 58,2 | 54,8 | 54,7 | 56,3 | 60,9 | 65,6 | 66,9 | 66,8 | 66,5 | 57,5 | 48,5 | 46,1 |
| Luxemburgo | 79,5 | 78,8 | 77,7 | 75,3 | 76,5 | 77,3 | 54,0 | 57,0 | 45,6 | 52,3 | 54,2 | 51,1 | 49,3 | 42,8 | 43,7 |
| **Países Bajos** | 51,2 | 52,6 | 50,5 | 50,5 | 47,8 | 47,2 | 48,6 | 50,1 | 52,3 | 54,7 | 57,5 | 58,5 | 56,5 | 55,5 | 51,8 |
| **Noruega** | 37,9 | 40,3 | 41,3 | 42,8 | 45,4 | 43,2 | 41,9 | 42,4 | 42,7 | 43,4 | 42,4 | 41,0 | 39,4 | 38,7 | 36,3 |
| Polonia | 64,9 | 64,6 | 60,6 | 57,3 | 53,8 | 54,4 | 63,2 | 61,1 | 56,8 | 57,8 | 57,3 | 57,7 | 51,5 | 42,0 | 46,8 |
| Portugal | 84,1 | 78,6 | 74,2 | 75,7 | 76,2 | 78,7 | 71,7 | 75,3 | 70,2 | 78,3 | 78,4 | 79,8 | 81,3 | 82,1 | 78,0 |
| Rumania | | | 50,6 | 57,0 | 59,8 | 72,3 | 69,1 | 79,8 | 79,1 | 79,1 | 84,0 | 79,0 | 71,2 | 63,3 | 64,3 |
| Eslovaquia | | | 50,6 | 46,7 | 49,1 | 51,5 | 51,7 | 55,8 | 62,4 | 69,5 | 66,5 | 70,1 | 69,1 | 56,2 | 58,7 |
| Eslovenia | | | 61,6 | 64,0 | 60,1 | 59,8 | 62,2 | 67,1 | 61,7 | 74,6 | 78,9 | 80,5 | 82,3 | 82,2 | 75,9 |
| **España** | 54,9 | 55,7 | 53,9 | 54,6 | 53,5 | 53,0 | 53,8 | 58,7 | 63,4 | 64,8 | 57,2 | 68,2 | 67,3 | 65,2 | 64,0 |
| **Turquía** | 45,8 | 45,6 | 49,7 | 52,2 | 48,4 | 53,3 | 46,8 | 49,6 | 49,7 | 53,0 | 56,0 | 54,9 | 56,9 | 56,8 | 58,7 |
| **Reino Unido** | 39,8 | 39,6 | 39,8 | 41,6 | 40,4 | 38,8 | 36,5 | 37,5 | 35,7 | 37,5 | 38,9 | 37,8 | 36,6 | 36,8 | 34,8 |
| **Estados Unidos** | 36,1 | 36,1 | 34,4 | 34,8 | 33,6 | 35,2 | 33,3 | 46,9 | 46,4 | 33,0 | 32,1 | 34,4 | 35,5 | 36,6 | 36,7 |
| **Promedio** | **56,6** | **56,6** | **52,6** | **53,0** | **52,0** | **54,6** | **53,4** | **57,0** | **57,5** | **59,1** | **59,1** | **62,4** | **61,5** | **59,1** | **57,5** |
| ***Promedio de los principales 9 países de la OTAN*** | ***47,9*** | ***48,2*** | ***48,0*** | ***48,8*** | ***47,7*** | ***47,6*** | ***46,3*** | ***48,1*** | ***48,4*** | ***48,4*** | ***48,1*** | ***55,8*** | ***55,3*** | ***54,3*** | ***53,0*** |

**Fuente**:www.nato.int

**Notas**:

Porcentajes dedicados a gastos de infraestructura no están incluidos en nuestro cuadro

Promedio simple de 9 incluye a Canadá, Francia, Alemania, Países Bajos, Noruega, España, Turquía, el Reino Unido y los Estados Unidos

Los gastos de personal incluyen los gastos militares y civiles y las pensiones.

El gasto en equipo incluye el gasto en equipo principal y la I + D dedicada a los equipos principales.

Esas proporciones se basan en tres factores puntuales: 1) Solamente remiten a la gama de asignaciones que se realizan en dos de los factores de producción (mano de obra y adquisiciones); 2) Parten de series presupuestarias de países que poseen capacidad operativa genuina; 3) Pero reconocen situaciones estratégicas distintas para cada país.

La proporción de GAMIL "40-60" subyace el principio del aumento geométricamente creciente de costos por unidad de los sistemas de armas mayores ("maltusianismo militar"). Esta evolución de costos de $K_B$ se observa junto con el consiguiente aumento en capital intensividad: Q/L = *f*(A/L, K/L). Esta situación empírica, evidente desde mediados del siglo XIX, afecta a todas las fuerzas armadas del mundo, por eso se presenta un rango aceptable de porcentajes en adquisiciones y costo laboral.

El rango 40 -60% y 15%-25% concibe situaciones estratégicas distintas para cada nación. Habría que señalar que la capital-

intensividad de una fuerza aérea suele ser mayor que la de una armada, y a su vez la de una armada suele ser mayor que el del ejército. Por supuesto este orden de fuerzas está afectado por la situación estratégica regional y por la configuración geográfica de cada país y de sus potenciales enemigos en términos relativos. Al mismo tiempo, se parte del supuesto de que un país mediano requiere (y quiere) capacidad militar genuina para desarrollar operaciones **autónomas** (porque de ellas depende su supervivencia como Estado) y **cooperativas** (en conjunto con otros actores regionales), siempre haciendo referencia a operaciones **convencionales** (no se tienen en cuenta ni la guerra de guerrillas, asimétricas, hibridas, ni el empleo de armas de destrucción masiva).

En tal situación, no se puede soslayar el hecho de que el costo por unidad creciente de $K_B$ (capital bélico), aun cuando el país no requiera armas mayores de última generación siga afectando geométricamente, pero con un rezago[12]. Así no deja de impactar en el planeamiento de las misiones militares asignadas (ver Pugh, 1993). Ahora bien, no responder a esta realidad condena al país a un atraso cada vez mayor, hasta llegar a una situación que caracteriza muchos países centroamericanos y caribeños. Sus fuerzas armadas, ya mano de obra intensivas, no tienen capacidad militar genuina; aun cuando ellos se llaman "las fuerzas armadas", en realidad son fuerzas constabularias, dedicadas al control interno policial de su propia población.

## Producción del sector de la defensa

El nivel de la defensa estará definido por un nivel deseable de la seguridad externa de la nación. El gobierno asume un nivel de riesgo potencial por retener misiones o no poder cumplir con todas las misiones identificadas. A su vez, también asume un nivel de "costo social" por elegir una combinación específicacon otros bienes públicos. Es importante recordar que en la teoría económica la elección de bienes públicos existe una lógica conceptual de óptimo de Pareto[13], es decir, al no variar el nivel del PBI[14] no se puede mejorar la situación de un bien público determinado sin perjudicar a otros bienes públicos.

Por su parte el CMa estará determinado por el gasto requerido para producir una misión adicional de defensa nacional. Al nivel microeconómico Scheetz, *et al.,* (2015) teorizan que el producto de la defensa puede ser explicado **didácticamente**[15] para orientar la política militar utilizando la función de producción *Cobb-Douglas*[16], donde: $Q_{DEF} = A K^{\alpha} L^{(1-\alpha)}$

**$Q_{DEF}$** es el servicio público de defensa producida por el gasto militar, GAMIL siendo p* $Q_{DEF,}$ (precio por cantidad de misiones). También se podría decir $Q_{misiones}$ o alternativamente $Q_{riesgos} = AK^{\alpha}L^{(1-\alpha)}$

**A** es tecnología, es decir, conocimiento sobre las herramientas de producción militar, *know-how* (para el economista "tecnología" no es sólo algo físico, también está presente en el capital humano)

**K** es capital físico (a su vez subdividido entre capital fijo y capital variable). Capital fijo incluye planta y equipo militar

[12] El *stock* de capital se deprecia como cualquier cosa física (Scheetz, *et al.*, 2015:121). Para disminuir el impacto negativo de la depreciación del capital se implementa una asignación constante de la pauta GAMIL de15%-25% anual invertido en $K_B$+$K_{NB}$.

[13] Se hace referencia a un punto de equilibro en el cual ninguno de los agentes económicos puede mejorar su situación sin empeorar o reducir el "bienestar" de otro.

[14] La *Ley de Wagner* supone que el crecimiento económico (PBI real o PBI real *per cápita*) suele traer consigo un incremento en el gasto público, donde la sociedad presiona al Estado para mejorar la calidad de los bienes y servicios públicos. En el caso de la defensa se pueden contemplar nuevas misiones que antes no se podían asumir.

[15] "Didácticamente" porque una expresión precisa sería un poco más complicada. En cualquier caso, una ecuación Cobb-Douglas es muy útil para entender la interacción de las variables A, K y L.

[16] A, K y L se relacionan necesariamente de forma multiplicativa, es decir, no se suma una variable a la otra. Más bien una existe solo cuando existe las otras (por ej., un soldado sin sus herramientas no es un soldado). Debe agregarse que la función de producción no es estrictamente Cobb-Douglas, pero esta ecuación simple es muy útil para describir y analizar GAMIL.

("artillado"—v.g., un tanque--- y "no artillado"—v.g., un camión). Capital variable incluye gastos en operaciones, mantenimiento y otros aspectos de mantener una fuerza en existencia—v.g., un estado mayor conjunto.

**L** es mano de obra: uniformados (activos, pasivos y pensionistas) y civiles.

**α** es el exponente que expresa la proporción del gasto en capital físico en la totalidad del GAMIL.

**(1 – α)** es el exponente que expresa la proporción del GAMIL dedicado a costos de mano de obra en defensa.

La teoría de la función de puede ilustrarse en el cuadro 3, el cual muestra el GAMIL diferenciando los Factores de Producción para el caso de estudio de la República Argentina (1994-2016). Este tipo de análisis permiten observar como tiende a evolucionar la política militar de un país en un periodo de tiempo específico. Para ello, se utilizan gastos devengados[17] y son expresados en pesos corrientes, salvo excepciones definidas en el cuadro

[17] Devengado es decir, "mandados a pagar". Concepto casi equivalente de "Ejecutado" a la fecha de cierre del periodo económico determinado.

**. Cuadro 3: Argentina**

**Gasto Militar por Factores de Producción**

Gastos devengados: pesos corrientes (salvo marcado "porción" o $US)

| Año | GAMIL: $ millones | Personal: porción | Adquisiciones: Incisos 4.3 y 4.4: porción | *Adquisic. De Armas Inciso 4.4: porción* | Otros Gastos en Capital Variable: Incisos 2 y 3: porción | Tipo de cambio promedio anual $/US$ | GAMIL: $US millones corrientes | Armas Inciso 4.4 US$ millones corrientes |
|---|---|---|---|---|---|---|---|---|
| **2016** | 66586 | 0,822 | 0,030 | *0,015* | 0,140 | 14,78 | 4506 | 67 |
| **2015** | 50621 | 0,796 | 0,040 | *0,021* | 0,157 | 9,27 | 5462 | 156 |
| **2014** | 40209 | 0,750 | 0,056 | *0,036* | 0,186 | 8,12 | 4949 | 178 |
| **2013** | 28050 | 0,763 | 0,042 | 0,017 | 0,187 | 5,48 | 5123 | 89 |
| **2012** | 20703 | 0,783 | 0,022 | 0,009 | 0,185 | 4,55 | 4549 | 42 |
| **2011** | 16634 | 0,794 | 0,022 | 0,012 | 0,172 | 4,13 | 4028 | 47 |
| **2010** | 13541 | 0,786 | 0,034 | 0,023 | 0,136 | 3,91 | 3461 | 79 |
| **2009** | 11063 | 0,782 | 0,027 | 0,016 | 0,182 | 3,73 | 2967 | 48 |
| **2008** | 8769 | 0,739 | 0,038 | 0,017 | 0,207 | 3,16 | 2775 | 48 |
| **2007** | 7109 | 0,743 | 0,045 | 0,013 | 0,201 | 3,12 | 2282 | 29 |
| **2006** | 5643 | 0,759 | 0,027 | 0,008 | 0,205 | 3,07 | 1836 | 14 |
| **2005** | 4935 | 0,764 | 0,031 | 0,005 | 0,199 | 2,92 | 1688 | 8 |
| **2004** | 4285 | 0,789 | 0,016 | 0,004 | 0,191 | 2,94 | 1457 | 5 |
| **2003** | 3988 | 0,827 | 0,014 | 0,005 | 0,154 | 2,95 | 1352 | 6 |
| **2002** | 3413 | 0,824 | 0,025 | 0,009 | 0,148 | 3,18 | 1073 | 10 |
| **2001** | 3182 | 0,828 | 0,013 | 0,010 | 0,156 | 1 | 3182 | 31 |
| **2000** | 3265 | 0,839 | 0,023 | 0,018 | 0,136 | 1 | 3265 | 57 |
| **1999** | 3460 | 0,807 | 0,059 | 0,055 | 0,131 | 1 | 3460 | 190 |
| **1998** | 3397 | 0,814 | 0,032 | 0,024 | 0,149 | 1 | 3397 | 81 |
| **1997** | 3339 | 0,818 | 0,024 | 0,015 | 0,141 | 1 | 3339 | 49 |
| **1996** | 3381 | 0,837 | 0,014 | 0,006 | 0,143 | 1 | 3381 | 20 |
| **1995** | 3387 | 0,829 | 0,023 | 0,012 | 0,150 | 1 | 3387 | 39 |
| **1994** | 3375 | 0,809 | 0,015 | 0,004 | 0,172 | 1 | 3375 | 14 |
| **Suma US$ millones corrientes 1994-2016:** | | | | | | | | **1241** |

**Fuente**: Fuente de la base de datos contables: Contaduría General de la Nación (datos desagregados y de dominio público).
**Notas**:
Personal incluye todo el gasto del IAF, así ignorando los gastos administrativos. Ergo, introduce un pequeño error.
Los GAMIL han sido consolidados, eliminando la transferencia del "Recursos Propios" de la suma del Inciso 1 y del GAMIL total.
"O&M" (Incisos 2 & 3) es un acercamiento a O&M (Programa 16). Incisos 2 y 3 incluyen muchas otras cosas también.
GAMIL aquí excluye pagos a Veteranos de la Guerra de Malvinas: $2.5 mil millones en 2014, $3,46 mil millones en 2015.

En primer lugar, a partir de 1994 se encuentra una tendencia que el GAMIL ha crecido nominalmente año tras año. Estos aumentos no tuvieron su correlato en el aumento proporcional del PBI, tan solo una pequeña actualización de los costos laborales. Todos muy por debajo de los niveles de inflación.

En segundo lugar, observando los paramentos de asignación de gasto militar, toma como referencia que el GAMIL asignado a los gastos en personal giran en torno del 80% del gasto total. Dicha tendencia se ha mantenido en los últimos 23 años. Por el contrario, la asignación en términos de armas mayores representa un 2,9 % del GAMIL tomando como referencia el mismo corte temporal. Este último punto, es crucial para el mantenimiento de capacidades militares o para desarrollo de nuevas, más aun dado el aumento "maltusiano" del costo por unidad de las armas.

Finalmente, una cuestión no menor, es que dado a la ausencia de incorporación de nuevos medios de combate, continua aumentando la edad "promedio" de los sistemas de armas mayores. El factor de envejecimiento de dichos sistemas posee una tasa de depreciación de entre el 9 al 11 por ciento anual afectando severamente su performance relativa e incrementando sustancialmente sus costos en términos de operaciones y mantenimiento. Por esta razón, se deben asignar entre el 15-25% todos los años en la incorporación de nuevos equipos.

## Consideraciones Finales

El principal desafío que se presentan para los países medianos es generar bienes públicos de calidad y sostenidos en el tiempo, manteniendo el nivel de bienestar de la sociedad. La defensa no escapa a esta lógica, con una particularidad, que de su financiamiento o no depende de la capacidad que posea el instrumento militar para contrarrestar agresiones que afecten los intereses vitales o estratégicos de la nación.

Así la Política Militar y la Política de Defensa deben "cerrar" simultáneamente en tres aspectos. Ser políticamente y diplomáticamente viables y sostenibles, militarmente factibles y eficientes, y económicamente posible y aceptable.

Los países medianos solo buscan proteger sus intereses vitales (tener la capacidad de desarrollar operaciones militares autónomas y convencionales), cooperar (en términos de riesgos y amenazas comunes), proyectar sus fuerzas a distintos puntos del territorio, en base a una actitud estratégica especifica. De aquí surgen las principales "demandas" de la defensa. Que en el presente artículo son asociadas al criterio de Beneficio Marginal (BMa).

De esta manera, cada misión (efectos) que el instrumento militar deba cumplir, tendrá un Costo Marginal específico (CMa). El modelo económico que permite explicar esta relación es que Q DEF = A K α L (1-α) y cada país tendrá una relación especifica entre BMa y el CMa de producir defensa. En estos términos, un determinado nivel de GAMIL responde al riesgo o amenaza que un país enfrenta. De esta manera, el 1% puede ser suficiente mientras en otro el 10% del PBI puede ser muy poco.

Tal como se ha desarrollado, la experiencia de la teoría económica indica que aquellos países con capacidad operativa genuina presentan una relación constante de GAMIL en el gasto de personal (militares activos, civiles, retirados) debería ubicarse entre un 40-60% y las adquisiciones bélicas (armas mayores, buques, blindados, etc) deberían representar un 15-25% todos los años. El resto del GAMIL se distribuye principalmente en operaciones y mantenimiento.

## Bibliografía

**Cusack, T. (2006).** Sinking budgets and ballooning prices: recent developments connected to military spending. Discussion papers // WZB. Wissenschaftszentrum Berlin fürSozialforschung. ForschungsschwerpunktMärkte und Politik. ForschungsgruppeInstitutionen. Staaten. Märkte, No. SP II.

**Cusack, T. & Susanne F. (2003).** Public expenditure statistics. http://wz-berlin.de/mp/ism/staff/cusack.en.htm

**Hartley, K. and Binyam, S. (2015).** Measuring defense output: an economic perspective. enMelese, F., Anke R. and Binyam, S. (Eds.). *Military cost-benefit analysis: theory and practice*. Routledge: New York.

**Hartley, K. (2011).** *The economics of defence policy: a new perspective*. Routledge: New York.

**Hill, Richard (1986).** *Maritime strategy for medium powers.* Naval Institute Press. Annapolis. 1986

**Krugman, P. (2006).** *Introducción a la microeconomía*. Editorial Reverté. Barcelona. España.

**David Kirkpatrick,** "The affordability of defence equipment", RUSI Paper, 1997.

**Lindert, Peter (2004).** *Growing Public Social Spending and Economic growth in the Eighteenth century*.Two volumes. Cambridge University Press.

**Posen, Barry (1984).** *The sources of military doctrine: France, Britain and Germany between the world wars.* Cornell University Press.

**Pugh, P. (1993).** The procurement nexus. Defense Economics. Vol. 4, N° 2.

**Scheetz, T., Pfurr, A., y Ansorena Gratacos, M., (2015).** *Manual de teoría de la gestión económica de las Fuerzas Armadas: una contribución a las bases conceptuales para la orientación de la política militar*. Nuevohacer Grupo Editores Latinoamericano. Buenos Aries.

**Scheetz, T. (2012).** Teoría de la gestión económica de las fuerzas armadas. Documento de Trabajo Nº 7. Escuela de Defensa Nacional. Buenos Aires. Ver www.mindef.gov.ar/edena/docs/inv/DOCT_07_SHEETZ.pdf

**Stiglitz, J. (2000).** *La economía del sector público*. Antoni Bosch Editor. Terceraedición. Barcelona. España.

# Hacia una medición del poder naval en América Latina*

## Towards the measurement of naval power in Latin America

*Noé Cuervo Vázquez***
CENTRO DE ESTUDIOS SUPERIORES NAVALES
SECRETARÍA DE MARINA – ARMADA DE MÉXICO, MÉXICO
*Marcos Pablo Moloeznik****
UNIVERSIDAD DE GUADALAJARA, MÉXICO
✉ mmoloeznik@yahoo.es

**Resumen:** A lo largo de esta contribución se lleva a cabo un esfuerzo por medir el poder naval de los países latinoamericanos con el objetivo de clasificar a las armadas de la región. Para ello, se parte de un proceso de selección de los indicadores más adecuados para cada dimensión de las variables independientes identificadas. Una vez seleccionados los indicadores, resulta necesario fijar los valores de ponderación de cada factor. Aquí, se debe establecer la medida estándar óptima de cada indicador evaluado, para que las medidas de los distintos países se comparen con el estándar óptimo y así obtener el valor del índice del poder naval; valor obtenido que se correlaciona con los índices del poder naval total de los otros países evaluados. El modelo generado para la simulación de los resultados es de ecuaciones lineales, considerando que no se contempla una retroalimentación dinámica de los datos.

**Palabras clave:** poder naval, poder naval total, América Latina, capacidades navales actuales, capacidades navales potenciales.

***Abstract:*** *This article attempts to measure the naval power of the Latin American countries in order to classify the navies of the region. To fulfill this objective, a selection process of the most appropriate indicators for each dimension of the independent variables identified was performed. Once the indicators have been selected, it was necessary to set the weight of each factor. Then, the optimum standard measure of each evaluated indicator was established, so that the measures from different countries could be compared with this optimum standard and the index value of naval power could be obtained. In other words, the value that correlates the indices of all naval power of each evaluated country. The model generated for the simulations is a linea regression, and does not consider dynamic feedback data.*

***Keywords:*** *naval power, total naval power, Latin America, current naval capabilities, potential naval capabilities.*

"A diferencia del ejército y de la fuerza aérea, cuyo tamaño y poder de fuego deben guardar relación con aquellos del adversario potencial, el tamaño de la armada es determiando por el *quantum* de activos e intereses marítimos que uno debe proteger."
Capitán de Fragata de Bangladesh Mohd Khursched Alam

## A manera de introducción

El poder naval, armada o marina de guerra es un instrumento del poder de un Estado-nación, cuya finalidad es la protección y preservación de los activos marítimos, y sus actividades deben ser vistas de acuerdo con los recursos que se le destinan y las misiones que se le encomiendan (Sheina 1991: 15).

Cabe señalar que una marina de guerra, como se conoce tradicionalmente a la armada, es en primer lugar un conjunto de medios: buques, aeronaves, apoyo; y el personal necesario para servirlos. La primacía se suele dar en los medios sobre el personal; lo que no niega que este último constituya la mayor riqueza del poder naval, pero son los medios los que, a diferencia de las otras fuerzas armadas, determinan la estructura de la armada, su modelo (de Saint Salvy 1994: 57).

De donde se desprende la doctrina naval británica clásica, que clasifica a las armadas por el color de las aguas (Moloeznik 2013):

• Blue Water Navy: 1) Estados Unidos de Norteamérica; 2) Reino Unido de la Gran Bretaña, Francia, Rusia, India y Japón.

• Green Water Navy: 1) China y Brasil (potencias en ascenso) 2) Colombia, Venezuela y México (guardacostas con capacidad de proyección oceánica).

• Brown Water Navy: 1) Guatemala, Honduras y el Salvador (Fuerzas Navales) 2) Bolivia y Paraguay (Fuerzas Fluviales)

En ese marco, los portaaviones, los destructores y las fragatas son reconocidos como las principales fuerzas de combate de superficie de las armadas.[1]

Los buques constituyen la esencia misma de la armada. Una marina de guerra podrá carecer de aeronaves, helicópteros, submarinos e infantería de marina, pero no puede concebirse una armada sin buques. A partir de estas ideas-fuerza, la presente contribución tiene por objeto poner a consideración de lector un modelo de medición del poder naval, mediante la determinación de las capacidades reales y potenciales de las armadas de América Latina. En cuanto al empleo del poder naval, conviene abrevar en la propuesta teórica de Milan Vego (2003), para quien el empleo moderno de las fuerzas de combate –consecuencia de la evolución del arte de la guerra– se puede dividir en dos grandes grupos: acciones tácticas navales y grandes operaciones navales, las cuales tienen los siguientes propósitos y acciones:

• Propósitos: destruir la flota enemiga en la mar o sus bases, desembarcar anfibios en costas con

[1] Véase: "Navy" en: International Institute for Strategic Studies (IISS), The Military Balance 2013, Publisher Routledge, London 2013.

oposición, destruir las instalaciones costeras enemigas, interrumpir el comercio marítimo enemigo, proteger el comercio marítimo propio, bloquear o contrabloquear, destruir fuerzas nucleares estratégicas embarcadas del enemigo, proteger las fuerzas nucleares embarcadas propias, apoyar a las fuerzas terrestres en la costa (Vego 2003: 184).

• Acciones: prevención del conflicto, protección del tráfico, libertad de navegación y sobrevuelo, operaciones de paz, conflictos de baja intensidad, asistencia humanitaria, auxilio en catástrofes naturales, búsqueda y salvamento (Vego 2003: 186).

Estos grupos de acciones permiten determinar, de manera objetiva, el nivel de dominio del mar y, con ello, generar un índice del poder naval de un Estado-nación a través de un modelo matemático.

Para dar cumplimiento al objetivo de esta contribución, se determinan dos grandes campos que permiten establecer el Poder Naval Total de un Estado, bajo un esquema estratégico-operacional: las Capacidades Navales actuales[2] y las Capacidades Navales potenciales.[3]

En tanto que, para estar en condiciones para realizar el presente trabajo de investigación, se establecieron los siguientes parámetros:

• Como objeto de estudio se identifica al Poder Naval.

• Como variables se identifica sólo una variable dependiente y dos variables independientes:

Variable Dependiente:

Vd1 = Poder Naval total (PNt).

Variables Independientes:

Vi1 = Capacidad Naval actual (CNa)

Vi2 = Capacidad Naval potencial (CNp)

La definición conceptual de las variables es como sigue:

Vd1 = Poder Naval total (Pnt) y es el valor de la capacidad bélica del Estado en la mar, expresada principalmente por los recursos de la marina de guerra.[4]

Vi1 = Capacidad Naval actual (CNa) y es el valor de la capacidad operativa de las unidades de superficie, aéreas y submarinas adscritas a la marina de guerra, que determinan el dominio positivo o negativo del mar y está determinada por once dimensiones (Diez 2006) con sus indicadores que son mostrados en el siguiente acápite.

Vi2 = Capacidad Naval potencial (CNp) y es el valor de la capacidad de transformación de las capacidades operativas de la marina de guerra, a partir de factores no operativos del Estado que tienen influencia en el aspecto naval (Moloeznik 2009) y está determinada por diez indicadores, en donde se describe el modelo de medición propuesto.

Mientras que la definición operacional de las tres variables es:

Vd = Poder Naval total (PNt)[5] y es el resultado del algoritmo que relaciona a la Capacidad Naval actual (CNa) con la capacidad Naval potencial (CNp), que se construyó durante el desarrollo de la presente investigación, y que se resolvió a partir de un instrumento informatizado desarrollado en el programa EXCEL 2013, quedando la fórmula sintetizada de la siguiente manera:

PNt=CNa+ CNp2

Vi1 = Capacidad Naval actual (CNa) y se midió a partir de un algoritmo que relacionó a las once (11) dimensiones con sus indicadores que conforman el CNa; este algoritmo consiste en la suma algebraica de cada dimensión multiplicada por su ponderación horizontal y vertical, las cuales serán explicadas durante el desarrollo del presente trabajo de investigación.

Vi2 = Capacidad Naval potencial (CNp) y se midió a partir del algoritmo que relaciona a las diez (10) dimensiones con los indicadores que conforman el CNp; este algoritmo consistirá en la suma algebraica de cada dimensión multiplicada por su ponderación horizontal únicamente, las cuales serán explicadas durante el desarrollo del presente trabajo de investigación.

[2] Se refiere al valor de la capacidad operativa de las unidades de superficie, aéreas y submarinasadscritas a la marina de guerra, que determinan el dominio positivo o negativo del mary está determinada por once dimensiones que se explican más adelante.

[3] Es el valor de la capacidad de transformación de las capacidades operativas de la marinade guerra, a partir de factores no operativos del Estado, que tienen influencia en el aspecto navaly está determinada por diez dimensiones que son desarrolladas a continuación.

[4] Esta definición está contenida en el "Glosario de términos unificados por personal de laSecretaría de la Defensa Nacional –SEDENA– y de la Secretaría de Marina (SEMAR)" del 14 de agosto del 2013, autorizado como doctrina por el Alto mando de la Secretaría de Marina – Armada de México en el sup. Of. # c0219/4345/13 del 5 de septiembre del 2013.

[5] Todos los algoritmos son explicados en el acápite "Modelo de medición del poder naval".

## Modelo de medición del poder naval

En este marco y a partir de un enfoque científico-cuantitativo, en primer lugar se lleva a cabo un proceso de selección de los indicadores más adecuados para cada dimensión de las variables independientes identificadas. Cabe destacar que los indicadores seleccionados cumplen principalmente con tres requisitos, a saber: ser válidos, confiables y universales.

Para verificar su validez se revisan, cuidadosamente, las dimensiones del poder naval consideradas por la publicación internacional *IHS Jane's Fighting Ships 2013–2014* (Saunders S. 2013), la enciclopedia naval ilustrada norteamericana, editada por el Departamento de Estado de los Estados Unidos de América, la Guía del Poder Naval en el Mundo (Wragg 2012), los textos especializados de Camil Busquets (Vilanova C. B. 2012) y Octavio Diez (2006) y la *Guía de Barcos de Guerra* actualizada de Chris Chant (2006), principalmente.

La confiabilidad fue establecida a partir de una revisión de la objetividad de la institución o autor de los textos revisados que contemplan a los indicadores del poder naval; y la universalidad, por su parte, se determina evaluando el uso de cada indicador en función de si se emplea a nivel mundial, regional o local.

Una vez seleccionados los indicadores, resulta necesario fijar los valores de ponderación de cada factor. Aquí, se debe establecer la medida estándar óptima de cada indicador evaluado, para que las medidas de los distintos países se comparen con el estándar óptimo y así obtener el valor del índice del poder naval; valor obtenido que se correlaciona con los índices del poder naval total de los otros países evaluados.

El modelo generado para la simulación de los resultados es un modelo de ecuaciones lineales, seleccionado siguiendo la propuesta de Heckbert *et al.* (2010, citado por Cardoso 2011: 7), considerando que no se contempla una retroalimentación dinámica de los datos. Las dimensiones establecidas como más adecuadas en la construcción del modelo para las variables independientes Capacidad Naval actual (CNa) y Capacidad Naval potencial (CNp) son citadas a continuación y están en negritas (Cuervo Vázquez 2014: 15–17).

**Poder Naval actual (PNa)**: **TB**: **Tipo de Buque (**Pa: portaaviones, ph: portahelicópteros, cp: cruceros pesados, cr: cruceros, subm: submarinos misilísticos, subc: submarinos crucero, suba: submarinos de ataque, Dd: destructores, fr: fragatas, Cb: corbetas, an: anfibios, min: minadores, dr:dragaminas/cazaminas, Pt: patrulleros); **Dz: Desplazamiento** (Se mide en toneladas); **Es: Eslora** (Se mide en metros); **Pr**: **Propulsión** (nu: Nuclear, nnu, No nuclear, dia: Doble/alternativa), **Arm: Armamento** (mb: Misil balístico, mcr: Misil crucero, mss: Misil superficie-superficie, msa: Misil superficie- aire, mssub: Misil superficie-submarino, tor: Torpedos, ame: Ametralladoras, min: Minas, car: Cargas de profundidad); **V: Velocidad** (Se mide en nudos); **Aem: Aeronaves embarcadas**; **#Aem: Número de aeronaves embarcadas**; **#Me: Número de misiles embarcados** (#Mb: Misil balístico, #Mcr: Misil crucero, #Mss: Misil superficie-superficie, #Msa: Misil superficie- aire, #mssub: Misil superficie-submarino); **#Us: número de unidades de superficie** (Se mide en números reales); **Sa: Sistemas de armas** (Aeg: Aegis/similar, Par: Parcial, Gss: Guerra superficie-superficie, Gsa: Guerra superficie-aire, Gssub: Guerra superficie-submarino); **CNp: Capacidad Naval potencial**, *per: Personal* (Se mide en número de efectivos encuadrados en el servicio activo); **Pib: Producto interno bruto** (Se mide en miles de dólares); **Ri: Reservas internacionales** (Se mide en millones de dólares); **Ip: Infraestructura portuaria** (Índice de infraestructura portuaria); **Im: Infantería de Marina** (Si existe el cuerpo de Infantería de Marina); **Fz: Fuerzas Navales** (Se mide la cantidad de Fuerzas o Flotas navales); **Enf: Educación naval de formación** (Si existe una escuela naval de formación de oficiales); **Enp: Educación naval de posgrado** (Si existe una escuela naval de nivel de posgrado); **Dtn: Desarrollo tecnológico naval** (Si existe un centro de desarrollo tecnológico naval); **Ane: Aeronaves no embarcadas**.

Una vez identificadas las dimensiones y sus indicadores, es necesario determinar el valor de ponderación por cada dimensión. Para ello, se aplica una encuesta dirigida a informantes clave de una población que cuente con información relevante del Poder Naval, que proporcione el nivel de importancia de cada dimensión y de cada indicador dentro de la valoración del Poder Naval de un Estado. Como población se determinó al personal de alumnos colegiados del Centro de Estudios Superiores Navales (CESNAV) de la Secretaría de Marina/Armada de México, habiendo seleccionado una muestra representativa de 37 oficiales superiores y jefes, con los grados de Capitanes de Navío, Capitanes de Fragata, Capitanes de Corbeta, así como de invitados, pertenecientes a la Maestrías de

Seguridad Nacional y del Diplomado de Estado Mayor.

Con el instrumento ya construido, se distribuyó y se les solicitó que enumeraran, de acuerdo al orden de importancia (siendo el número uno el más importante), las dimensiones y los indicadores de cada reactivo, obteniéndose los siguientes resultados:

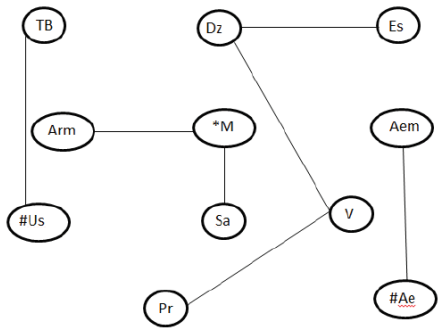
| Nivel de importancia | Dimensión | Valor de ponderación "p" | Orden "p" |
|---|---|---|---|
| 1 | Tipo de Buque | 1 | *P1* |
| 1 | Número de Buques | 1 | *P3* |
| 3 | Sistema de Armas | .830 | *P2* |
| 4 | Número de misiles embarcados | .747 | *P4* |
| 4 | Aeronaves embarcadas | .747 | *P5* |
| 6 | Número de aeronaves embarcadas | .581 | *P11* |
| 8 | Armamento | .415 | *P10* |
| 10 | Velocidad | .249 | *P9* |
| 10 | Eslora | .249 | *P7* |
| 12 | Propulsión | .083 | *P8* |
| 12 | Desplazamiento | .083 | *P6* |

Fuente: elaboración propia.

**Tabla 1 .** Valores ponderados Capacidades Navales Actuales

En tanto que, para poder construir una algoritmo que mida el Poder Naval, se debe entender que la sostenibilidad de las Capacidades actuales del Poder Naval debe ser entendida como un problema complejo que presenta relaciones no lineales entre todos los factores que lo componen. En términos intuitivos significa, por ejemplo, que mayores niveles de esfuerzos navales (cantidad de embarcaciones principalmente), no tienen necesariamente mayores beneficios en el Poder Naval de un Estado.

Si bien no interesa caer en tecnicismos matemáticos, hay que tener presente algunas nociones básicas del proceso de modelación, para facilitar la comunicación del modelo que se propone (Cuervo Vázquez 2014: 15–17). Es decir, la comprensión del planteamiento del problema y requieren al menos un manejo intuitivo del funcionamiento del proceso de modelación matemática.




Fuente: elaboración propia.

**Figura 1 .** Relación de las Capacidades Navales Actuales

Así, en la figura 1 se muestra cómo quedaron relacionados los factores correspondientes a las Capacidades Navales actuales para poder encontrar su relación matemática.

Bajo los resultados de la figura anterior, se puede observar que se forman cuatro conjuntos con características similares en relación directa:

• Conjunto 1: Unidad de superficie, que relaciona al Tipo de Buque (TB) con la cantidad de unidades de superficie (#Us) de manera directa, por lo que se consideró multiplicar ambos factores.

• Conjunto 2: Capacidad de Fuego, que relaciona al Armamento (Arm) con los Sistemas de armas (Sa) y con el número de Mísiles (#M). Aquí también se consideró efectuar una multiplicación entre los tres factores relacionados.

• Conjunto 3: Aeronaves, que relaciona al factor Aeronaves embarcadas (Ae) con el factor Número de aeronaves embarcadas (#Aem), factores que también fueron multiplicados.

• Por último, el Conjunto 4: Características del Buque, contempla cuatro factores, tres de los cuales, Eslora (Es), Desplazamiento (Dz) y Propulsión (Pr) se consideró que debían ser solo sumados y su resultado multiplicarlo por el factor Velocidad (V).

Tomando en consideración los resultados obtenidos tanto en la encuesta (que permitió obtener los valores de las ponderaciones “p” y “q”) y de las relaciones que definieron los conjuntos anteriores, el algoritmo resultante para obtener el valor de la variable: Capacidad Naval actual (CNa), es el siguiente:

$$CNa = \sum_{1}^{n}\left[\left((TBp_1q_1 * \#U_sp_2) + (S_ap_2q_2 * \#M_ep_4 * A_{rm}p_{10}q_5) + (A_{em}p_5 * \#A_{em}p_{11}) + \right.\right.$$
$$\left.\left. + \left(\frac{D_z}{D_{z\,Base}}p_6 + \frac{E_s}{E_{s\,Base}}p_7 + P_rp_8q_3\right) * Vp_9q_4\right)\right]\left(\frac{100}{CN_{a\,Base}}\right)$$

En donde las dimensiones de la variable CNa se multiplican por sus valores ponderados (p y q) y el producto total se multiplica por cien y se divide entre el valor de la variable CNa del país base del modelo, que para este trabajo de investigación es el valor del Poder Naval de los Estados Unidos de América.

En cuanto a la segunda variable independiente CNp, se puede apreciar el siguiente orden de importancia, resultado de la encuesta realizada a expertos en el tema:

| Nivel de importancia | Dimensión | Valor de ponderación "p" | Orden "p" |
|---|---|---|---|
| 1 | Producto Interno Bruto | 1 | *P1* |
| 1 | Flota Naval | 1 | *P2* |
| 1 | Desarrollo Tecnológico Naval | 1 | *P3* |
| 2 | Infraestructura portuaria | 0.88 | *P4* |
| 4 | Personal | 0.66 | *P5* |
| 7 | Infantería de Marina | 0.33 | *P6* |
| 8 | Educación Naval de Formación | 0.22 | *P7* |
| 9 | Educación Naval de Postgrado | 0.11 | *P8* |
| 9 | Reservas Internacionales | 0.11 | *P9* |
| 12 | Aeronaves NO embarcadas | 0.083 | *P10* |

Fuente: elaboración propia.

**Tabla 2 .** Valores ponderados Capacidades Navales Potenciales

Tomando en consideración los resultados obtenidos, se analizó que la relación entre los factores de las Capacidades Navales potenciales no tenían una relación entre ellos que obligara a realizar alguna multiplicación, y todo quedó reducido a la sumatoria de los citados factores.

Sin embargo, fue necesario establecer una constante que nos aproximara a un valor más real de esta variable. Por ello, se consideró que el Producto Interno Bruto (Pib), las Flotas Navales (Fz) y el Desarrollo Tecnológico (Dtn) son los factores más significativos y debían multiplicarse por dos; el factor Infraestructura Portuaria (Ip) se multiplica por la constante 1.5 y el factor Personal (Per) por la constante 1.3; el resto de los factores no son multiplicados por constante alguna y sólo se multiplican al igual que los demás factores por sus ponderaciones "p" y "q".

El algoritmo resultante para obtener el valor de la Capacidad Naval potencial (CNp), es:

En ambas variables independientes las consonantes "p" y "q" se refieren al porcentaje de ponderación tanto a nivel horizontal (que corresponde a la ponderación dentro de la variable y a la ponderación dentro de la propia dimensión).

$$CNp = \left((2)\left(\frac{p_{tb}}{p_{tb\ Base}}p_1\right) + (2)\left(\frac{f_z}{f_{z\ Base}}p_2\right) + (2)\left(\frac{d_{tn}}{d_{tn\ Base}}p_3\right) + (1.5)\left(\frac{i_p}{i_{p\ Base}}p_4\right) + \right.$$
$$\left. + (1.3)\left(\frac{p_{er}}{p_{er\ Base}}p_5\right) + \frac{i_m}{i_{m\ Base}}p_6 + e_{nf}p_7 + e_{np}p_8 + \left(\frac{r_t}{r_{t\ Base}}\right)p_9 + A_{ne}p_{10}\right)$$

Una vez obtenidos los valores de las variables independientes, el algoritmo final para obtener el de la variable dependiente (Poder Naval) quedó de la siguiente manera:

$$PNt = \frac{CN_a + CN_p}{2}$$

Con los valores correspondientes las variables independientes y la variable dependiente, se integra nuevo algoritmo, con el fin de determinar un índice de riqueza marítima nacional que permitiera interactuar con los valores obtenidos y encontrar cómo se ve reflejado el Poder Naval de un Estado las riquezas marítimas que debe proteger. Para ello, y de acuerdo al marco teórico propuesto, se establece que el Indice de Riqueza Marítima Nacional (IMRN)[6] está en función de los siguientes factores (Cuervo Vázquez 2014: 22): pc: plataforma continental (se mide en kilómetros cuadrados), zp: zonas de pesca (se mide en kilómetros cuadrados), Aa: Área arrecifal (se mide en kilómetros cuadrados), zee: zona económica exclusiva (se mide en kilómetros cuadrados), ep: exportaciones petroleras (se mide en barriles diarios), lpi: Índice de eficiencia logística (se mide según el Banco Mundial), tmc: tráfico marítimo de contenedores (se mide en número de contenedores), ipib: % importaciones del PIB (se mide en porcentaje), epib: % exportaciones del PIB (se mide en porcentaje).

El algoritmo para obtener el IRMN[7] que se utiliza en el presente modelo quedó sujeto a una sumatoria de todos los factores multiplicados por su valor de ponderación "p", de la siguiente manera:

$$IRMN = \left(\left(\frac{k_{lc}}{k_{lc\ Base}}p_1\right) + \left(\frac{p_c}{p_{c\ Base}}p_2\right) + \left(\frac{z_p}{z_{p\ Base}}p_3\right) + \left(\frac{A_a}{A_{a\ Base}}p_4\right) + \left(\frac{z_{ee}}{z_{ee\ Base}}p_5\right) + \frac{e_p}{e_{p\ Base}}p_6 + \right.$$
$$\left. + \left(\frac{l_{pi}}{l_{pi\ Base}}p_1\right) + \left(\frac{t_{mc}}{t_{mc\ Base}}p_1\right) + \left(\frac{i_{pib}}{i_{pib\ Base}}\right)p_9 + \left(\frac{e_{pib}}{e_{pib\ Base}}p_1\right)\right)$$

Una vez con el valor del IRMN, se procedió a obtener el índice de defensa marítima (IDM), el cual es el resultado de multiplicar el Poder Naval total por 100 y dividirlo entre el IRMN; la diferencia del IDM con 100 nos dará el porcentaje de riqueza marítima sin protección (%RSP). Estos valores para la presente contribución son indicadores de cobertura del Estado ante actores no estatales; para obtener un comparativo entre naciones, es necesario comparar el Poder Naval total (PNt) de cada país.

[6] Este índice de riqueza marítima nacional no abarca todos los intereses marítimos de un Estado, por ser tema del Poder Marítimo Nacional, el cual no es abordado en la presente contribución. Sin embargo, los factores considerados permiten interactuar con un nivel de confianza aceptable a la variable obtenida del Poder Naval total de un país y determinar el nivel de protección de la citada riqueza.

[7] El IRMN, es un índice de la riqueza marítima de un país con relación a valores base obtenidosde los primeros puestos de los reportes publicados, donde se localizan los indicadores seleccionados.

$$IDM = \frac{PN_t * 100}{IRMN} \qquad \%RSP = 100 - IDM$$

El modelo concluye asignando el tipo de armada que su poder naval total le otorga, según la siguiente propuesta de nueve niveles de Till (2007: 153–154):

• Armada de proyección de fuerza global mayor – completa (ejemplo: EE.UU.). Puede trasladar su poder naval a cualquier parte del mundo y en varios escenarios a la vez de manera permanente.

• Armada de proyección de fuerza global mayor-parcial (ejemplo: extinta Unión de Repúblicas Socialistas Soviéticas). Puede trasladar su poder naval a cualquier parte del mundo en máximo dos escenarios a la vez de manera temporal.

• Armada de proyección de fuerza global mediana (ejemplo: Francia, Gran Bretaña). Puede trasladar una parte de su poder naval a cualquier parte del mundo en un escenario a la vez de manera temporal.

• Armada de proyección de fuerza regional mediana (ejemplo: India, China, Japón). Puede trasladar su poder naval a escenarios cercanos a su territorio dentro de la región geográfica que ocupa.

• Armada de proyección de fuerza adyacente (ejemplo: Portugal, Israel, Sudáfrica). Puede proyectar su poder naval a las áreas marítimas adyacentes a su zona económica exclusiva (ZEE).

• Armada de defensa territorial marítima (ejemplo: Noruega, Egipto). Tiene la capacidad de negar el uso del mar al enemigo y presentar combate sólo en la ZEE.

• Armada de defensa territorial costera (ejemplo: Omán, Singapur). Tiene la capacidad de negar el uso del mar al enemigo y presentar combate sólo en el mar territorial.

• Armada de vigilancia policial (ejemplo: México, Sri Lanka). Tiene la capacidad de mantener el Estado de derecho en su ZEE contra la delincuencia organizada, pero no tiene la capacidad de negar el uso del mar a la fuerza naval de otro Estado.

• Armadas simbólicas. No tiene la capacidad de mantener el Estado de derecho en su ZEE contra la delincuencia organizada.

## Una aproximación a la medición del poder naval en América Latina

El continente americano cuenta con 35 países divididos principalmente en dos regiones, una conformada por los Estados Unidos de América y Canadá y otra que integra a los países latinoamericanos[8]. En la presente tesis, se realizó un análisis de las Armadas nacionales de los 33 países que integran la región de Latinoamérica[9], divididos, a su vez, en cuatro áreas:

| Área norte | El Caribe | Centroamérica | Sudamérica |
|---|---|---|---|
| México | Antigua y Barbuda | Belice | Argentina |
| | Bahamas | Costa Rica | Bolivia |
| | Barbados | El Salvador | Brasil |
| | Cuba | Guatemala | Chile |
| | Dominica | Honduras | Colombia |
| | Granada | Nicaragua | Ecuador |
| | Haití | Panamá | Guyana |
| | Jamaica | | Paraguay |
| | República Dominicana | | Perú |
| | San Cristóbal y Nieves | | Surinam |
| | San Vicente y las Granadinas | | Uruguay |
| | Santa Lucía | | Venezuela |
| | Trinidad y Tobago | | |

Fuente: elaboración propia.

**Tabla 3 .** Países según área de ubicación

Cabe señalar que se hace una presentación de las armadas de los países latinoamericanos a partir de la consideración que no se tomaron en cuenta los buques de porte menor a 200 toneladas de desplazamiento, con excepción de las seis patrullas costeras clase Constitución de Venezuela, que a pesar de tener un desplazamiento de 173 toneladas, sus misiles superficie–superficie (SSM) les confieren un importante poder de fuego.

Tratándose del área del Caribe, de los 13 países que la integran, Jamaica cuenta con dos patrullas costeras, Trinidad y Tobago con tres patrullas

[8] Esta división tradicional se utiliza en el presente trabajo, en el que se consideraron como parte de Latinoamérica, a los países del Caribe y Sudamérica que no son hispano-parlantes, pero que por sus condiciones de países en vías de menor grado de desarrollo relativo con respecto al centro desarrollado, tienen características similares como nación.

[9] Los datos de las Armadas, se basan sólo en fuentes abiertas especializadas, principalmente la información que contiene *el Jane´s Fighting Ships 2011–2012, The World Sea Power Guide del 2012 y Barcos de Guerra* (Chant 2006).

costeras y República Dominicana con dos patrullas costeras, sin embargo, tienen un valor de su poder naval menor a la unidad, por lo que no requieren que se les analice mayormente. Cuba, por su parte, cuenta con un buque de la clase Pauk II artillado con seis misiles superficie-aire (SAM) SA-N-5, una patrulla costera clase Trawler con 46 misiles SSM y seis patrullas costeras clase OSA II, también artillada con 46 SSM, ambas con misiles SS-N-2B, así como con cuatro unidades de superficie más. El resto de los países del Caribe no tienen unidad de superficie alguna que desplace el tonelaje requerido.

En Centroamérica, solamente dos países cuentan con unidades de superficie a considerar: Panamá que tiene dos patrullas costeras y El Salvador que cuenta con una. Sin embargo, su índice de poder naval, junto con el resto de los países de esa área, no resultó significativo para la presente contribución.

En Sudamérica la situación es diferente. Bolivia, Guyana y Surinam no cuentan con buques de porte mayor a 200 toneladas y su nivel de poder naval tiende a cero. Uruguay, por su parte, cuenta con dos fragatas clase Joao Belo, una patrulla oceánica clase Wangerooge, tres patrullas clase Kondor II y dos patrullas clase Vigilante, todas sin capacidad de misiles. Paraguay también cuenta con una armada muy pequeña, con cinco buques divididos de la siguiente manera: todos son buques patrulla, uno de la clase River Defense, dos de la clase Bouchard, uno de la clase Itaipu y uno de la clase River Patrol. Al igual que Uruguay, su armada no cuenta con capacidad de misiles. Los países restantes de Sudamérica cuentan con armadas más estructuradas y mejor equilibradas, algunas, como Brasil, con portaaviones y la mayoría con fuerza submarina.

Argentina tiene 1.084.386 km² de Zona Económica Exclusiva (ZEE), 5.029 km lineales de costa, 785.879 km² de plataforma continental, 166.486 km² de zonas pesqueras, un tráfico de contenedores de 2.136.911 TEU[10], un índice de infraestructura portuaria del 3,7 y una exportación petrolera de 238.100 barriles de crudo diarios, como parte de sus riquezas marítimas. Para su protección, la Armada Argentina (ARA) cuenta con 18.249 elementos, de los cuales 2.800 están destinados a la Infantería de Marina y 2.000 a la Aviación Naval. Tiene una pequeña fuerza submarina de construcción alemana integrada con un submarino de ataque de la clase Salta y dos de la clase Santa Cruz y tiene planes de construir un submarino de propulsión nuclear (Wragg 2012: 254) [11]. Además, cuenta con cuatro destructores de la clase Meko 360, artillados con 70 SSM Exocet MM40, 13 SAM Aspide y espacio para un helicóptero Fennec; tres fragatas clase Drummond, con 42 SSM Exocet MM38, seis fragatas clase Meko 140 con 42 SSM Exocet MM38; dos patrullas clase Intrépida, con 42 SSM Exocet MM38 y 15 buques patrullas de desplazamiento mayor a 200 toneladas.

Brasil tiene una ZEE de 3.179.693 km², 7.491 km lineales de costa, 708.805 km² de plataforma continental, 376.117 km² de zonas pesqueras, un tráfico de contenedores de 8.649.821 TEU, un índice de infraestructura portuaria de 2,7 y una exportación petrolera de 801.200 barriles de crudo diarios como parte de sus riquezas marítimas. La Marina de Guerra de Brasil tiene 38.800 elementos de los cuales 15.800 son infantes de marina, siendo la única del subcontinente –y unas de las diez del orbe– en contar con un portaaviones de la clase Clemenceau (São Paulo), con un ala embarcada de 15 aviones Mcdonnell Douglas Skyhawk, al que se suman cuatro submarinos de ataque de la clase Scorpene modificada, cuatro submarinos de ataque de la clase Tupi y un submarino de ataque de la clase Tikuna. Al igual que Argentina, existen planes para la construcción de un submarino de propulsión nuclear y ha habido informes no confirmados que la República Popular China está ayudando en el diseño a cambio de ayuda con el funcionamiento de arrastre de aviones de ala fija embarcados (Wragg 2012: 518). Su fuerza de misiles en unidades de superficie está distribuida en tres fragatas Broadsword con 42 SSM Exocet MM38 y cinco SAM Sea Wolf, capaz de transportar dos helicópteros Súper Lynx ASW; seis fragatas Niteroi con 70 SSM Exocet MM40 y 21 SAM Aspide 2000, cuatro corbetas clase Inhauma con 70 SSM Exocet MM40 y una corbeta clase Barroso con 70 SSM Exocet MM40, capaz de embarcar un helicóptero Súper Lynx; cuenta, además, con 34 buques tipo patrullas, dos buques de guerra anfibia de la clase Thomaston y uno de la clase Newport, uno de la clase Sir

[10] El tráfico portuario de contenedores mide el flujo de contenedores del modo de transporte terrestre a marítimo y viceversa, en unidades equivalentes a 20 pies (TEU), un contenedor de tamaño estándar.

[11] Cabe destacar que esta afirmación hecha por Wragg (2012) parece muy aventurada y completamente descartada por Moloeznik y Guevara (2014).

Galand, uno de la clase Sir Bedivere, tres barcazas de desembarco de más de 200 toneladas de desplazamiento y seis buques tipo dragaminas de la clase Schutze. De acuerdo con Moloeznik (2016), el 1 de marzo de 2013, la entonces presidenta Dilma Rousseff inauguró la planta de fabricación de naves a propulsión nuclear. Con esto, Brasil ingresará al selecto grupo de países equipados con submarinos de propulsión nuclear y se convertirá en el sexto país en el mundo capaz de desarrollar ese tipo de submarino con la clara intención de proyectarse sin descuidar sus zonas marítimas. Tampoco debe soslayarse el reciente anuncio del ministro brasileño de defensa, Celso Amorim, quien afirmó que la construcción de un portaaviones propio figura entre los futuros proyectos del país.

Chile, por su parte, cuenta con 2.009.299 km² de ZEE, 6.435 km lineales de costa, 160.916 km² de plataforma continental, 211.070 km² de zonas pesqueras, un tráfico de contenedores de 3.406.267 TEU, un índice de infraestructura portuaria del 5,2 y una exportación petrolera de 52.390 barriles de crudo diarios, como parte de sus riquezas marítimas. Mientras que para su protección, la Armada de Chile está conformada por 25.699 elementos, de los cuales 807 son reclutas en entrenamiento voluntario de 22 meses. Tiene en servicio activo dos clases de submarinos, con dos unidades igualmente, la clase Scorpene y la clase Thomson; cuenta con dos fragatas clase Doorman con 130 SSM Harpoon y 15 SAM Sea sparrow, dos fragatas clase Latorre de construcción holandesa artilladas con 130 SSM Harpoon y 46 SAM SM-1MR, tres fragatas de la clase Leander con 130 SSM Harpoon y 6 SAM Sea wolf, una fragata Clase Broadsword con 130 SSM Harpoon y 10 SAM Barak I y dos buques patrulla clase SAAR 4 armadas con 36 SSM Gabriel II. Tiene, además, tres clases de buques tipo patrulla: cuatro clase Tiger (Riquelme), dos clase Piloto Pardo y seis clase Micalvi; dos buques de guerra anfibia de la clase Batral (Maipo), uno de la clase Newport, uno de la clase Alvsborg y dos de la clase Elicura.

Colombia tiene 817.816 km² de ZEE en dos litorales, 3.208 km lineales de costa, 43.316 km² de plataforma continental, 36.460 km² de zonas pesqueras, un tráfico de contenedores de 2.572.012 TEU, un índice de infraestructura portuaria de 3,5 y una exportación petrolera de 400.700 barriles de crudo diarios. Por su parte, la Armada colombiana tiene en servicio activo a 21.000 elementos, de los cuales 7.200 son conscriptos, 146 son de aviación naval y 9.000 son infantes de marina. Tiene también dos submarinos de ataque de la clase Pijao, cuatro fragatas clase Alm. Padilla con 70 SSM Exocet MM40 (siendo las únicas con misiles embarcados con que cuenta) con capacidad para un helicóptero ligero como un Fennec o un Bo-105, dos buques de guerra de minas, 18 buques patrullas y siete barcazas de desembarco de la clase Morrosquillo.

Ecuador es poseedor de una ZEE de 236.597 km², de 2.237 km lineales de costa, 24.679 km² de plataforma continental, 23.894 km² de zonas pesqueras, un tráfico de contenedores de 1.291.494 TEU, un índice de infraestructura portuaria de 4,2 y una exportación petrolera de 333.400 barriles de crudo diarios. Su Armada es de 7.283 efectivos encuadrados, incluyendo a 2.160 infantes de marina y 375 de aviación naval. Tiene dos submarinos de ataque la clase Shyri, dos fragatas clase Leander con 70 SSM Exocet MM40 y 5 SAM Seacat con capacidad para un helicóptero Bell Jet Ranger, seis corbetas de la clase Esmeralda con plataforma de anaveaje, armadas con 70 SSM Exocet MM40 y 13 SAM Aspide, tres buques patrulla de la clase Lurssen y 42 SSM Exocet MM40. Cuenta además con seis buques patrullas sin misiles clases Cherokee (1), Espada (2) e Isla Fernandina (3).

Perú es un país andino con litoral en el Pacífico, tiene 906.454 km² de ZEE, 2.997 km lineales de costa, 79.198 km² de plataforma continental, 55.339 km² de zonas pesqueras, un tráfico de contenedores de 1.621.484 TEU, un índice de infraestructura portuaria de 4,7 y una exportación petrolera de 73.280 barriles de crudo diarios. La marina de guerra de Perú está compuesta por 23.246 elementos, incluyendo 3.500 infantes de marina, 1.000 miembros de la guardia costera y 800 de aviación naval. Tiene seis submarinos de ataque clase Angamos, un crucero de batalla (el único en Latinoamérica) clase De ruyter armado con 160 SSM Otomat Mk2, cuatro fragatas clase Lupo modificada con 160 SSM Otomat Mk2 y 13 SAM Aspide, cuatro fragatas Lupo (Aguirre) artilladas con 160 misiles SSM Otomat Mk2 y 13 SAM Aspide con capacidad para un helicóptero Bell 212, seis buques patrulla clase Velarde con 42 SSM, 11 buques patrullas sin capacidad de misiles y cuatro buques de guerra anfibia de la clase Terrebone Parrish.

El último país a analizar del área de Sudamérica es la República Bolivariana de Venezuela, la cual cuenta con una ZEE de 471.507 km², 4.800 km

lineales de costa, 99.889 km² de plataforma continental, 109.426 km² de zonas pesqueras, un tráfico de contenedores de 1.296.419 TEU, un índice de infraestructura portuaria de 2,5 y una exportación petrolera de 1.871.000 barriles de crudo diarios. Su marina de guerra está compuesta por 17.994 elementos que incluyen a 3.200 conscriptos que prestan servicio hasta por 30 meses, aunque el servicio militar obligatorio es por selección y el periodo es variable; tiene 7.000 infantes de marina y 500 en el cuerpo de aviación naval. Sus barcos han sido adquiridos de diferentes países, incluyendo a Corea de Sur, pero el país se ha ido moviendo hacia la izquierda en el ámbito político y ha sido la primera nación latinoamericana en realizar ejercicios navales con la Armada Rusa, cuando los barcos de la Flota del Norte visitaron el Caribe en el 2008. Es probable que en el futuro, la Armada Bolivariana de Venezuela se acerque más a Rusia e incluso a la Armada China (Wragg 2012), aunque, de acuerdo con Moloeznik (2016), el gobierno se está acercando a los chinos para obtener suministros, logística y equipo terrestre (blindados y artillería) para la infantería de marina, pero la armada apuesta por la obtención de equipo europeo únicamente. Cuenta con dos submarinos de ataque de la clase Sabalo y 61,2 mts. de eslora, seis fragatas clase Lupo modificada 160 SSM Otomat Mk2 y 13 SAM Aspide con capacidad para un helicóptero AB-212 ASW, seis patrullas costeras clase Constitución con 80 SSM Otomat Mk2. Estos son los únicos buques que tienen capacidad de lanzamiento de misiles. Tiene, además, cuatro buques patrullas de la clase Alligator, cuatro buques patrulla clase Guaiqueri, cuatro patrullas clase Guaicamacuto, dos barcazas de guerra anfibia clase Ajeera y un buque logístico auxiliar de la clase AORH.

México es el último país de la región (aunque del área norte) que cuenta con una Armada estructurada. Tiene una ZEE de 3.269.386 km² de ZEE en dos litorales, 11.953 km lineales de costa, 402.064 km² de plataforma continental, 251.122 km² de zonas pesqueras, un tráfico de contenedores de 3.893.946 TEU, un índice de infraestructura portuaria de 4,4 y una exportación petrolera de 1.511.000 barriles de crudo diarios. Su fuerza naval está constituida por 56.324 elementos que incluyen a 18.000 infantes de marina y 1.250 en el cuerpo de aviación naval. Como unidades de superficie tiene un destructor clase Gearing Fram I, sin capacidad de misiles, cuatro fragatas clase Knox, con un lanzador octuple Mk 25 para SAM Sea Sparrow, dos fragatas clase Bronstein, dos buques patrullas clase SAAR 4.5 con 36 SSM Gabriel y 10 SAM Barak I, y los siguientes buques tipo patrulla oceánica sin capacidad de misiles: cuatro de la clase Holzinger, cuatro de la clase Durango, tres de la clase Sierra, seis de la clase Oaxaca, seis de la clase Uribe, dos de la clase Demócrata y 10 de la clase AUK. Además cuenta con dos buques de guerra anfibia de la clase Newport y dos buques de guerra anfibia de la clase Montes Azules. Los buques antes mencionados, con excepción de los clase AUK, tienen plataforma de anaveaje y su aviación de ala móvil tiene incorporados helicópteros Phanter, Black Hawk, Bolkow, Fennec, MI-17 y MD.

Recapitulando, el modelo de medición utiliza las variables descritas para obtener los valores de los siguientes índices: Capacidades Navales actuales, Capacidades Navales potenciales, Poder Naval Total, Tipo de Armada, Índice de Riqueza Marítima Nacional, Índice de Defensa Marítima Policial, Índice de Defensa Naval, Porcentaje de Riqueza Marítima sin protección actual (contra infractores de la ley), Porcentaje de Riqueza Marítima sin protección actual (contra otra Fuerza Naval).

Dentro del primer rubro Capacidades Navales actuales, se observa que Chile es el país que actualmente tiene el mayor índice de esta categoría. Su poder de fuego obtenido gracias a sus fragatas clase Doorman, Latorre y Leander con sus misiles Harpoon ha sido determinante para alcanzar el primer puesto por encima de las demás naciones.

En segundo lugar, se encuentra Perú teniendo como buques más representativos a sus ocho fragatas Lupo (4 modificadas y 4 “Aguirre”) con sus misiles Otomat MK2.

Brasil, a pesar de ser el único país con portaaviones de la región, no cuenta con una capacidad de misiles representativa, y por esa razón sus capacidades navales actuales lo colocaron solo en el tercer puesto. De hecho, al ser su ala embarcada en el portaaviones São Paulo un tanto antigua, los buques que más incrementaron su índice de Capacidades Navales actuales fueron sus seis fragatas Niteroi con sus misiles Exocet MM40.

En cuarto lugar se colocó Venezuela con sus seis fragatas Lupo modificadas y sus misiles Otomat MK2. Casi con las mismas capacidades navales se encuentra Ecuador, teniendo como buques más importantes a sus seis corbetas clase Esmeralda

artilladas con misiles Exocet MM40.

Argentina le sigue en capacidades navales actuales con sus cuatro fragatas MEKO 360 y sus misiles Exocet MM40, mientras que Colombia, Cuba y México son los últimos tres países de los nueve analizados, que el modelo coloca con las capacidades navales actuales más bajas (obviamente, sin considerar a los países del Caribe, Centroamérica y Sudamérica, que no cuentan con armadas significativas). El modelo indica que los buques que aportan más al índice de capacidades actuales a Colombia, son sus cuatro fragatas clase Alm. Padilla con 70 SSM Exocet MM40, a Cuba son sus seis patrullas costeras clase OSA II artilladas con misiles SS-N-2B y a México son sus dos buques patrullas clase SAAR 4.5 con misiles Gabriel. (Cuervo Vázquez 2014: 33–34)

| PAÍS | Capacidades actuales |
|---|---|
| Chile | 23,95 |
| Perú | 17,1 |
| Brasil | 9,87 |
| Venezuela | 6,42 |
| Ecuador | 6,32 |
| Argentina | 4,94 |
| Colombia | 2,72 |
| Cuba | 1,63 |
| México | 1,38 |

Fuente: elaboración propia.[12]

**Figura 4 .** Capacidades Navales actuales

Con relación a sus Capacidades Navales potenciales, el país que tiene en estos momentos el mayor potencial de desarrollo es México, basado principalmente en la cantidad de elementos en servicio activo junto a la cantidad de infantes de marina, que supera a todos sus vecinos, aunado a la calidad de su infraestructura portuaria. Sus valores analizados en el modelo de medición del Poder Naval, lo ubicaron escasamente por encima de Brasil, ya que ambos tienen importantes Productos Internos Brutos y Reservas Internacionales, y muy por encima de naciones como Colombia, Argentina, Venezuela y, sobre todo, Cuba. Los valores que se obtuvieron se indican en la figura 5.

| PAÍS | Capacidades potenciales |
|---|---|
| México | 23,95 |
| Brasil | 17,1 |
| Chile | 9,87 |
| Perú | 6,42 |
| Ecuador | 6,32 |
| Colombia | 4,94 |
| Argentina | 2,72 |
| Venezuela | 1,63 |
| Cuba | 1,38 |

Fuente: elaboración propia.

**Figura 5 .** Capacidades Navales potenciales

La suma algebraica de las anteriores variables (Variables Independientes del presente trabajo), arrojan el siguiente valor de la variable dependiente Poder Naval total: el país con el mayor Poder Naval total en Latinoamérica es Chile, seguido de cerca por Perú y Brasil. Este Poder está basado en su importante arsenal de misiles y sus sistemas de armas. A una distancia alejada, se encuentran Ecuador, México, Argentina, Venezuela y Colombia (los cuales tienen valores muy similares de su Poder Naval total, ya que han basado su desarrollo naval en torno a patrullas oceánicas sin misiles embarcados), y en un último y muy alejado lugar se encuentra Cuba con una armada pequeña y de poco potencial.

| PAÍS | Poder Naval Total |
|---|---|
| Chile | 20,37 |
| Perú | 16,94 |
| Brasil | 14,25 |
| Ecuador | 10,7 |
| México | 10,16 |
| Argentina | 9,63 |
| Venezuela | 9,19 |
| Colombia | 8,53 |
| Cuba | 2,87 |

Fuente: elaboración propia.

**Figura 6 .** Poder Naval Total

Con los valores anteriores, fue posible determinar en qué tipo de armada se encuentra clasificado cada país, las más altas: Chile, Perú y Brasil son del Tipo 6 (Till 2007, Vid Supra), lo que las ubica como Armadas de Defensa Territorial Marítima, las cuales tienen capacidad de negar el uso del mar al enemigo y presentar combate en su Zona Económica Exclusiva (ZEE). Ecuador, México, Argentina y Venezuela tienen Armadas de nivel 8, de la clase: Armadas de Vigilancia policial, con la capacidad de mantener el Estado de derecho en su ZEE contra la delincuencia organizada, pero no tienen la capacidad de negar el uso del mar a una fuerza Naval de otro Estado (Cuervo Vázquez 2014: 37–38). En la figura 8 se observa el Tipo de Armada de cada país analizado; conforme se va acercando al centro de la figura, la Armada va adquiriendo mayor Poder Naval total.

[12] Todas las figuras que se presentan, toman en consideración, por una parte, a un país de Latinoamérica y, por otra, el valor de un índice obtenido por medio del modelo de medición del Poder Naval descrito.

| PAÍS | Tipo de Armada |
|---|---|
| Brasil | 6 |
| Chile | 6 |
| Perú | 6 |
| Argentina | 8 |
| Colombia | 8 |
| Ecuador | 8 |
| México | 8 |
| Venezuela | 8 |
| Cuba | 9 |

Fuente: elaboración propia.

**Figura 8 .** Tipos de Armada

El Modelo de medición del Poder Naval, permite también encontrar el valor del Índice de Riqueza Marítima Nacional: Brasil es el país que cuenta con más de 14% de la riqueza marítima de Latinoamérica, seguido por México con más del 12%; de ahí, ningún otro país cuenta con más de 10% de la riqueza marítima de la región (Figura 9).

A partir del valor anterior (IRMN), se obtienen dos valores más, igualmente importantes: el índice de Defensa Marítima Policial, el cual nos indica a partir de la relación de su Poder Naval total y su índice de riqueza, qué porcentaje de esta riqueza está siendo protegida contra infractores de la ley y cuánto de este porcentaje se encuentra sin protección.

Cinco países cuentan con armadas capaces de proteger al 100% a su riqueza marítima contra los infractores de la ley: Chile, Colombia, Ecuador, Perú y Venezuela. Argentina la protege en un 81,3%, Brasil y Venezuela en un poco más del 70 % y, por último, México, que con su armada actual alcanza a proteger un 62,9 % de sus riquezas marítimas. Las gráficas siguientes nos muestran los porcentajes de riqueza marítima sin protección actual contra infractores de la ley (conforme más se acerca el país al centro, mayor es el porcentaje sin protección, Figura 10).

| PAÍS | Índice de Riqueza Marítima | |
|---|---|---|
| Brasil | 18 | 14,17% |
| México | 16 | 12,60% |
| Argentina | 12 | 9,45% |
| Chile | 9 | 7,09% |
| Venezuela | 9 | 7,09% |
| Colombia | 5 | 3,94% |
| Perú | 5 | 3,94% |
| Cuba | 4 | 3,15% |
| Ecuador | 4 | 3,15% |

Fuente: elaboración propia.

**Figura 9 .** Indice de Riqueza Marítima Nacional

El último valor que se obtiene con el modelo, es el Índice de Defensa Naval, el cual nos permite relacionar las Capacidades Navales actuales con el índice de Riqueza Marítima Nacional, y obtener un porcentaje de defensa actual contra amenazas provenientes de otra fuerza naval. Su valor nos proporciona también el porcentaje de riqueza marítima sin proteger.

| PAÍS | Índice de Defensa contra Infractores de la Ley |
|---|---|
| Chile | 100 |
| Colombia | 100 |
| Ecuador | 100 |
| Perú | 100 |
| Venezuela | 100 |
| Argentina | 81,3 |
| Brasil | 78,6 |
| Cuba | 74,6 |
| México | 62,9 |

Fuente: elaboración propia.

**Figura 10 .** Indice de Defensa contra Infractores de la Ley.

| PAÍS | % Riqueza Marítima sin proteger contra infractores de la ley |
|---|---|
| México | 37,1 |
| Cuba | 25,4 |
| Brasil | 21,4 |
| Argentina | 18,7 |
| Chile | 0 |
| Colombia | 0 |
| Ecuador | 0 |
| Perú | 0 |
| Venezuela | 0 |

Fuente: elaboración propia.

**Figura 11 .** Porcentaje de Riqueza Marítima sin proteger contra Infractores de la Ley.

Los valores obtenidos permiten observar que Chile, Ecuador y Perú cuentan con armadas capaces de proteger[13] al 100 % a sus riquezas marítimas contra otro Estado agresor. Venezuela tiene un índice de protección del 73 %, Brasil, Colombia, Cuba y Argentina cuentan con un porcentaje de protección alrededor del 50% y sólo México cuenta con un valor muy bajo de menos de 10 % de protección de sus riquezas contra otra fuerza naval de un Estado agresor (Figura 12).

| PAÍS | Índice de Defensa contra Flota Naval |
|---|---|
| Chile | 100 |
| Ecuador | 100 |
| Perú | 100 |
| Venezuela | 73 |
| Brasil | 54,5 |
| Colombia | 49,8 |
| Cuba | 42,3 |
| Argentina | 41,8 |
| México | 8,6 |

Fuente: elaboración propia.

**Figura 12 .** Indice de Defensa contra Flota Naval

[13] Esto se refiere solo a la proporción entre sus capacidades navales actuales y su riqueza marítima, en función de datos cuantitativos. Queda claro que la defensa de un territorio contra otro Estado enemigo pasa también por datos cualitativos como voluntad de lucha y resistencia, experiencia en combate, nivel de capacitación y adiestramiento, unidad nacional, fortaleza ideológica, entre otros intangibles, variables que no son abordadas en el presente estudio.

| PAÍS | %Riqueza Marítima sin proteger contra Flota Naval |
|---|---|
| México | 91,4 |
| Argentina | 58,2 |
| Cuba | 57,7 |
| Colombia | 50,2 |
| Brasil | 45,5 |
| Chile | 0 |
| Ecuador | 0 |
| Perú | 0 |
| Venezuela | 0 |

Fuente: elaboración propia.

**Figura 13 .** Porcentaje de Riqueza Marítima sin proteger contra otra Flota Naval

A partir de la aplicación del modelo y la descripción previa de las armadas, se puede observar que en Latinoamérica conviven tres paradigmas del poder naval: el brasileño, el chileno y el colombiano (Moloeznik 2013). Sólo Brasil y Chile (quien resultó el mejor calificado según el modelo), aspiran a dar un salto cualitativo y proyectar su poder nacional en apoyo a sus intereses marítimos y a su política exterior, es decir, al activo papel que persiguen en el concierto de las naciones.

De conformidad con The Military Balance (2013), la armada brasileña (a pesar de salir en tercera posición), tiene un programa muy ambicioso de adquisición de fragatas, submarinos y patrulleros de altura. Se encuentran en construcción, entre otros, submarino nuclear ordenado en 2009 para estar listo en 2025 así como cuatro submarinos de ataque de propulsión diésel que pretenden estar listos en el 2017.

Chile es un país esencialmente marítimo (su visión operacional actual de su armada lo colocó en el primer sitio); el mar es vital para su desarrollo y fundamental para la subsistencia de su población, manifiesta la voluntad y compromiso internacional de ejercer presencia en el espacio de la alta mar aledaño a su zona económica exclusiva, denominado "mar presencial", donde ha asumido una serie de responsabilidades internacionales relacionadas con la protección de la vida humana en el mar, el control del tráfico marítimo y la conservación del medio ambiente (Moloeznik 2016).

La Armada Nacional de Colombia (que representa al tercer paradigma) se encuentra inadecuadamente equipada para hacer frente a las responsabilidades como fuerza bioceánica (mar Caribe y Océano Pacífico). Recientemente, sus esfuerzos de modernización de la flota se concentraron en los buques patrulleros de río y aviación de patrullaje, así como en su infantería de marina, instrumento ad hoc para combatir la insurgencia y el narcotráfico.

El modelo colombiano (en donde se debe incluir a México) constituye la antítesis del brasileño, según la propuesta de paradigmas de Moloeznik (2016). A pesar de su condición de país bioceánico, ha otorgado prioridad a la amenaza del llamado narcoterrorismo y, al igual que México, ambos otorgan preeminencia a las lanchas patrulleras costeras, interceptoras y oceánicas, en detrimento de destructores, cruceros, fragatas e incluso corbetas y, asimismo, presentan una infantería de marina sobredimensionada.

## Conclusiones y soluciones para el caso mexicano

Las conclusiones que a continuación se exponen se desprenden de los resultados obtenidos y permiten establecer lo siguiente:

• Las Capacidades Navales actuales de México se encuentran en el último sitio de los nueve países seleccionados como muestra. En contraste, sus Capacidades Navales potenciales son las más altas de la región, lo que explica que el Poder Naval total de México se ubique en la posición número cinco de los nueve evaluados respecto a su Poner Naval total.

• La clasificación de los países con el mayor Índice de Poder Naval en Latinoamérica es: primer lugar Chile, seguido por Perú, Brasil, Ecuador, México, Argentina, Venezuela, Colombia y Cuba, consecutivamente.

• El país con el mayor índice de Capacidades Navales potenciales es México, seguido de Brasil.

• El país con el mayor índice de Capacidades Navales actuales es Chile, seguido de Perú.

• El país con el mayor índice de Riqueza Marítima Nacional es Brasil, seguido de México.

• El país con el mayor porcentaje de Riqueza Marítima Nacional sin proteger, es México, esto en función de la relación entre su Poder Naval y la cantidad de Riqueza Marítima del País.

• Los buques más importantes, de acuerdo a su incidencia en el valor total del modelo empleado, fueron los buques tipo fragata, corbeta y patrulla SAAR 4.5 (Aliya), por encima de buques de tipo mayor.

• Las Armadas de Chile, Perú y Brasil son del tipo seis (Armadas de Defensa territorial Marítima), las Armadas de Ecuador, México, Argentina, Venezuela y Colombia son Armadas del tipo ocho

(Armadas de Vigilancia policial) y la Armada de Cuba es del tipo nueve (Armadas simbólicas). El resto de las Armadas de Latinoamérica no tienen recursos para ser analizadas dentro del modelo propuesto.

• Los misiles más empleados en la región son los tipo superficie-superficie Exocet, seguidos por los Harpoon; en tanto en los del tipo superficie-aire fueron los Aspide seguidos por los Sea Wolf.

• En relación a México, se puede concluir que la enorme Riqueza Marítima Nacional que tiene en su territorio, solo por debajo de Brasil, obliga a tener un Poder Naval total mayor, a partir de aprovechar el importante potencial con que cuenta.

• La posición de México se puede resumir de la siguiente manera: es el país con el mayor índice de Capacidades Navales potenciales, con el índice más bajo de Capacidades Navales actuales, se encuentra en el quinto sitio en cuanto a su Poder Naval total, es el segundo lugar en cuanto al índice de Riqueza Marítima Nacional, pero tiene, de acuerdo al modelo utilizado, casi un 40 % de su riqueza marítima desprotegida contra infractores de la ley y más del 90 % de su riqueza marítima desprotegida contra otra fuerza naval en caso de un ataque en estos momentos.

• Como conclusión final se identificó que en la actualidad, para aumentar el Poder Naval de un Estado, no sólo son necesarios los tipos de buques, ni portaaviones, ni submarinos; la clave para una armada pequeña o mediana son los misiles y sus sistemas de armas. Las unidades de superficie constituyen la columna vertebral de una armada, el contar con misiles lo convierte en un multiplicador de fuerza.

A partir del análisis realizado y las conclusiones obtenidas, se pudo observar que los buques que están siendo más preponderantes en el Poder Naval total en Latinoamérica son los de mediano desplazamiento, principalmente del tipo fragatas y corbetas, pero armadas con misiles tanto del tipo superficiesuperficie y del tipo superficie-aire.

La propuesta de solución que se plantea en el presente trabajo de investigación es la continuación de la construcción de los buques patrulla oceánica polivalentes y multipropósito, con la variante de integrar en su armamento sistemas de armas y lanzadores de misiles tanto de superficie-superficie y de superficie-aire, junto a una dotación importante de misiles en cada unidad de superficie; asimismo, iniciar en el Instituto de Investigación y Desarrollo de la Armada de México un programa de construcción de prototipos de misiles como armamento fundamental en las armadas modernas.

Bajo estas dos premisas, basadas primordialmente en el empleo de misiles a bordo de las nuevas patrullas oceánicas, México podrá aumentar significativamente el valor de las Capacidades Navales actuales y por ende, el valor del Poder Naval total de la Armada Nacional.

## Bibliografía


Athieu H. (2012), *Anuario 2012 de la Seguridad Regional en América Latina y el Caribe*, FES Seguridad, Bogotá.

Centro de Estudios Superiores Navales (CESNAV) (2003), *Poder Marítimo Mexicano*, CESNAV, México.

Chant C. (2006), *Barcos de Guerra*, LIBSA, Madrid.

Colom G. (2009), *Entre la revolución y la transformación en los asuntos militares y la configuración de los pilares estratégicos de Estados Unidos para el siglo XXI*, tesis doctoral, Instituto Universitario Gutierrez Mellado, Madrid.

Couteau-Begarie H. (2010), *La potencia marítima*, Ediciones Ejército, Madrid.

Crisher B., Souva M. (15 de septiembre de 2013), *Power at sea: a naval power dataset, 1865– 2011*. Universidad de Florida, Florida, Estados Unidos de América.

Cuervo Vázquez N. (2014), *El Poder Naval en Latinoamérica: Análisis correlacional del Poder Naval de México, Centroamérica y Sudamérica. (Construcción de un instrumento para medir el Poder Naval de un Estado)*, tesis de maestría, Secretaría de Marina, Armada de México, Centro de Estudios Superiores Navales, México, D.F.

de Saint Salvy A. F. (1994), *Concevoir la marine: un art difficile*, "Défense Nationale", Revue mensuelle, Mai 1994, Dossier La marine nationale, Comité d'Études de Défense National, Paris.

Diez O. (2006), *Buques, Submarinos y Portaaviones*, UDYAT, Madrid.

Friedman N. (2006), *The Naval Institute Guide to Word Naval Weapons*, Naval Institute Press, Annapolis.

Fuller M. (2013), *IHS Jane´s Weapons Naval*, Polestar Wheatons, Reino Unido.

Gray S. (2006), *La pujanza del Poder Naval*, Ministerio de Defensa, Madrid.

Gresham J. D. (2005), *SEAPOWER, El dominio del mar*, Océano, México.

Hardy D. (2005), *La proyección del poder militar a través del mar; máxima contribución naval del accionar conjunto*, "REVISMAR", no 6, 2005, pp. 517–528.

Hill J. (1990), *Estrategia marítima para potencias medianas*, Instituto de Publicaciones Navales, Buenos Aires.

International Institute for Strategic Studies (IISS) (2013), *The Military Balance 2013***,** Routledge, London.

Jackson R. (2011), *Barcos de Guerra*, Edimat Libros S.A, Madrid.

Martinez D. (2009), *Poderío marítimo*, Escuela de Guerra Naval, Buenos Aires.

Mey C. (14 de octubre de 2013), *El equilibrio naval durante la época del apostadero. Historia y arqueología naval*, disponible en: Histamar, http://www.histamar.com.ar

Moloeznik M. (2009), *Hacia un marco teórico y analítico del poder naval en México. Contribución doctrinaria al desarrollo de la Armada de México*, Análisis, Guadalajara.

Moloeznik M. (2013), *La Armada de México frente a sus pares de América Latina*, "Revista del CESLA", no 14, 2011, pp. 39–71.

Moloeznik M. (2016), *Derroteros y paradigmas navales en Latinoamérica*, en: *Przeobrażenia geopolityczne i nowe zagrożenia w Ameryce Łacińskiej – Transformaciones geopolíticas y nuevas amenazas en América Latina*, K. Krzywicka, P. Trefler (eds. y coords.), Estudios Iberoamericanos de la UMCS, vol. IV, Editorial de la Universidad Maria Curie-Skłodowska, Lublin.

Ness L. (2013), *Jane´s Weapons Ammunition*, Polestar Wheatons, Reino Unido.

Payne C. M. (2010), *Principles of Naval Weapons Systems*, Naval Institute Press, Annapolis.

RESDAL (2012), *Atlas comparativo de la Defensa en América Latina y el Caribe*, RESDAL, Buenos Aires.

Ricardi C. (2008), *Tesis: Cuantificar intereses marítimos*, Escuela de Guerra Naval, Montevideo.

Saunders S. (14 de octubre de 2013), *Analysis 2013 Global naval developments trends and outlook*, obtenido de IHS Jane´s: http://www.ihs.com.jfs

Saunders S. (2013), *IHS Jane's Fighting Ships 2013–2014*, JANE´S HIS, Virginia.

SIPRI (2010), *SIPRI Yearbook* 2010, SIPRI – UNAM, Estocolmo.

Sheina R. L. (1991), *Iberoamérica. Una Historia Naval 1810–1987*, Editorial San Martín, Madrid.

Till G. (2007), *Poder Marítimo: una guía para el siglo XXI*, Instituto de Publicaciones Navales, Buenos Aires.

U.S. Military, Department of Defense, U.S. Navy, World Spaceflight News (2012), *Ultimate illustrated navy equipment*.

Vego M. (2009), *Estrategia Naval y operaciones en aguas restringidas*, Ministerio de Defensa, Madrid.

Vilanova C. B. (2006), *El hombre y la mar*, Grupo Cultural, Madrid.

Vilanova C. B. (2012), *LHD La máxima proyección estratégica*, Real del Catorce Editores, Madrid.

Wragg D. (2012), *Word Sea Power Guide*, Pen & Sword, Maritime, South Yorkshire.

Revista Escola de Guerra Naval – Janeiro-Abril 2019 – v. 25, n.1



DOI 10.22491/1809-3191. v25n1.p89-128

# O ENCONTRO DA GUERRA CIBERNÉTICA COM AS GUERRAS ELETRÔNICA E CINÉTICA NO ÂMBITO DO PODER MARÍTIMO

Alan Oliveira de Sá [1]
Raphael Carlos Santos Machado [2]
Nival Nunes Almeida [3]

## R E S U M O

A busca por melhores capacidades operacionais e gerenciais no Poder Marítimo tem motivado o aumento do uso de sistemas híbridos, onde componentes cibernéticos interagem com plantas físicas e com sensores/dispositivos que exploram o espectro eletromagnético. Entretanto, ao mesmo tempo em que esta integração traz vantagens, ela também expõe tais sistemas a novas ameaças, resultantes do encontro da guerra cibernética com as guerras eletrônica e cinética. O presente artigo analisa como estas novas ameaças podem afetar o Poder Marítimo, caracterizando, por meio de exemplos, seus possíveis alvos. Para dar suporte a esta discussão, propõese uma taxonomia que abarca novas classes de ataque que exploram os domínios cibernético, eletrônico e cinético. A análise aponta para a necessidade de políticas capazes de promover a segurança dos sistemas cibernéticos do Poder Marítimo. Neste viés, são discutidas políticas de qualificação de pessoal e de homologação e certificação de productos cibernéticos, ambas com o potencial de contribuir de forma abrangente para a segurança do Poder Marítimo.

**Palavras-chave:** Guerra Cibernética; Guerra Eletrônica; Guerra Cinética; Poder Marítimo Doutor. Escola de Guerra Naval (EGN), Rio de Janeiro (RJ), Brasil.

---

[1] Doutor.Professor do Centro de Instrução Almirante Wandenkolk (CIAW), Rio de Janeiro (RJ), Brasil. E-mail: alan.oliveira.sa@gmail.com
*ORCID: http://orcid.org/0000-0001-6311-9672*

[2] Doutor. Professor pela Universidade Federal Fluminense (UFF), Rio de Janeiro (RJ), Brasil. E-mail: rcmachado@inmetro.gov.br

[3] Doutor. Escola de Guerra Naval (EGN), Rio de Janeiro (RJ), Brasil.
E-mail: nivalnunes@yahoo.com.br

## INTRODUÇÃO

A inclusão do domínio cibernético[4] na arte da guerra vem sendo amplamente discutida nas áreas de Ciência e Tecnologia, Defesa, Estratégia e Relações Internacionais. Por sua complexidade e peculiaridades, as ameaças cibernéticas têm feito com que pesquisadores e estrategistas revisitem os princípios da guerra erguidos ao longo do tempo com base nas literaturas de Sun Tzu, Nicolau Maquiavel, Carl von Clausewitz, Antoine-Henri Jomini, Basil Liddell Hart, dentre outros. Tais princípios, originalmente formulados considerando milênios de guerras cinéticas[5], não aderem integralmente à guerra praticada no domínio cibernético.

Segundo a avaliação de Parks e Duggan (PARKS; DUGGAN, 2011), dentre os princípios da guerra cinética (WEIGLEY, 2013; MINISTÉRIO DA DEFESA, 2007; MINISTRY OF DEFENSE, 2014), há aqueles que se aplicam à guerra cibernética, há aqueles que não têm significado na guerra cibernética, e há alguns poucos que, de fato, podem ser considerados antagônicos à guerra cibernética. Todavia, desde os primeiros estrategistas e teóricos da guerra cinética aos pesquisadores atuais da guerra cibernética, observa-se uma característica comum entre os dois tipos de guerra. Ambas devem produzir efeito no mundo real.

Na guerra cibernética esta característica está explícita em um dos oito princípios propostos por Parks e Duggan (PARKS; DUGGAN, 2011): o princípio de Efeitos Cinéticos. Este princípio enuncia que a guerra cibernética deve produzir efeitos no mundo cinético, só tendo sentido quando afeta alguém ou alguma coisa no mundo real. Em outras palavras, podemos dizer que a energia dispendida por guerreiros cibernéticos em combate só resulta em trabalho quando os resultados afetam – direta ou indiretamente – o mundo físico.

Apesar das dificuldades para descobrir e dissecar ataques cibernéticos – por vezes mantidos sob sigilo –, o princípio de Efeitos Cinéticos é frequentemente identificado nos casos estudados. Dentre os ataques mais conhecidos, cujos efeitos produzidos/alegados reforçam a pertinência deste princípio, citamos o ataque associado à explosão no gasoduto transiberiano (REED, 2005; CLARK; KNAKE, 2010), o ataque cibernético que apoiou a Operação Orchard (ADEE, 2008; CLARK; KNAKE, 2010; DIPERT, 2013), e o worm Stuxnet (LANGNER, 2011; ZETTER, 2014) que impactou o programa nuclear iraniano.

Os três casos são exemplos de ataques em que os efeitos no mundo físico conferiram aos atacantes – Estados-Nações segundo (CLARK; KNAKE, 2010; ZETTER, 2014) – vantagens táticas ou estratégicas, seja impondo danos físicos diretos ao inimigo ou manipulando informações táticas referentes ao Teatro de Operações. Estes exemplos reforçam a necessidade de compreender as formas de manifestação do principio dos Efeitos Cinéticos para, a partir de então, estabelecer contramedidas – sejam elas políticas ou técnicas. Isto tem motivado estudos sobre a segurança cibernética nos mais diversos setores, principalmente naqueles classificados como infraestrutura crítica[6] o que, inevitavelmente, abarca o Poder Marítimo[7] . De

[4] O conceito de domínio cibernético adotado neste artigo agrega a definição de mundo cibernético apresentada por Parks e Duggan (PARKS; DUGGAN, 2011). Segundo aqueles autores, um mundo cibernético é "qualquer realidade virtual contida em um conjunto de computadores e redes". Note que esta definição admite a existência de diversos mundos cibernéticos, onde a Internet seria o mais relevante. Sendo assim, o termo domínio cibernético é usado neste artigo para representar o conjunto de todos os mundos cibernéticos existentes.

[5] Na definição apresentada por Parks e Duggan (PARKS; DUGGAN, 2011), também adotada neste artigo, o termo guerra cinética refere-se à guerra praticada em terra, mar, ar e espaço. É a guerra protagonizada por tanques, navios, aeronaves, soldados etc.

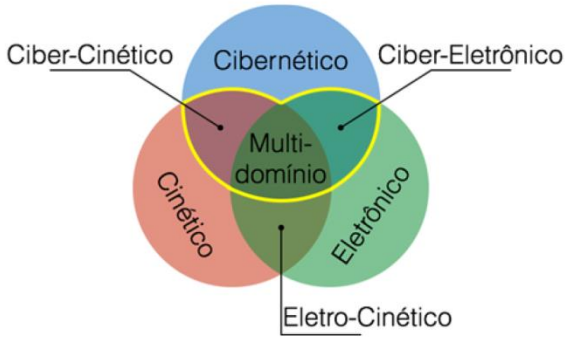
[6] De acordo com (MANDARINO JUNIOR, 2010) entende-se por infraestruturas críticas (IEC) "as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade." Dentre as infraestruturas críticas de um país podemos citar, por exemplo: Energia, Defesa, Transporte, Telecomunicações, Finanças, dentre outras. (WHITE HOUSE, 2003; MANDARINO JUNIOR, 2010)

[7] Adotamos neste estudo o conceito de Poder Marítimo definido na Doutrina Básica da Marinha (MARINHA DO BRASIL, 2014): "*O Poder Marítimo é a capacidade resultante da integração dos recursos de que dispõe a Nação para a utilização do mar e das águas interiores, quer como instrumento de ação política e militar, quer como fator de desenvolvimento econômico e social". Segundo a referida doutrina, o poder marítimo é formado pelos seguintes elementos: "o Poder Naval; a Marinha Mercante, as facilidades, os serviços e as organizações relacionados com os transportes aquaviários (marítimo e fluvial); a infraestrutura hidroviária: portos, terminais, eclusas, meios e instalaçõ es de apoio e de controle; a indústria naval: estaleiros de construçã o e de reparos; a industria bélica de interesse do aprestamento naval; a indústria de pesca: embarcaçõ es, terminais e indústrias de processamento de pescado; as organizações e os meios de pesquisa e de desenvolvimento tecnológico de interesse para o uso do mar, das águas interiores e de seus recursos; as organizações e os meios de exploração ou de aproveitamento dos recursos do mar, de seu leito e de seu subsolo; e o pessoal que desempenha atividades relacionadas com o mar ou com as águas interiores e os estabelecimentos destinados à sua formaçã o e ao seu treinamento".*

fato, dependendo das circunstâncias, um incidente – cibernético ou não – em um sistema naval (civil ou militar) pode trazer impactos aos setores de transporte, energia, defesa, alimentos etc. comprováveis prejuízos econômicos, ambientais e à segurança.

Neste contexto, o presente artigo discute algumas formas pelas quais ataques com componentes cibernéticas podem alcançar o princípio dos Efeitos Cinéticos, afetando, por exemplo, um combate naval, a navegação, ou mesmo a exploração/uso do mar e de águas interiores. Mais especificamente, discute-se como o princípio dos Efeitos Cinéticos pode ser alcançado quando a guerra cibernética encontra outros dois tipos de guerra comumente praticados no ambiente naval – a guerra eletrônica e a guerra cinética. A análise considera, portanto, três domínios de atuação para os ataques ora estudados: domínio cibernético; o domínio eletrônico; e o domínio cinético. Mais estritamente, o foco deste trabalho está nos subconjuntos de ataques contidos nas interseções destacadas no diagrama da **Figura 1**.

Figura 1 - Classificação dos ataques quanto aos seus domínios de influência/ impacto.




O restante deste artigo está organizado da seguinte forma. Primeiramente, são descritos alguns ataques cibernéticos relevantes já ocorridos, bem como as suas formas de impacto no mundo real. Em seguida, é apresentada uma taxonomia que abrange ataques que exploram os domínios cibernético, eletrônico e cinético. Esta taxonomia visa apoiar a discussão sobre possíveis ataques envolvendo estes três domínios. Posteriormente, o trabalho discute as classes de ataques ciber-cinéticos, ciber-eletrônicos e multidomínio, caracterizando, por meio de exemplos, seus possíveis alvos no Poder Marítimo. Em seguida, são discutidas políticas com o potencial de mitigar os referidos ataques. Por fim, são apresentadas as conclusões.

## ATOS DE GUERRA CIBERNÉTICA

Até o presente, a humanidade não experimentou a guerra cibernética de forma tão ampla quanto o fez com a guerra cinética. Se, por um lado, os conhecimentos sobre a guerra cinética foram construídos com base em observações e registros feitos ao longo de milhares de anos, por outro, os conceitos sobre a guerra cibernética se baseiam em experiências adquiridas ao longo de algumas décadas. Ainda assim, os ataques cibernéticos já ocorridos representam uma valiosa fonte de informações para o estudo da guerra cibernética e suas vertentes. Esta seção, portanto, apresenta exemplos de ataques de guerra cibernética com diferentes propósitos e formas de emprego. Embora os ataques aqui descritos não tenham sido praticados em áreas navais – i.e. contra belonaves, embarcações civis ou infraestruturas existentes nas margens, sob ou sobre a superfície da água –, os mesmos servem, de forma geral, como referência ou prova de conceito para possíveis ataques que possam vir a causar incidentes em jurisdições navais.

## ATAQUE À ESTÔNIA

Em 2007, a Estônia foi alvo de uma série de ataques cibernéticos que afetaram de forma significativa serviços essenciais do país. Para compreender a motivação destes ataques é necessário retornar ao final da Segunda Guerra Mundial. Com a Grande Guerra Patriótica[8] o Exército Vermelho tirou a Estônia do domínio nazista, forçando-a se integrar à União das Repúblicas Socialistas Soviéticas (URSS). Após o período de domínio Soviético, com a desintegração da URSS, a Estónia se tornou independente e estabeleceu novamente sua capital em Tallin. Durante seu domínio, para que os povos do leste Europeu se lembrassem dos sacrificios feitos para libertá-los dos nazistas, a URSS ergueu em muitas capitais da região grandes estátuas de um heroico soldado do Exército Vermelho. E assim também o fez em Tallin.

Tais estátuas eram vistas com muito apreço pelos líderes soviéticos. No entanto, aos olhos dos estonianos, a estátua erguida em Tallin representava um símbolo das cinco décadas de opressão que eles foram obrigados a passar como parte da URSS (CLARK; KNAKE, 2010).

Assim, em 2007, atendendo aos sentimentos da população, o legislativo da Estônia aprovou a Lei

[8] Termo usado pelos russos para se referir à Segunda Guerra Mundial.

das Estruturas Proibidas que determinava a remoção da estátua do soldado do Exército Vermelho, o que desagradou Moscou. Para evitar um incidente, o então presidente da Estônia vetou a lei. Nesse contexto, as pressões em torno da preservação, ou não, do símbolo soviético aumentaram.

De um lado, a opinião pública estoniana defendia a remoção da estátua e um grupo nacionalista a tentava destruir. De outro, grupos étnicos russos dedicados a protegê-la se tornavam cada vez mais ativos.

Este conflito culminou em uma revolta, conhecida como a Noite de Bronze (KAISER, 2015), que se seguiu da remoção da estátua para um cemitério militar. Foi quando o conflito migrou para o ciberespaço. A Estônia foi atingida por um ataque DDoS[9] de grande escala – até então o maior registrado. O ataque, lançado por diversas botnets[10] , durou semanas e derrubou serviços eletrônicos do governo, bancos, sites de jornais e servidores da rede de telefonia. Devido ao grande impacto, o País Báltico levou o caso ao Conselho do Atlântico Norte, da OTAN. A Estônia alegou que os computadores que controlavam as botnets estavam na Rússia que, por sua vez, negou estar envolvida nos ataques cibernéticos (CLARK; KNAKE, 2010).

## GUERRA RUSSO-GEORGIANA

Outro ataque cibernético conhecido – também envolvendo uma antiga república soviética – ocorreu em 2008 na Geórgia (SHAKARIAN, 2011), durante a chamada Guerra Russo-Georgiana. Na época, a Ossétia do Sul era reconhecida internacionalmente como território da Geórgia, no entanto se considerava independente e recebia proteção, financiamento e vivia sob influência russa (CLARK; KNAKE, 2010). Naquele ano, rebeldes da Ossétia do Sul organizaram uma série de ataques com mísseis contra aldeias da Geórgia. Em resposta, a Geórgia bombardeou a capital da Ossétia do Sul e invadiu a região. No dia seguinte à invasão georgiana, veio a resposta do exército russo expulsando os militares georgianos da Ossétia do Sul. Ocorre que a ofensiva física não foi a única deflagrada contra a Geórgia.

Antes que os ataques cinéticos começassem, ataques cibernéticos já atingiam sites do governo georgiano. Ao longo do conflito, a Geórgia sofreu ataques DDoS direcionados aos seus meios de comunicação, com o objetivo de dificultar que os georgianos percebessem o que estaba acontecendo. Os sistemas bancários, de cartões de crédito e de telefonía móvel foram afetados. A maioria dos roteadores que conectavam a Geórgia à Internet, via Turquia e Rússia, foram atacados. A Geórgia perdeu o acesso às fontes de informação e notícia externas. No auge da ofensiva, seis botnets foram mobilizadas para gerar o tráfego de ataque (CLARK; KNAKE, 2010). Embora alguns especialistas considerem que a coordenação entre os ataques cibernéticos e cinéticos tenha sido baixa (SHAKARIAN, 2011), e os russos alegarem que os ataques cibernéticos estavam fora do comando do Kremlin (CLARK; KNAKE, 2010), alguns eventos identificados sugerem ter havido tal coordenação. As instalações físicas da mídia e de sistemas de comunicação, por exemplo, não sofreram ataques cinéticos, apenas cibernéticos. Além disso, hackers russos atacaram um site usado para aluguel de geradores elétricos a diesel, provavelmente em complemento aos ataques convencionais que atingiram a infraestrutura elétrica do país (SHAKARIAN, 2011). É digno de nota que, segundo (SHAKARIAN, 2011), os objetivos de isolar e desgastar a Geórgia foram limitados em seu escopo, tendo os atacantes evitado causar danos permanentes às redes georgianas e aos seus sistemas SCADA[11] .

## STUXNET

O ataque a sistemas SCADA, com consequências cinéticas diretas no mundo real, é verificado em um contexto diferente da Guerra Russo-Georgiana, com o emprego da – possivelmente – mais emblemática arma cibernética já usada: o malware Stuxnet. Seu propósito estratégico não foi a negação de serviços de internet, mas sim a

[9] No contexto dos serviços de internet, um ataque de negação de serviço, ou Denial of Service (DoS), é um tipo de ataque em que o serviço executado por um determinado servidor é interrompido devido à quantidade de requisições maior do que a sua capacidade de processamento e resposta. Um ataque distribuído de negação de serviços, ou Distributed Denial of Service (DDoS), por sua vez, é um ataque DoS em que um grande conjunto de equipamentos – composto por até milhares de máquinas – é usado para gerar o tráfego responsável por sobrecarregar o servidor e negar o seu serviço. Os equipamentos atacantes, denominados zumbis, podem ser computadores, servidores, equipamentos de rede ou mesmo dispositivos de Internet das Coisas, ou Internet of Things (IoT).

[10] Rede de dispositivos zumbis, ou bots, controlados remotamente por um computadormestre que, por sua vez comanda os ataques DDoS.

[11] Os sistemas de Supervisão e Aquisição de Dados, ou Supervisory Control and Data Acquisition (SCADA), são sistemas usados para controlar, monitorar e fazer a aquisição de dados de sistemas físicos automatizados. Os sistemas físicos controlados vão desde plantas industriais até infraestruturas críticas.

negação de armas nucleares ao Irã de forma furtiva e sem o emprego de armas físicas. Mais especificamente, seu alvo eram as centrífugas de enriquecimento de urânio que operavam na usina de Natanz. Estas centrífugas, que funcionavam em um sistema de cascatas, eram controladas e operadas através de um sistema SCADA composto por controladores Siemens STEP 7.

Utilizando a analogia feita em (ZETTER, 2014), podemos descrever o Stuxnet como um míssil digital usado para transportar dois tipos de ogiva. A porção "míssil" se encarregava de transportar as ogivas digitais até os Controladores Lógicos Programáveis (CLP) que controlavam as centrífugas. Em outras palavras, a parte "míssil", era responsável por fazer com que o malware – mais especificamente um worm – se propagasse e replicasse até encontrar um sistema que tivesse a assinatura do sistema a ser atacado. Uma vez encontrando o sistema alvo – CPLs Siemens conectados às centrífugas –, o worm liberava as ogivas digitais que se instalavam nos CLPs e iniciavam ações sutis de degradação e destruição das centrífugas.

Uma das ogivas digitais continha um código que alterava a velocidade de rotação das centrífugas de forma reduzir a eficiência do processo de enriquecimento, causando também vibrações destrutivas. A outra ogiva atuava na abertura e fechamento das válvulas que interconectavam as centrífugas em cascata, causando aumento de pressão interna e avaria das centrífugas. Cabe ressaltar que o sistema de controle das centrífugas do Irã não estava diretamente conectado à Internet, de forma que, para alcançar a rede de controle, o malware precisava vencer o air gap[12] existente entre as duas redes. Sendo assim, dentre outras formas de difusão, o Stuxnet se propagava através de mídias removíveis (pen drives) e instalava seu código malicioso nos CLPs através das máquinas que eram utilizadas para programá-los.

Após a descoberta do Stuxnet, pesquisas demonstraram que, além de complexo, o mesmo dispunha de uma quantidade de recursos nunca antes vistos juntos em uma arma digital. Em sua parte "míssil", o malware reunia ao todo oito formas de propagação (ZETTER, 2014), das quais quatro eram zero-day exlpoits[13] (FALLIERE, 2011), o que demonstra o grau de comprometimento e investimento aplicado no projeto.

O Stuxnet foi encontrado em 2010 e investigado por diversos especialistas ao redor do mundo (ZETTER, 2014), tanto da área de sistemas de controle industriais (LANGNER, 2011), quanto da área de segurança da informação (FALLIERE, 2011). As evidências e investigações apontam para a autoria conjunta de EUA e Israel (ZETTER, 2014). O Stuxnet é considerado uma prova de conceito de como as armas digitais podem afetar diretamente o mundo físico, sendo capazes de cumprir os mesmos propósitos estratégicos de ataques com armas cinéticas como mísseis e bombas.

## ATAQUE AO GASODUTO TRANSIBERIANO

Embora o Stuxnet seja considerado um marco nos ataques a sistemas ciberfísicos, a literatura (WEISS, 1996; CLARK; KNAKE, 2010; MILLER, 2012) indica a existência de outra bomba lógica de impacto físico anterior ao referido worm. A arma teria sido usada para causar destruição em uma tubulação de transporte de gás situada na Sibéria, no início da década de 1980 (CLARK; KNAKE, 2010) – ou seja, antes mesmo de a Internet estar difundida como nos dias do Stuxnet. À época, sem a grande conectividade da rede mundial de computadores, os atacantes – i.e. a CIA com o apoio de Canadenses, segundo (CLARK; KNAKE, 2010) – utilizaram outra estratégia para fazer o código malicioso chegar ao sistema de controle do gasoduto. Para tal, implantaram o código malicioso diretamente no controlador, antes mesmo de o equipamento ser obtido pela Rússia e instalado em seu sistema de automação de dutos (CLARK; KNAKE, 2010).

O controlador seria utilizado para comandar a abertura e o fechamento de válvulas, bem como para controlar o acionamento de bombas que faziam fluir gás na tubulação. Sendo assim, segundo (CLARK; KNAKE, 2010), o código malicioso foi programado para comandar o fechamento da válvula de um segmento do gasoduto, ao mesmo tempo em que a bomba era acionada em capacidade máxima para injetar gás dentro da tubulação. Este acionamento indevido dos atuadores do sistema – i.e. a bomba e a válvula – resultou no aumento da pressão interna

[12] Air gap é o termo utilizado para se referir à medida de segurança de redes onde a rede a ser protegida é fisicamente isolada das redes inseguras – como a Internet, por exemplo –, não havendo conectividade entre as mesmas.

[13] Zero-day exploits são ferramentas que exploram vulnerabilidades do tipo zero-day – i.e. vulnerabilidades desconhecidas por quem estaria interessado em mitiga-las.rmo usado pelos russos para se referir à Segunda Guerra Mundial. Vulnerabilidades zero-day são raras e seus exploits, quando comercializadas no mercado cinza ou negro (ZETTER, 2014) de armas digitais, são caros.

do duto, causado, por sua vez, a maior explosão não nuclear até então registrada, acima de três quilotons (CLARK; KNAKE, 2010; MILLER, 2012).

## OPERAÇÃO ORCHARD

Um novo tipo de ataque veio à discussão com a Operação Orchard, lançada em 2007 pelo Estado de Israel contra a Síria. Na madrugada de 06 de setembro de 2007, aeronaves da Força Aérea Israelense entraram no espaço aéreo sírio e bombardearam uma instalação industrial que estaba sendo construída no território daquele país. Tal instalação era uma planta nuclear que, segundo (CLARK; KNAKE, 2010), a Síria estava construindo com o apoio da Coréia do Norte. Na ocasião, além da repercussão do próprio bombardeio e das discussões em torno do propósito da planta atacada, chamou a atenção internacional o fato de a Síria, que já havia investido bilhões de dólares em sistemas de defesa aérea (CLARK; KNAKE, 2010), não ter reagido ao ataque. Naquela noite, a Síria estava em alerta, uma vez que Israel, na manhã anterior, havia posicionado suas tropas nas colinas de Golã. Os militares sírios observavam atentamente seus radares. No entanto, no momento em que as aeronaves F-15 Eagles e F-16 Falcons de Israel invadiram o espaço aéreo sírio, nada de incomum apareceu nas telas dos radares do sistema de vigilância.

Na busca por explicações plausíveis para a falha do sistema de vigilância sírio, alguns analistas sugerem que aquele país tenha sido vítima de um ataque de guerra eletrônica. No entanto, este ataque se diferenciava das demais Medidas de Ataque Eletrônico[14] (MAE) conhecidas, por explorar uma vulnerabilidade implantada no domínio cibernético do sistema de vigilância sírio (ADEE, 2008; CLARK; KNAKE, 2010).

Radares, como sensores, são interfaces abertas para o ambiente. Para captar informações sobre possíveis alvos, um radar transmite pulsos através de sua antena e capturam, de uma forma geral, todo e qualquer eco que chegue de volta ao seu receptor. Os ecos recebidos, por sua vez, são digitalizados, armazenados em uma memória e processados por um sistema computacional que apresenta ao operador informações relevantes sobre os alvos detectados como, por exemplo, posições e velocidades (BOLE, 2005). Dessa forma, é possível afirmar que um transmissor, apto a transmitir pulsos no mesmo padrão dos transmitidos pelo radar, seja capaz de fazer com que ecos falsos – sinteticamente produzidos – cheguem à antena do radar (ABDALLA et al., NENG-JING; YI-TING, 1995). Estes ecos falsos, uma vez digitalizados, passam a ser representados na forma de bits na memória do radar (BOLE; DINEY; WALL, 2005). Isto significa dizer que é possível manipular os bits da memória de dados de um radar através de MAE conhecidas – o que não representa grande novidade em face do estado da arte da guerra eletrônica (ABDALLA et al.; 2015). No entanto, neste ataque, é possível que houvesse no sistema de vigilancia um gatilho digital – i.e. uma vulnerabilidade implantada em software e/ou hardware – observando constantemente as informações captadas e salvas na memória do radar, em busca de informações com um padrão específico que acionasse tal gatilho digital (ADEE, 2008; CLARK; KNAKE, 2010). Este gatilho digital, por sua vez, iniciaria rotinas maliciosas no sistema computacional dos radares. Basicamente seriam duas rotinas maliciosas: uma rotina de gravação e outra de reprodução de cenários.

As informações, ou bits, com tal padrão específico de acionamento seriam introduzidas na memória pela MAE, através da antena do próprio radar.

Uma vez identificado o padrão de acionamento da rotina de gravação, o gatilho digital dava início a gravação de um cenário a priori normal – i.e. sem alvos que representassem ameaças. Posteriormente, ao identificar o padrão de acionamento da rotina de reprodução, o gatilho digital passava a reproduzir para os operadores o cenário de operação normal, previamente gravado durante a rotina de gravação. Desta forma, estima-se que uma MAE em conjunto com um gatilho digital no sistema computacional do radar tenha sido capaz de negar aos operadores sírios a detecção de aeronaves inimigas durante a execução do bombardeio (CLARK; KNAKE, 2010).

## SÍNTESE DOS ATAQUES

As ações de guerra cibernética apresentadas nesta seção não esgotam os ataques cibernéticos já ocorridos. No entanto, demonstram a

[14] De acordo com (MARINHA DO BRASIL, 2014), as Medidas de Ataque Eletrônico (MAE) correspondem a um "conjunto de ações tomadas para evitar ou reduzir o uso efetivo, por parte do inimigo, do espectro eletromagnético e, também, degradar, neutralizar ou destruir sua capacidade de combate por meio de equipamentos e armamentos que utilizem este espectro". As MAE têm natureza fundamentalmente tática e representam um dos três ramos das Medidas de Guerra Eletrônica (MGE) – que também englobam as Medidas de Proteção Eletrônica (MPE) e as Medidas de Apoio à Guerra Eletrônica (MAGE) (MARINHA DO BRASIL, 2014).

diversidade dos ataques, bem como as formas em que os mesmos foram eficazmente usados como ferramenta para causar danos físicos ou econômicos a nações adversárias, ou mesmo para apoiar a execução de ataques cinéticos em operações militares. No caso do ataque à Estônia, notamos que os ataques executados foram exclusivamente cibernéticos, causando impacto no mundo real por meio da negação de serviços essenciais para a economia e sociedade estonianas. Na guerra Russo-Georgiana, os ataques cibernéticos foram empregados para apoiar ataques de forças convencionais (SHAKARIAN, 2011), com algum grau de coordenação entre eles. Nos exemplos do Stuxnet e do ataque ao gasoduto transiberiano, as armas digitais foram empregadas para causar danos físicos diretos ao inimigo, sem a necessidade do uso de forças convencionais. Já na operação Orchard um ataque envolvendo ações de guerra cibernética e eletrônica foi usado para apoiar, de forma coordenada, a execução de ataques usando forças convencionais. É possível, portanto, perceber nestes exemplos três tipos de ataque:

- ataques cibernéticos com o objetivo de afetar sistemas de informação e de comunicação, porém sem o propósito de afetar diretamente sistemas físicos (ataques à Estônia e da Guerra Russo-Georgiana);
- ataques cibernéticos com o propósito de afetar diretamente sistemas físicos (Stuxnet e o ataque ao gasoduto transiberiano); e
- ataques cibernéticos envolvendo MAE visando prejudicar a obtenção de informações táticas, mas sem o propósito de manipular diretamente sistemas físicos (ataque na Operação Orchard).

Uma análise mais profunda destas ofensivas sugere a possibilidade de serem desenvolvidos ataques cibernéticos envolvendo MAE, capazes de afetar diretamente sistemas físicos. Em sistemas navais, mais especificamente, esta possibilidade decorre da crescente integração entre sistemas computacionais, plantas físicas, sistemas de comunicação e sensores que fazem uso do espectro eletromagnético (BOYES; ISBELL, 2017; LAGOUVARDOU, 2018; BHATTI; HUMPHREYS, 2017). Deste modo, o foco da discussão deste trabalho se concentra em ações ofensivas que transitam entre os domínios cibernético, eletrônico e cinético, com possíveis impactos no ambiente naval.

## TAXONOMIA

A adição de tecnologias às ferramentas e técnicas de combate por muitas vezes provocou, ao longo do tempo, a revisão da taxonomia militar.

Tais revisões taxonômicas visam apoiar a discussão e o estudo da guerra, bem como estabelecer conceitos que promovam o desenvolvimento de capacidades de defesa. Neste viés, esta seção apresenta uma taxonomía que reúne terminologias existentes na literatura e estabelece novos termos e conceitos atinentes a ataques que explorem os domínios cibernético, eletrônico e cinético. Primeiramente, é necessário observar as definições das guerras cibernética, eletrônica e cinética:

• Guerra cibernética, segundo Parks e Duggan (PARKS; DUGGAN, 2011), é uma combinação de ataques, defesas e operações técnicas especiais em redes de computadores. O ambiente em que tais ações ocorrem é referido como mundo cibernético, cujo conceito, segundo Parks e Duggan, corresponde a:

> *"... qualquer realidade virtual contida em um conjunto de computadores e redes."* (PARKS; DUGGAN, 2011, p. 1, tradução nossa)

Note que esta definição admite a existência de diversos mundos cibernéticos, uma vez que diferentes realidades virtuais, contidas em diferentes conjuntos de computadores e redes, não interconectadas, podem coexistir. Ainda segundo Parks e Duggan (PARKS; DUGGAN,2011), dentre os diversos mundos cibernéticos existentes, a Internet seriao mais relevante.

O conceito de domínio cibernético adotado no presente artigo agrega a definição de mundo cibernético apresentada por Parks e Duggan (PARKS; DUGGAN, 2011). Neste contexto, o domínio cibernético corresponde ao ambiente composto por todos os mundos cibernéticos existentes.

• Guerra eletrônica, segundo (SHELTON, 1998), corresponde a:

> "... qualquer ação militar envolvendo o uso de energía eletromagnética, dirigida para controlar o espectro eletromagnético ou atacar o inimigo."(SHELTON, 1998, p.II-5, tradução nossa)

Em consonância com esta definição, a Política de

Guerra Eletrônica de Defesa (MINISTÉRIO DA DEFESA, 2004) estabelece que as atividades de guerra eletrônica nas Forças Armadas visam, de uma forma geral, assegurar o uso do espectro eletromagnético e impedir, reduzir ou prevenir seu uso contra os interesses do país. O domínio da guerra eletrônica, portanto, reside no espectro eletromagnético, mais especificamente nas faixas de frequência em que operam sensores – e.g. sistemas radar –, equipamentos de guerra eletrônica e sistemas de comunicação por ondas eletromagnéticas.

• Guerra cinética, de acordo com (PARKS; DUGGAN, 2011), é definida como:

> *"...a guerra praticada em terra, mar, ar e espaço. Todos os tanques, navios, aviões e soldados tradicionais são os protagonistas da guerra cinética."* (PARKS; DUGGAN, 2011, p.1, tradução nossa)

Note que, a definição de guerra cinética apresentada por (PARKS; DUGGAN, 2011) não permite uma caracterização clara do domínio deste tipo de guerra, visto que ações de guerra cibernética e eletrônica também podem ser praticadas em terra, mar, ar e espaço. Por este motivo, para caracterizar o domínio da guerra cinética, recorremos ao significado de cinética. Considerando que a cinética é a parte da física que estuda as mudanças de movimento produzidas pela força, podemos estabelecer que o domínio da guerra cinética reside no mundo real – i.e. não virtual – sujeito a mudanças mediante a aplicação de forças.

Os exemplos de ofensivas digitais discutidas previamente neste artigo demonstram a existência de ataques cibernéticos híbridos que, para produzir o efeito cinético desejado, exploram também os domínios eletrônico e cinético. No diagrama da Figura 1 destacamos três classes de ataques híbridos, que podem derivar da exploração conjunta do dominio cibernético com os domínios eletrônico e/ou cinético:

• Ciber-Cinéticos: a classe de ataques ciber-cinéticos engloba ofensivas originadas no domínio cibernético, com o objetivo decausar impactos diretos no domínio cinético. Seus alvos são sistemas onde computadores e redes de comunicação são utilizados para acionar ou controlar processos físicos. Em outras palavras, neste tipo de ofensiva, medidas de ataque digitais são empregadas para produzir forças físicas capazes de modificar diretamente o mundo real.

• Ciber-Eletrônicos: ataques ciber-eletrônicos são ataques compostos em parte por ações de guerra eletrônica contendo também elementos de guerra cibernética. De acordo com (YASAR, 2012), pode-se dizer que o conceito de ataque ciber-eletrônico corresponde a uma nova e aprimorada forma de ataque eletrônico. Em uma guerra eletrônica tradicional, uma MAE – e.g. uma ação de jamming – pode ser usada, por exemplo, para negar o uso do espectro eletromagnético ao radar inimigo. Por outro lado, em um ataque ciber-eletrônico, o uso do espectro eletromagnético não é essencialmente negado ao sistema alvo. Neste caso, o espectro eletromagnético é utilizado pelo atacante para enviar um fluxo de dados ao processador do sistema alvo de forma a manipular seu processo computacional, comprometendo assim o seu funcionamento.

Para tal, um ataque ciber-eletrônico explora, como porta de entrada, os mesmos dispositivos de captação de ondas eletromagnéticas que o sistema alvo usa para cumprir sua função tática/operacional.

• Multidomínio: os ataques multidomínio correspondem a ofensivas que permeiam os três domínios: cibernético, eletrônico e cinético.

Têm como alvo sistemas que de alguma forma interconectam plantas físicas, sistemas computacionais de automação e controle, e dispositivos/ sensores que exploram o espectro eletromagnético. Nestes sistemas, computadores e redes são utilizados para acionar ou controlar procesos físicos, possuindo também interligação – e, eventualmente, interação – com sistemas que operam no domínio da guerra eletrônica. Conceitualmente, estes ataques se iniciam no espectro eletromagnético e utilizam como porta de entrada os dispositivos de captação de ondas eletromagnéticas – e.g. a antena de um radar. Têm como objetivo manipular ou causar danos físicos diretos à planta física. Para tal, utilizam uma componente cibernética como pivô entre os domínios das guerras eletrônica e cinética. Esta componente cibernética, mecanismo digital implantado em software e/ou hardware, se encarrega de transformar informações recebidas a partir do espectro eletromagnético em ações cinéticas maliciosas na planta controlada. Na Figura 1, podemos verificar ainda um quarto subconjunto de ataques que, por definição, agem simultaneamente – e exclusivamente – nos domínios eletrônico e cinético. Estes ataques,

que não agem no domínio cibernético, não estão no enfoque deste trabalho (que se concentra no encontro da guerra cibernética com as guerras eletrônica e cinética). Porém, por uma questão de completude da presente taxonomia, os definimos como ataques eletro-cinéticos.

A título de exemplo, podemos enquadrar nesta classe de ataques eventuais ofensivas eletromagnéticas lançadas contra espoletas de proximidade utilizadas na Segunda Guerra Mundial (BONNER, 1947; BROWN, 1993). Estas espoletas de proximidade, embutidas em projéteis, eram basicamente constituídas por um transmissor de ondas eletromagnéticas e um receptor conectado diretamente a uma cadeia de explosivos (BONNER, 1947; BROWN, 1993). Para deflagrar a cadeia de explosivos, bastava que o receptor do projétil captasse as ondas eletromagnéticas refletidas pelo alvo, as quais deveriam atender a um determinado padrão de amplitude e frequência Doppler. O processo de detonação não passava pelo domínio cibernético. Com base na arquitetura de espoleta apresentada em (BONNER, 1947; BROWN, 1993), é possível dizer que o lançamento de interferências eletromagnéticas específicas contra este tipo de espoleta seria capaz de eventualmente induzir a detonação do projétil, causando efeitos diretos no domínio cinético. Note que um ataque deste tipo contra as referidas espoletas age, conjuntamente, nos domínios eletrônico e cinético sem fazer uso, em nenhum momento, do domínio cibernético. Por este motivo, o classificamos como um ataque eletro-cinético.

Cabe ressaltar que, na taxonomia ora proposta, as classes de ataques ciber-cinéticos, ciber-eletrônicos e multidomínio visam apenas especificar os domínios que são explorados durante a execução de uma dada ofensiva.

Entretanto, as nomenclaturas adotadas e os exemplos discutidos neste artigo não restringem todos os possíveis caminhos que um ataque pode percorrer ao transitar entre os domínios de sua respectiva classe.

## DISCUSSÃO

Uma vez estabelecida uma taxonomia abrangendo ataques cibercinéticos, ciber-eletrônicos e multidomínio, apresentamos nesta seção uma discussão quanto ao emprego destas classes de ataque contra albos pertencentes ao Poder Marítimo. Primeiramente, discutimos de forma sucinta os ataques ciber-cinéticos, ciber-eletrônicos e multidomínio, e caracterizamos alguns de seus possíveis alvos. Em seguida, discutimospolíticas que podem contribuir de forma ampla para a mitigação destes tipos de ameaça.

Pelos exemplos de ataque já reportados neste artigo, é possível observar que seus alvos não são exclusivamente militares. Enquanto o ataque ciber-eletrônico da Operação Orchard tinha como alvo um sistema militar de vigilância aérea, os ataques à Estônia e à Geórgia tinham – em grande parte – alvos civis, assim como o ataque ciber-cinético ao gasoduto transiberiano. Sendo assim, na presente discussão, é necessário considerar tanto alvos civis quanto militares. Ainda que por vezes existam diferenças notórias entre estes dois tipos de alvo, é comum que os mesmos compartilhem das mesmas tecnologias – muitas vezes duais. Além disso, um ataque a qualquer um dos dois tipos de alvo pode trazer impactos significativos ao Poder Naval, ao Poder Marítimo e à nação.

## ATAQUES CIBER-CINÉTICOS

De acordo com a taxonomia apresentada, um ataque cibercinético busca causar impactos diretos em uma planta física, por meio de manipulações digitais no domínio cibernético. Neste tipo de ataque, o alvo é composto tipicamente por plantas físicas, sistemas computacionais, sensores, atuadores e sistemas de comunicação (DE SÁ; CARMO; MACHADO, 2017; LANGNER, 2011). Os sensores têm o papel de medir o comportamento físico da planta, ao passo que os atuadores cumprem a função transformar sinais de controle em ações físicas capazes de alterar o estado da mesma. Os sinais de controle são calculados por computadores convencionais, microcontroladores, ou computadores projetados especificamente para o controle de processos físicos, como os Controladores Programáveis (CP) ou Controladores Lógicos Programáveis (CLP[15]). Sendo os dois últimos (i.e. CPs e CLPs)

[15] CLPs e CPs são sistemas computacionais projetados especificamente para executar o controle/automação de plantas físicas. Em geral, são dispositivos de prateleira, genéricos, que podem ser utilizados para o controle de diversos tipos de sistemas bastando, para tal, programá-lo em função das características da planta. São compostos por microprocessadores, memórias, interfaces de programação/comunicação, e interfaces de entrada e saída de sinais. As interfaces de entrada de sinais são utilizadas para receber sinais medidos por sensores na planta. As interfaces de saída de sinais transmitem os sinais de controle para os atuadores da planta.

empregados em grande parte dos sistemas de automação e controle de plantas físicas.

De forma ampla, podemos dizer que o conjunto de potenciais alvos para um ataque ciber-cinético compreende dispositivos de Internet das Coisas (ou Internet of Things – IoT) (GUBBI et al., 2013), sistemas da Indústria 4.0 (LEE; BAGHERI; KAO, 2015; LASI et al., 2014) e outros sistemas de controle e automação de plantas não necessariamente industriais. De forma mais estrita, no que tange ao Poder Marítimo, os alvos podem ser, por exemplo:

- Sistemas de automação e controle de navios o que inclui, por exemplo, sistemas de propulsão (HART, 2004) e sistemas de geração de energia (ZIVI, 2005) tanto em meios da marinha mercante quanto do Poder Naval. No caso de ataques a sistemas geradores de energia, citamos como prova de conceito o experimento de ataque Aurora realizado pelo Idaho National Laboratory, subordinado ao Department of Homeland Security dos EUA. No experimento, os atacantes causam a destruição de um gerador de energia a diesel de 2,25MW por meio de 20 linhas de código de um virus (AYALA, 2016);
- Sistemas de combate navais, onde sensores e armas são conectados a computadores e redes – ainda que locais –, conforme os exemplos discutidos em (NORCUTT, 2001; JANER; PROUM; 2014);
- Diques flutuantes cujo controle de estabilidade e flutuabilidade é feito via sistemas SCADA (TOPALOV; KOZLOV; KONDRATENKO, 2016);
- Sistemas offshore de exploração, produção e transporte de óleo e gás (WADHAWAN; NEUMAN, 2015; ERICKSON et al., 2003), frequentemente controlados por sistemas SCADA;
- Sistema de automação de canais e controle de eclusas (AMIN et al., 2010; AMIN et al. 2013; SMITH, 2015);
- Usinas de geração de energia elétrica a partir de fonte maremotriz, controladas por CLPs e sistemas SCADA (KUMAR; MAJUMDAR; BABU, 2012);
- Parques eólicos *offshore*[16] automatizados (SUN; HUANG; WU, 2012; FLEMING et al. 2017);
- Estaleiros que empreguem sistemas de automação e controle típicos da Indústria 4.0, tanto nos seus processos industriais quanto em suas infraestruturas (ARAKAKI, 2009).

Evidentemente, estes exemplos não esgotam as posibilidades de alvo em um eventual ataque ciber-cinético no Poder Marítimo. No entanto, ajudam a retratar o amplo espectro de sistemas sujeitos a este tipo de ameaça.

Note que em muitos dos exemplos acima mencionados, os controladores (e.g. CLPs e CPs) também são conectados a sistemas supervisórios (SCADA) por meio de redes de comunicação. Além disso, dependendo do propósito da planta física, pode haver ainda a conexão física entre os sistemas SCADA e outras redes – o que eventualmente inclui um caminho físico até a Internet.

Nos casos em que há a necessidade de uma conexão física entre a rede de controle e outras redes, a literatura recomenda a adoção de soluções de segurança envolvendo, por exemplo, firewalls, zonas desmilitarizadas (ou demilitarized zones – DMZ), sistemas de detecção de intrusão (ou Intrusion Detection System – IDS) e arquiteturas de rede específicas (STOUFFER; FALCO; SCARFONE, 2011). Evidentemente, uma medida de segurança simples e eficiente para minimizar a probabilidade de ataques a estes tipos de sistema consiste em manter a rede de controle isolada de outros tipos de rede – i.e. sem conectividade física entre as mesmas. Esta estratégia, também conhecida como air-gapping[17] , é comumente adotada em sistemas críticos como, por exemplo, sistemas nucleares, militares, etc. No entanto, é importante grifar que o uso de air-gapping não garante a segurança plena dos sistemas cibernéticos. Um malware pode, por exemplo, vencer o air-gap por meio do uso de mídias removíveis, como no caso do Stuxnet (FALLIERE; MURCHU; CHIEN, 2011); ou mesmo ser implantado no sistema antes ou durante o seu comissionamento, como no caso do ataque ao gasoduto transiberiano (CLARK; KNAKE, 2010). Isto sugere a necessidade de adoção de outras medidas de segurança – além das medidas técnicas acima exemplificadas – capazes de mitigar eventuais ataques a estes tipos de sistema, isolados ou não por air-gap.

## ATAQUES CIBER-ELETRÔNICOS

O conceito de ataque ciber-eletrônico ora

[16] Embora ainda esteja começando a ser explorada no Brasil (LUNA, 2018), um estudo do Instituto Nacional de Pesquisas Espaciais (INPE) aponta que "o potencial energético offshore na ZEE brasileira é cerca de 12 vezes maior que na área continental do país, sendo capaz de alavancar o desenvolvimento sustentável do Brasil em longo prazo." (ORTIZ; KAMPEL, 2011)

[17] *Air-gapping* é uma medida de segurança de rede utilizada para garantir que a rede de computadores a ser protegida esteja fisicamente isolada de redes desprotegidas, como a Internet ou uma rede local insegura. Neste tipo de medida, como não há conectividade física entre as redes, diz-se que elas estão isoladas por uma barreira conceitual de ar (air-gap).

apresentado estabelece que este tipo de ofensiva reúne elementos da guerra eletrônica e da guerra cibernética. Evidentemente, portanto, os potenciais alvos para estetipo de ataque têm por característica uma arquitetura que interconecta dispositivos que atuam nos domínios eletrônico e cibernético. Tipicamente estes alvos são compostos por equipamentos de transmissão/recepção de ondas eletromagnéticas e sistemas computacionais que se encarregam de processar as informações recebidas via espectro eletromagnético.

Para facilitar a compreensão de como este tipo de ataque pode ocorrer, trazemos, como exemplo, uma descrição sucinta do funcionamento de um radar de busca com vídeo sintético. Neste tipo de radar, os ecos recebidos por sua antena na forma de ondas eletromagnéticas são tratados eletronicamente, convertidos para valores binários e armazenados em uma memória para posterior processamento. Enquanto o radar varre o espaço de busca, todos os ecos válidos recebidos são armazenados na memória formando, assim, um retrato da situação da área monitorada.

Para reproduzir a informação armazenada, um processo computacional iterativamente lê os dados contidos na memória e os converte em imagen para o operador do radar (BOLE; DINELEY; WALL, 2005).

Observe que, assim como os ecos reais do ambiente são convertidos em bits e armazenados na memória, os ecos sintéticos, eventualmente transmitidos por um atacante, também serão convertidos em bits e armazenados na mesma memória. Dessa forma, é possível que um atacante transmita comandos codificados em sequências de ecos sintéticos, os quais, ao serem recebidos pelo radar alvo, serão armazenados na memória do sistema como se fossem ecos do ambiente monitorado. Evidentemente, este processo – por ora caracterizado apenas como MAE – por si só não tem a capacidade de alterar o funcionamento normal do radar. Se o sistema não estiver comprometido por um proceso computacional mal intencionado, esta informação falsa (inserida por meio de ecos sintéticos) será tratada pelo sistema e pelo operador como dados de alvo ou clutter (BOLE; DINELEY; WALL, 2005). Ainda que esta MAE possa atrapalhar a interpretação do que ocorre no ambiente, ou ainda influencie o processo decisório do usuário, o sistema continuará operando da mesma forma em que foi projetado. Contudo, se o sistema estiver comprometido por um processo computacional malicioso, é possível fazer com que as informações introduzidas na memória do radar por meio de ecos sintéticos (transmitidos pelo atacante) sejam interpretadas como comandos. Neste caso, a componente cibernética do ataque ciberelétrônico se encarrega de interpretar tais comandos podendo, em função destes, acionar rotinas maliciosas que alterem o processo computacional normal do sistema. Tais rotinas maliciosas podem, por exemplo, causar o desligamento do sistema, interromper a atualização das imagens para o operador, ou mesmo reproduzir imagens previamente gravadas de uma operação normal – como supostamente ocorreu no caso da operação Orchard (CLARK; KNAKE, 2010).

De forma similar ao exemplo acima descrito, outros sistemas que processem informações recebidas via espectro eletromagnético também estão sujeitos a ataques ciber-eletrônicos. Sem a pretensão de esgotar os potenciais alvos deste tipo de ataque, são apresentados aqui alguns exemplos:

- Sistemas Radar e ARPA (Automatic Radar Plotting Aids) que, de forma geral, façam uso de sinais de vídeo digitalizados (BOLE; DINELEY; WALL, 2005). Isto inclui, por exemplo, radares de navegação, de busca aérea e de busca combinada, utilizados por embarcações e instalações civis e militares;
- Sistemas de Exibição de Cartas Eletrônicas e Informação (Eletronic Chart Display and Information Systems – ECDIS) (WARD; ROBERTS; FURNESS, 2000) que integram às cartas eletrônicas informações obtidas de outros sistemas como radar, gps, etc.;
- Sistemas Integrados do Passadiço (Integrated Bridge System – IBS), que interconectam sistemas radar/ARPA, GPS, etc. a Sistemas de Exibição de Cartas Eletrônicas e Informação (ECDIS), bem como a sistemas de controle de leme e propulsão de navios (BHATTI; HUMPHREYS, 2017);
- Sistemas de Medida de Apoio à Guerra Eletrônica (MAGE), composto tipicamente por antenas, receptores de micro-ondas e sistemas computacionais responsáveis por processar, classificar e identificar as emissões eletromagnéticas presentes no ambiente (MATUSZEWSKI, 2008).

Em geral, estes sistemas são mantidos isolados de outras redes de comunicação (e da Internet). Isto significa que, em grande parte dos casos, a componente cibernética do ataque ciber-

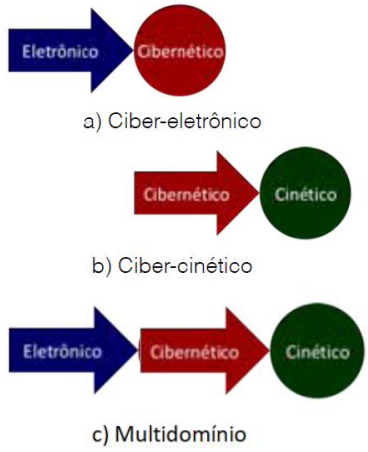
eletrônico deve ser capaz de vencer o air-gap para se instalar no ambiente computacional do alvo. Contudo, apesar da dificuldade imposta pelo air-gap, estes sistemas não podem ser considerados integralmente seguros do ponto de vista cibernético. Assim como relatamos no caso de ataques ciber-cinéticos, um malware pode, por exemplo, vencer o air-gap através de mídias removíveis. Além disso, um gatilho lógico pode ser implantado no alvo durante a sua fabricação ou comissionamento.

## ATAQUES MULTIDOMÍNIO

Na taxonomia apresentada descrevemos os ataques multidomíniovcomo aqueles cuja execução permeia os três domínios ora em discussão: cibernético, eletrônico e cinético. Já tratamos conceitualmente neste artigo como um ataque cibe-eletrônico pode manipular um sistema computacional –e acionar processos mal intencionados– a partir de comandos/informações sintéticas recebidas do domínio da guerra eletrônica. Tal conceito de ataque é representado e exemplificado na Figura 2a. Discutimos conceitualmente, também, como manipulações digitais mal intencionadas no domínio cibernético podem produzir efeitos cinéticos diretos em uma planta física, através de ataques ciber-cinéticos. Para comparação, este conceito de ataque também é representado na Figura 2b.

Em ataques multidomínio, a componente cibernética do ataque atua como um pivô entre os domínios das guerras eletrônica e cinética. Conforme ilustrado na Figura 2c, a componente cibernética pode ser implantada para permitir, por exemplo, que comandos originados no domínio da guerra eletrônica sejam interpretados e convertidos em efeitos cinéticos diretos em uma planta física.

Figura 2 –Fluxos de acionamento dos ataques.




Portanto, os potenciais alvos para este tipo de ataque são sistemas que integram equipamentos de transmissão/recepção de ondas eletromagnéticas e sistemas computacionais que controlam plantas físicas. Um exemplo de potencial alvo para ataques multidomínio são os Sistemas Integrados do Passadiço (Integrated Bridge System – IBS), ou ainda sistemas Smartship (FULLERTON et al., 2004). Dentre os dispositivos de transmissão/recepção de ondas eletromagnéticas conectados à um IBS há sistemas radar/ARPA, receptores GPS, e receptores AIS (Automatic Identification System). Tipicamente, os IBSs reúnem em um único local informações oriundas destes sistemas, plotando em uma carta náutica digital as informações do navio e de outras embarcações – detectadas pelos radares de navegação. A interligação do IBS com os sistemas de controle da propulsão e do leme permite a realização de funções de piloto automático, eliminando a necessidade de atuação contínua de um timoneiro (FULLERTON et al., 2004; BHATTI; HUMPHREYS, 2017). O uso de IBSs em meios navais proporciona como vantagens a redução das tripulações, o aumento da prontidão dos navios, a redução do tempo necessário para treinamento, o aumento da consciência situacional, e a redução da carga administrativa sobre o pessoal (FULLERTON et al., 2004). Estes beneficios têm motivado o aumento do uso destes sistemas tanto em navios mercantes quanto em navios de guerra (FULLERTON et al., 2004).

Ao mesmo tempo em que sistemas do tipo IBS trazem uma série de vantagens, também podem expor os meios navais a novos tipos de ameaça, como os ataques multidomínio. Do mesmo modo que a componente cibernética de um ataque ciber-eletrônico pode acionar procesos computacionais maliciosos a partir da interpretação de comandos oriundos do espectro eletromagnético, isto também pode ocorrer em um ataque multidomínio. No entanto, em um ataque multidomínio, o proceso computacional malicioso, ao ser acionado, estende suas ações e atinge os processos físicos controlados. Em um IBS, por exemplo, isto significa que o controle da propulsão pode ser afetado por comandos recebidos por uma antena (e.g. a antena de um radar), se o sistema estiver infectado por um código malicioso capaz de interpretar/converter as informações recebidas em comandos para a máquina do navio. Note que, mesmo que o alvo esteja protegido pelo air-gap, a componente

cibernética do ataque pode ser injetada no sistema mor meio de mídias removíveis. Além disso, conforme já discutido anteriormente, este tipo de gatilho lógico também pode ser implantado no alvo durante a sua fabricação ou comissionamento. A motivação de um ataque deste tipo está na capacidade de o atacante acionar remotamente rotinas maliciosas que impactem fisicamente o funcionamento dos meios, sem a necessidadede ter acesso direto ao ambiente cibernético do alvo.

## POLITICAS PARA MITIGAÇÃO DE ATAQUES

Nesta seção são discutidas algumas políticas para a segurança do poder marítimo em relação às três classes de ataque em questão. Considerando que o domínio cibernético é a parcela comum aos referidos ataques, o foco da discussão se concentra em políticas voltadas para a segurança deste domínio. Mais especificamente, são abordadas políticas visando a qualificação de pessoal e a homologação e certificação de produtos.

## QUALIFICAÇÃO DE PESSOAL

Em 2003, o governo dos EUA publicou a sua estratégia nacional para segurança do ciberespaço (WHITE HOUSE, 2003), onde declara como propósito:

> *"... envolver e capacitar os Americanos para proteger as parcelas do ciberespaço que possuem, operam, controlam ou com as quais interagem."* (WHITE HOUSE, 2003, p.vii, tradução nossa)

Ao mesmo tempo em que a referida estratégia traça este objetivo, a mesma reconhece que:

> *"Proteger o ciberespaço é um desafio estratégico difícil, que requer esforço coordenado e concentrado de toda a nossa sociedade – o governo federal, os governos estaduais e locais, o setor privado e o povo Americano."* (WHITE HOUSE, 2003, p.vii, tradução nossa).

De fato, proteger o ciberespaço é um desafio estratégico complexo, a começar – no caso específico daquela Estratégia – pelo objetivo de envolver e capacitar o povo Americano na proteção de suas parcelas do ciberespaço. Algo difícil de ser alcançado de forma plena, se considerarmos todos os elementos e setores da sociedade previstos em (WHITE HOUSE, 2003). No entanto, apesar das dificuldades impostas pela abrangência, é indiscutível a necessidade de uma nação perseguir o objetivo de envolver e capacitar a sua sociedade na segurança do ambiente cibernético. Da mesma forma, inspirados no propósito de White House (2003), consideramos imprescindível envolver e capacitar os atores do Poder Marítimo quanto à proteção de suas parcelas do ciberespaço.

Embora o Poder Marítimo represente público menor do que o visado por White House (2003), trata-se ainda de um público abrangente. Por este motivo, qualificar o pessoal do Poder Marítimo quanto à segurança de suas parcelas do ciberespaço é uma tarefa desafiadora, que sugere o emprego de políticas de conscientização e capacitação de pessoal. Estas políticas devem abranger não só os recursos humanos do Poder Naval e da Marinha Mercante, mas também de setores industriais e infraestruturas pertencentes ao Poder Marítimo.

No Brasil, os recursos humanos do Poder Naval e da Marinha Mercante, são formados pelo Sistema de Ensino Naval e pelo Sistema de Ensino Profissional Marítimo, ambos de responsabilidade da Marinha do Brasil (BRASIL, 2006). É desejável, portanto, que os currículos dos referidos Sistemas de Ensino contenham disciplinas que abarquem conceitos sobre o funcionamento e a segurança do domínio cibernético e de sistemas híbridos (onde o domínio cibernético interage diretamente com os domínios eletrônico e/ou cinético).

A exemplo da discussão apresentada em (SCHNEIDER, 2013; CONKLIN; CLINE; ROOSA, 2014) - onde a educação sobre segurança cibernética visa um público mais abrangente do que nos casos do Poder Naval e da Marinha Mercante - o desafio maior está em promover a qualificação dos recursos humanos dos setores industriais e de infraestruturas pertencentes ao Poder Marítimo, no que concerne à segurança cibernética e de sistemas híbridos. Isto porque a formação técnico-profissional de seu pessoal conta com a participação de um grande número de instituições e estabelecimentos de ensino, públicos e privados.

Deste modo, e com base na discussão apresentada em (SCHNEIDER, 2013), é razoável concluir não ser trivial solucionar a questão através de um processo amplo de aprimoramento curricular - ainda que necessário.

Neste caso, soa ser adequado apoiar estes setores através de programas de treinamento e conscientização promovidos, a priori, pelos órgãos do Estado responsáveis pela Segurança e Defesa cibernética no Brasil – i.e. o Gabinete de Segurança Institucional e o Comando do Exército, respectivamente.

Iniciativa similar a esta é praticada, por exemplo, pelo Department of Homeland Security, dos EUA, através dos programas de treinamento conduzidos pelo Industrial Control Systems Cyber Emergency ReadinessTeam (ICS-CERT). O ICS-CERT oferece continuamente cursos de segurança cibernética de sistemas de controle industrial para o pessoal da indústria ede infraestruturas críticas daquele país, bem como para desenvolvedores/fornecedores de dispositivos e softwares. É importante ressaltar que os programas de treinamento do ICS-CERT não se restringem à industria do Poder Marítimo dos EUA, abrangendo também outros setores da indústria. No modelo do ICS-CERT, o referido órgão federal apoia de forma centralizada a qualificação do pessoal da indústria no assunto. No caso do Poder Marítimo brasileiro, guardadas as devidas proporções, um modelo similar de apoio centralizado à capacitação parece ser adequado para suprir a necessidade da sua indústria e infraestruturas, no que concerne à na segurança dos tipos de sistema discutidos neste artigo.

## HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTOS

Discutiu-se neste artigo uma possível estratégia de qualificação de pessoal para promover a segurança de sistemas cibernéticos e híbridos do Poder Marítimo. Contudo, ainda que a esta qualificação seja de extrema importância, ela não é, por si só, suficiente para maximizar a segurança dos sistemas (BAARS et al.; 2015). Para uma maior segurança, as políticas de qualificação de pessoal devem ser complementadas por políticas que combatam possíveis vulnerabilidades tecnológicas nos hardwares e softwares.

As vulnerabilidades de um sistema podem surgir de forma não intencional (DU; MATHUR, 1998; GROVER; CUMMINGS; JANICKI, 2016), por falhas de projeto, implementação ou configuração, ou podem ser intencionalmente introduzidas por agentes maliciosos (ADEE, 2008; ROBERTSON; RILEY, 2018) durante o projeto, fabricação, distribuição, comissionamento, operação e manutenção do sistema. Uma forma de combater vulnerabilidades – intencionais ou não – é por meio da adoção de um conjunto de requisitos de segurança, estabelecidos de acordo com a criticidade do sistema, os quais devem ser rigorosamente atendidos (HERRMANN, 2002).

Chega-se, então, à seguinte pergunta: como garantir que um equipamento em uso pelo Poder Marítimo atende a um determinado conjunto de requisitos de segurança, permitindo afastar ou mitigar determinado conjunto de riscos de segurança cibernética? Tal pregunta traz uma série de desafios, sobre os quais passamos a dissertar, a seguir.

Considere a complexidade da cadeia de produção dos productos de hardware e software usados pelo Poder Naval, pela Marinha Mercante, pelas indústrias e infraestruturas pertencentes ao Poder Marítimo. A indústria responsável pela produção de equipamentos civis, militares ou duais do Poder Marítimo brasileiro não apenas opera distante do monitoramento dos órgãos de Segurança e Defesa cibernética do Brasil como também, por pertencer à cadeia global de valores de eletrônicos, muitas vezes depende de intricadas cadeias de produção que incluem a subcontratação de empresas baseadas em outros países (PINTO, 2016) – o que dificulta ainda mais o monitoramento da produção. Dessa forma, mesmo que se tenha um entendimento pleno a respeito dos requisitos de segurança cibernética a serem atendidos pelos hardwares/softwares, pouca confiança pode ser trazida por um processo de avaliação baseado tão-somente em testes “funcionais” – i.e. testes que caracterizem o comportamento do hardware/software em condições típicas de operação.

De fato, conforme os exemplos apresentados em (ZETTER, 2014; ADEE, 2008; CLARK; KNAKE, 2010), caso um equipamento viesse a ser objeto de manipulação com vistas à implantação de um comportamento malicioso por parte de uma nação hostil, certamente tal comportamento malicioso eria ativado por meio de operações não triviais, dificilmente identificados através de testes meramente associados às condições típicas de uso do equipamento.

Note que a literatura tem reportado casos com indícios/evidencias de implantações maliciosas em sistemas cibernéticos críticos, embora muitas vezes careçam de detalhes em virtude do sigilo. Um exemplo é o caso do ataque ao sistema de vigilância aéreo sírio ocorrido durante a operação

Orchard, já discutido neste artigo. Conforme relatado em (ADEE, 2008), especula-se que os microprocessadores comerciais no radar sírio possam ter sido propositalmente fabricados com um backdoor escondido.

Ao enviar um código pré-programado para esses chips, um atacante desconhecido teria a capacidade de bloquear temporariamente o radar.

Sobre a prática de implantar vulnerabilidades em hardwares, Adee afirma ainda que:

> *falou sob condição de anonimato, um "fabricante europeu de chips" recentemente embutiu em seus microprocessadores uma chave de desligamento que pode ser acessada remotamente."* (ADEE, 2008, p.1, tradução nossa)

Um exemplo mais recente de implantação de chips maliciosos em hardwares de sistemas críticos é relatado em (ROBERTSON; RILEY, 2018). Trata-se de um ataque à cadeia de produção – ou supply chain attack – reportado pela Amazon.com Inc. às autoridades dos EUA. Neste caso, especialistas identificaram um minúsculo microship, "não muito maior do que um grão de arroz" (ROBERTSON; RILEY, 2018), escondido em placas mãe de servidores. Tal microship não fazia parte do projeto original das placas. Segundo Robertson e Riley, investigadores concluíram que os referidos chips permitem que invasores criem uma entrada furtiva em qualquer rede que contenha as máquinas com as placas alteradas. Além disso, segundo Robertson e Riley, investigadores relatam que os chips foram inseridos em fábricas controladas por empresas subcontratadas na China (ROBERTSON; RILEY, 2018). Dentre os sistemas críticos comprometidos pelo supply chain attack estão centros de dados do Departamento de Defesa dos EUA, sistemas de operação de drones da CIA e as redes a bordo de navios de guerra da Marinha dos EUA (ROBERTSON; RILEY, 2018).

Sendo assim, com o objetivo de mapear e mitigar os riscos associados ao uso de softwares e hardwares produzidos em ambientes não monitorados, algumas nações ao redor do mundo têm implantado sistemas de homologação de produtos cibernéticos (FNCA, 2018; DSD, 2015; NIST, 2011; DISA, 2017). Trata-se de metodologias que permitem atestar, com um grau mínimo de confiança, e por meio de testes e ensaios sistemáticos, que um produto de software ou hardware atende a um conjunto de requisitos de segurança – mesmo que o seu processo de produção não esteja completamente sob controle/supervisão dos órgãos de segurança e defesa cibernética do país. Dentre os sistemas deste tipo existentes pelo mundo citamos Certification de Sécurité de Premier Niveau (CSPN) (FNCA, 2018) utilizado na França, o Australasian Information Security Evaluation Program (AISEP) (DSD, 2015) implementado na Autrália e Nova Zelândia (DSD, 2015), o Department of Defense Information Network Approved Products List (DoDIN/APL) dos EUA e o Federal Information Processing Standard 140-2 (FIPS 140-2) (NIST, 2011) adotado tanto nos EUA quanto no Canadá.

O Brasil vem ocupando uma posição de relativo pioneirismo nessa área, ao estabelecer o chamado Sistema de Homologação e Certificação de Produtos de Defesa Cibernética (SHCDCiber). O SHCDCiber foi concebido em 2015 e tem por objetivo estabelecer um sistema de avaliação de segurança cibernético objetivo e baseado nas principais normas internacionais, garantindo o rigor científico nas avaliações de segurança e o reconhecimento internacional por parte dos fabricantes que submeterem seus produtos à avaliação.

A exemplo dos sistemas CSPN, AISEP, DoDIN/APL e FIPS 140-2, o SHCDCiber consiste num sistema voltado para o uso de mecanismos de avaliação da conformidade com o objetivo de avaliar a segurança de ativos de tecnologia e equipamentos com software embarcado. Trata-se, portanto, de um sistema com potencial de contribuir para o aumento da segurança dos sistemas cibernéticos e híbridos do Poder Marítimo. O SHCDCiber segue uma abordagem de avaliação da conformidade composta de três etapas:

1 - Análise de riscos da aplicação. Cada aplicação apresenta um conjunto de riscos específicos e que deve ser levando em consideração na construção de mecanismos de avaliação.

2 - Especificação de requisitos. Os requisitos exatos de segurança a serem atendidos por uma aplicação serão determinados pelos riscos apresentados por aquela aplicação.

3 - Ensaios de segurança. O atendimento a um conjunto de requisitos de segurança é realizado por meio da execução de ensaios que correspondem a procedimentos sistemáticos de validação.

As três etapas acima, realizadas conjuntamente, contemplam o que se pode denominar como um Programa de Avaliação da Conformidade. Na área de segurança da informação, tais programas são particularmente desafiadores, na medida em que o comportamento de um ativo de Tecnologia de Informação e Comunicação (TIC) depende de seu software embarcado. Dessa forma, pesquisas vêm sendo desenvolvidas no sentido de aumentar a confiança em avaliações de segurança nas áreas de criptografia (MACHADO et al., 2016; KOWADA; MACHADO; 2017), aleatoriedade (RIBEIRO et al. 2018), protocolos de segurança (MACHADO et al., 2015), análise de software (BENTO, 2017, no prelo) e testes caixapreta (TELES; MACHADO, 2017).

Cabe observar que a aprovação em um programa de avaliação da conformidade não significa uma confiança total na segurança do objeto aprovado. Afinal, os requisitos são especificados em consistência com os riscos de aplicação – e variações no cenário de riscos podem levar a eventuais mudanças na condição de segurança de um produto ou sistema.

**Análise crítica.** Mesmo após o sucesso nas etapas anteriores, dependendo da criticidade, cabe ainda observar aspectos adicionais que podem levar à decisão pela não adoção de uma tecnologia. Tais aspectos incluem, tipicamente, as características do desenvolvedor e do seu processo produtivo. Como exemplo, listamos algumas perguntas a serem respondidas antes da adoção de uma tecnologia – mesmo que a mesma tenha superado adequadamente as etapas 1 a 3:

- O fornecedor da tecnologia tem condições de atender aos pedidos na escala demandada?
- O fornecedor da tecnologia possui um sistema de gestão de segurança da informação implantado?
- Mais especificamente nos sistemas do Poder Naval, dependendo da criticidade do sistema, os desenvolvedores e produtores – pessoas a serviço de entidades públicas ou privadas – possuem a devida credencial de segurança para lidar com o produto ou tecnologia em questão?
- O fornecedor da tecnologia cumpre processos adequados de proteção e descarte de dados sensíveis?
- O fornecedor da tecnologia mantém o núcleo de sua produção (conhecimento crítico para a produção) no país?

## CONCLUSÕES

Neste artigo discutimos como o encontro da guerra cibernética com as guerras eletrônica e cinética pode impactar diretamente o Poder Marítimo. Visando dar suporte à discussão sobre as novas vertentes da guerra cibernética que decorrem deste encontro, apresentamos uma taxonomía que estabelece classes de ataques híbridos que, além de explorar o dominio cibernético, exploram também os domínios eletrônico e cinético. Desta taxonomia, emergem três classes de ataque – ciber-cinético, ciber-eletrônico e multidomínio – que ampliam o espectro das formas de manifestação do princípio dos efeitos cinéticos. Discutimos estas três classes de ataque e caracterizamos, por meio de exemplos, seus potenciais alvos dentro do Poder Marítimo. A discussão, pautada em casos conhecidos, evidências ededuções tecnológicas, indicam ser factível a ocorrência de estes tipos de ataque no referido Poder. Sendo assim, o estudo aponta para a necessidade de desenvolver políticas capazes de promover a segurança dos sistemas cibernéticos e híbridos do Poder Marítimo.

Considerando que o domínio cibernético é a parcela comum entre as três classes de ataque analisadas neste artigo, concentramos a nossa discussão em políticas voltadas para a segurança deste domínio, abordando tanto a questão de qualificação de pessoal, quanto o combate às vulnerabilidades em produtos cibernéticos. No que concerne à qualificação de pessoal, encorajamos a adoção de um modelo apoiado nos sistemas de ensino naval e profissional marítimo, já existentes, complementado pela atuação de um órgão centralizado de capacitação sobre segurança cibernética. O Sistema de Ensino Naval e o Sistema de Ensino Profissional Marítimo, com currículos continuamente atualizados quanto ao assunto, se encarregariam da capacitação do pessoal do Poder Naval e da Marinha Mercante, respectivamente (como já é previsto). Já um órgão centralizado de capacitação sobre segurança cibernética se encarregaria de promover a qualificação dos recursos humanos dos setores industriais e de infraestruturas pertencentes ao Poder Marítimo.

No que tange a mitigação de vulnerabilidades em produtos cibernéticos em uso no Poder Marítimo, o estudo aponta para a solução por meio de um sistema de homologação e certificação de produtos cibernéticos, o que já vem sendo

adotado de alguma forma por países como a França, Austrália, Nova Zelândia, EUA e Canada. Cabe ressaltar, que as políticas de qualificação de pessoal, homologação e certificação de produtos aquí discutidas não têm a pretensão de assegurar, de forma plena, a segurança dos sistemas cibernéticos e híbridos do Poder Marítimo. No entanto, têm o potencial de contribuir, de forma positiva e abrangente, para a segurança destes sistemas.

## REFERÊNCIAS

ADEE, Sally. The hunt for the kill switch. IEEE Spectrum, v. 45, n. 5, p. 34-39, 2008.

AMIN, Saurabh et al. Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks. IEEE Transactions on Control Systems Technology, v. 21, n. 5, p. 1963-1970, 2013.

AMIN, Saurabh et al. Stealthy deception attacks on water SCADA systems. In: Proceedings of the 13th ACM international conference on Hybrid systems: computation and control. ACM, 2010. p. 161-170.

ARAKAKI, Glenn T. Yokosuka Naval Base Prepares for Nuclear Aircraft Carrier. Army Engineer School Fort Leonard Wood MO, 2009.

AYALA, Luis. Prevent Hackers from Destroying a Backup Generator. In: Cyber-Physical Attack Recovery Procedures. Apress, Berkeley, CA, 2016. p. 41-42.

BENTO, Lucila MS et al. Dijkstra graphs. Discrete Applied Mathematics, 2017. No prelo.

BHATTI, Jahshan;HUMPHREYS, Todd E. Hostile control of ships via false GPS signals: Demonstration and detection. NAVIGATION: Journal of the Institute of Navigation, v. 64, n. 1, p. 51-66, 2017.

BOLE, Alan G.; DINELEY, William O.; WALL, Alan. Radar and ARPA manual. 2. ed. Oxford: Elsevier Butterworth Heinemann, 2005.

BONNER, Henry M. The radio proximity fuse. Electrical Engineering, v. 66, n. 9, p. 888-893, 1947.

BOYES, Hugh; ISBELL, Roy. Code of Practice: Cyber Security for Ships. 2017.

BRASIL. Lei nº 11.279, de 9 de fevereiro de 2006. Dispõe sobre o ensino na Marinha. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004- 2006/2006/Lei/L11 279.htm>. Acesso em: 29 out. 2018.

BROWN, Louis. The proximity fuze. IEEE Aerospace and Electronic Systems Magazine, v. 8, n. 7, p. 3-10, 1993.

CLARK, Richard A.; KNAKE, Robert K. Cyber War: The next threat to national security and what to do about it. New York: Ecco, 2010.

DE SÁ, Alan Oliveira; DA COSTA CARMO, Luiz F. Rust; MACHADO, Raphael CS. Covert attacks in cyber-physical control systems. IEEE Transactions on Industrial Informatics, v. 13, n. 4, p. 1641-1651, 2017.

DIPERT, Randall R. Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy. Journal of Military Ethics, v. 12, n. 1, p. 34-53, 2013.

DISA. Department of Defense Information Network (DoDIN) Approved Products List (APL) Process Guide. Defense Information Systems Agency (DISA). 2017.Disponível em: https://aplits.disa.mil/docs/aplprocessguide. pdf> Acesso em: 28 out. 2018.

DSD. Australian government information and communications technology security manual. Defence Signals Directorate (DSD) Auditing, v. 3, p. 31, 2005.

ERICKSON, Kelvin T. et al. Reliability of S CADA Systems in Offshore Oil and Gas Platforms. In: Stability and Control of Dynamical Systems with Applications. Birkhäuser, Boston, MA, 2003. p. 395-404.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. W32. Stuxnet dossier. White paper, Symantec Corp., ecurity Response, v. 5, n. 6, p. 29, 2011.

FLEMING, Paul et al. Field test of wake steering at an offshore wind farm. Wind Energy Science, v. 2, n. 1, p. 229-239, 2017.

FNCA. Catalogue of the Qualified Solutions. French National Cybersecurity Agency (FNCA). 2018. Disponível em: https://www. ssi.gouv.fr/uploads/2018/01/catalogue_ qualified_solutions_anssi.pdf Acesso em: 28 out. 2018.

FULLERTON, Jeff et al. Operational Impacts of the Aegis Cruiser Smartship System. NAVAL SEA SYSTEMS COMMAND WASHINGTON DC, 2004.

GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, v. 29, n. 7, p. 1645-1660, 2013.

HART, Dennis. An approach to vulnerability assessment for Navy Supervisory Control and Data Acquisition (SCADA) system. 2004. Tese de Mestrado. Monterey, California. Naval Postgraduate School.

JANER, Denis; PROUM, Chauk-Mean. Open Architecture for Naval Combat Direction System. In: Complex Systems Design & Management. Springer, Cham, 2014. p. 73-84.

KAISER, Robert. The birth of cyberwar. Political Geography, v. 46, p. 11- 20, 2015.

KOWADA, L. ; MACHADO, R.C.S. . Esquema de Acordo de Chaves de Conferência Baseado em um Problema de Funções Quadráticas de Duas Variáveis. Anais do XVII Simpósio Brasileiro em Segurança da Informaçãoe de Sistemas Computacionais (SBSeg), 2017, Brasília, 2017.

KUMAR, Nishant; MAJUMDAR, Sayan; BABU, G. Madhu. Automatic control of tidal power plant. In: Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM), 2012 International Conference on. IEEE, 2012. p. 24-28.

LAGOUVARDOU, Sotiria. Maritime Cyber Security: concepts, problems and models. 2018.

LANGNER, Ralph. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, v. 9, n. 3, p. 49-51, 2011.

LASI, Heiner et al. Industry 4.0. Business & Information Systems Engineering, v. 6, n. 4, p. 239-242, 2014.

LEE, Jay; BAGHERI, Behrad; KAO, Hung-An. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, v. 3, p. 18-23, 2015.

LUNA, D. Petrobrás vai gerar energia eólica no mar. O Estado de S.Paulo, São Paulo, 24 de julho de 2018. Disponível em: < https://economia. estadao.com.br/noticias/geral,petrobras-vai-gerar-energia-eolica-nomar, 70002412545> Acesso em: 17 out. 2018.

MACHADO, Raphael CS et al. Fair fingerprinting protocol for attesting software misuses. In: Availability, Reliability and Security (ARES), 2015 10th International Conference on. IEEE, 2015. p. 110-119.

MACHADO, Raphael CS et al. Software control and intellectual property protection in cyber-physical systems. EURASIP Journal on Information Security, v. 2016, n. 1, p. 8, 2016.

MANDARINO JUNIOR, Raphael; CANONGIA, Claudia. Livro verde: segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010.

MARINHA DO BRASIL. Doutrina Básica da Marinha. Rev. 2. Brasília 2014.

MATUSZEWSKI, Jan. Specific emitter identification. In: Radar Symposium, 2008 International. IEEE, 2008. p. 1-4.

MILLER, Bill; ROWE, Dale. A survey SCADA of and critical infrastructure incidents. In: Proceedings of the 1st Annual conference on Research in information technology. ACM, p. 51-56, 2012.

MINISTÉRIO DA DEFESA. Política de Guerra Eletrônica de Defesa – MD32-P-01, 1ª Edição, 2004.

MINISTÉRIO DA DEFESA. Manual de Doutrina Militar de Defesa – MD51-M-04, 2ª Edição, 2007.

MINISTRY OF DEFENSE. UK Defense Doctrine – Joint Doctrine Publication 0-01. 5 ª Edição, 2014.

NIST. FIPS 140-2: Security Requirements for Cryptographic Modules. National Institute of Standards and Technology (NIST) v. 25, 2001.

NORCUTT, L.S. Ship Self-Defense System Architecture. Johns Hopkins Apl Technical Digest, v.22, n.4, p. 536-546, 2001.

ORTIZ, G. P.; KAMPEL, M. Potencial de energia eólica offshore na margen do Brasil. Instituto Nacional de Pesquisas Espaciais. V simpósio Brasileiro de Oceanografia, Santos, 2011.

PARKS, Raymond C.; DUGGAN, David P. Principles of cyberwarfare. IEEE Security & Privacy, v. 9, n. 5, p. 30-35, 2011.

REED, Thomas C. At the abyss: an insider's history of the Cold War. Presidio Press, 2005.

RIBEIRO, Leonardo C. et al. True Random Number Generators for Batch Control Sampling in Smart Factories. In: 2018 Workshop on Metrology for Industry 4.0 and IoT. IEEE, 2018. p. 213-217.

ROBERTSON, Jordan.; RILEY, Michael. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg Businessweek,04 de outubro de 2018. Disponível em: <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny -chip-toinfiltrate- america-s-top-companies> Acesso em: 27 out. 2018.

SHAKARIAN, Paulo. The 2008 Russian cyber campaign against Georgia. Military review, v. 91, n. 6, p. 63, 2011.

SHELTON, H. JP3-13: Joint Doctrine for Information Operations. 1998. http://www.c4i.org/jp3_13.pdf.

SMITH, Roy S. Covert misappropriation of networked control systems: Presenting a feedback structure. IEEE Control Systems, v. 35, n. 1, p. 82-92, 2015.

STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. NIST special publication, v. 800, n. 82, p. 16-16, 2011.

SUN, Xiaojing; HUANG, Diangui; WU, Guoqing. The current state of offshore wind energy technology development. Energy, v. 41, n. 1, p. 298- 312, 2012.

TELES, C. ; MACHADO, R.C.S. . Testes de sobrecarga: uma avaliação sobre requisitos de Disponibilidade e Desempenho. Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Workshop sobre Regulação, Avaliação da Conformidade, Testes e Padrões de Segurança (SBSeg/WRAC+), Brasília, 2017.

TOPALOV, Andriy; KOZLOV, Oleksiy; KONDRATENKO, Yuriy. Control processes of floating docks based on SCADA systems with wireless data transmission. In: Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2016 XII International Conference on. IEEE, 2016. p. 57-61.

WADHAWAN, Yatin; NEUMAN, Clifford. Evaluating Resilience of Oil and Gas Cyber Physical Systems: A Roadmap. In: Annual Computer Security Application Conference (ACSAC) Industrial Control System Security (ICSS) Workshop. 2015.

WARD, Robert; ROBERTS, Chris; FURNESS, Ronald. Electronic chart display and information systems (ECDIS): State-of-the-art in nautical charting. Marine and Coastal Geographical Information Systems, p. 149- 161, 2000.

WEIGLEY, Russell F. JP1 Doctrine for the Armed Forces of the United States. 2013.

WEISS, Gus W. The Farewell Dossier. Center for the Study of Intelligence, Central Intelligence Agency (CIA), Washington DC, 1996.

WHITE HOUSE. The national strategy to secure cyberspace. Washington, DC: White House, 2003.

YASAR, Nurgul; YASAR, Fatih Mustafa; TOPCU, Yucel. Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield. In: Cyber Sensing 2012. International Society for Optics and Photonics, 2012.

ZETTER, Kim. Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books, 2014.

ZIVI, Edwin. Design of robust shipboard power automation systems. Annual Reviews in Control, v. 29, n. 2, p. 261-272, 2005.

*U.S Naval Institute Blog*

By Captain John Cordle, U.S. Navy (Retired)

April 12, 2019



**Captain John Cordle, U.S. Navy (Retired)**

Captain Cordle retired in 2013 after 30 years of service. He commanded the USS Oscar Austin (DDG-79) and USS San Jacinto (CG-56) and was chief of staff for Naval Surface Forces Atlantic. He is the 2010 recipient of the U.S. Navy League's Captain John Paul Jones Award for Inspirational Leadership.

# Redefine 'SWO Culture'

Years ago, as I walked down the pier after the outgoing change of command ceremony, my wife noticed that I kept looking up and back at the beautiful warship that I was leaving as we headed towards the car. "Would you like me to get you a lawn chair?" she asked, "that way you can sit here and stare at it!" I realized at that moment that a phase of my life was coming to an end, but what I failed to appreciate was that in those past two years my tour had contributed—for better or worse—to one of the most important overarching themes of my life: surface warfare officer (SWO) culture. Culture is a common theme these days; no matter what generation, retired SWOs get together in real or virtual life and opine that the SWO culture has gone to hell in a hand basket since they retired, with the unspoken implication that during their time, it was solid.

I have been part of many of those conversations and pressed others to elaborate and define what they think SWO culture really is and in what ways it has deteriorated. They often dismiss the question or provide a one word answer such as "millennials" or "mercenaries" and bemoan a general "deterioration of standards." But what does that really mean? Ask an aviator what he does for a living and he'll proudly say "I fly jets!" Ask a surface warfare officer what he does, and he'll tell you "I'm the auxiliaries division officer." A friend of mine who leads the Afloat Culture Workshop, a great program for commanding officers (COs)to help them assess their command culture, uses the question: "Are you a "San Jac

sailor or are you a Sailor on the San Jacinto" to help gauge the level of culture, commitment, and pride in the ship. The point is culture defines who we are and how we associate ourselves with our profession, not what we do; the difference between these speaks volumes about what is wrong and perhaps an idea on how to address it.

Recently, I recently mentored a first-class midshipmen who had to make a choice between submarine and surface nuclear power over the next weekend. His comment to me was "Here at the Naval Academy, surface warfare seems to be for those who don't have any other options and pretty much have to settle." What a shame. True, it has been that way for a while, but why? Have we examined the contributing factors and addressed them? Let's . . .

Webster's defines culture "as a set of values, goals and actions that define a group of people." A look at each of those tenets could help us dissect the question:

**Values.** The Navy has shifted a few times but settled on clear "Core Values" of honor, courage, and commitment, and has invested in defining them. Recently, however, these values have come under attack as the Fat Leonard scandal decimated the ranks of SWO captains and admirals and dragged on way too long, but without an exhaustive study of the root cause—what aspect of the SWO culture allowed it to spread so malignantly?

It always is difficult to talk ethics without sounding preachy—especially when some of your peer group are headed to jail. The value of courage has also come under fire of late as the Navy deals with the aftermath of two deadly collisions in 2017 and faces hard choices in identifying and addressing the root causes and is starting to address some of them. That said, the two review boards and other initiatives convened after these events address the concept of culture, but give grave warnings about the Navy's following "checklist mentality" without addressing underlying cultural issues which may take years to change. At the individual level, courage could take the form of a questioning attitude, addressing shortcomings in fellow watch standers—or even superiors—or in assessing the risk of a situation and telling a superior through forceful backup that a mission is either unsafe or unnecessary. The next level of courage simply is reporting your intention to not execute the task—rather than asking permission. Commitment to these values will manifest in the SWO community's ability to stay the course and implement the additional changes in the way they train sailors and operate ships, as well as looking beyond the surface warfare community to leverage lessons learned and best practices.

**Goals.** This is an area where the Navy has drifted a bit over the years—following slogans instead of actual goals—and now seems to be headed in the right direction. I can recall being in a room with a three-star admiral and a bunch of prospective COs who were told "We are building this damn ship—it's your job to go out there and define a mission for it!" OK, I grew up in Georgia, and down there we have a word for that kind of reasoning: Backasswards! You don't stop building hurricane-proof houses because there hasn't been a hurricane in a while and the United States should not stop building warships and weapons if it prepares us for the inevitable rise of a peer competitor. Goals like improving sailors' professional development, developing maintenance policies that get ships fixed, and a focus on warfighting and maritime proficiency will get the Navy there. As a former Air Boss (then my strike group commander) put it, "The two things we hold sacred in aviation are our pipeline training and our intermediate maintenance capability— you SWO's scrapped both of them and it will take a decade to recover," (this was in 2012)! He was right.

**Actions**. This is the final piece of the culture and possibly the most important. Everyone closely watches the leader and immediately recognizes any gaps between their words and actions. Great naval heroes—Josephus Daniels, Arleigh Burke, and John Bulkeley, to name a few—are not remembered for their lofty words but for their brave actions in battle. Admirals Hyman G. Rickover and Wayne E. Meyer are remembered for their warfighting focus—inside the strategic battlefield of the Pentagon. In a culture whose focus is going to sea, these actions manifest themselves in the way the service prioritizes maritime and tactical skills in the detailing process and in promotion and selection boards.

Recent actions such as the lengthening of division officer sea tours, the shortening of the period ashore between department head and command, and increased opportunities for junior sea command on patrol craft, minesweepers, and MK VI riverine boats all are examples that fit this mold. But how long is a strike troup command tour? A command tour? These should be the seminal career milestones— not the ones in the "5 Sided Puzzle Palace." (More on that later).

On an individual basis, actions taken to improve proficiency, remove barriers, and train the personnel under will yield results. These things take time—in some cases a generation—but there are things the Navy leaders can do to move them along:

**Define SWO Culture—On Our Terms.** With its incredibly dedicated people and awesome equipment, the Navy has both the recipe and the ingredients to "bake in" the right SWO culture. Here are some thoughts:

1. Never again change the Core Values. As a Marine once told me, "If they change, they aren't Core Values.
2. Keep goals focused on maritime proficiency and war fighting, in that order. A SWO pin is not the end of the journey, but the beginning.
3. Take bold actions aligned to the goals and values. A few examples at the"corporate" level:

    - Continue realigning the training pipeline to focus on these issues, strengthening check points to make sure individuals have the necessary proficiency before moving on. And don't leave leadership training out of the equation; that also is a skill that requires a learning environment.
    - Institutionalize crew endurance and fatigue mitigation policies into the SWOS training curriculum, starting at basic officer indoctrination through command, focusing on the science and operational advantages. Taking care of sailors' health—including the CO— is a warfighting necessity.
    - Incentivize formal, broad sharing of near misses and lessons learned, even if they're painful. Eliminate the practice of "sanitizing" and redacting the reports and remove immediate superior in command endorsements; this fosters the mentality that mistakes are something to be ashamed of. As a junior officer (JO), I was part of a relatively famous nuclear "incident report"—everybody figured out it was me and I was able to share my story as a learning point, and at least one peer thanked me years later for saving his career because he almost did the same thing as I did way back them—it was my mistake, I owned it, and he learned from it.
    - Align the weapons and tactics instructor (WTI) process with the Plans and Tactics Officer (PTO) program, similar to how the aviation squadrons utilize the "Super JO," and reward those who follow that path at selection boards.
    - Open more junior command opportunities. Make sure they are not seen as "too risky" by allowing room to make mistakes and learn. There is a famous story of Admiral Nimitz running a ship aground and still moving on to lead a fleet. It always finishes with, "That could never happen today." Why not? The Navy should examine the reasons for this cultural change.
    - Continue the plan to expand and enhance the Afloat Culture Workshop to gage progress of culture change. Currently, the report is completely "inside the lifelines" and depends on the CO's initiative to act on their recommendations. This is a good thing, but imagine what could be learned by pulling the teams together for an annual "culture health check" with Navy leaders!
    - Identify and weed out toxic leaders. I don't need to name names, but the "SWO's Eat their Young" mantra is not yet in our wake. Every 0-6 whose name popped into to the reader's mind just now was known to act in a toxic way in 0-5 command or as a department head—just ask their peers or former bosses. A positive culture will not tolerate this in the future.
    - When a CO is fired, share the basic facts – "loss of confidence" does not help anyone learn from the mistakes of others. If a CO's actions result in them being relieved

of command, they have forfeited the right to complete privacy as to why.

Individual actions at the senior level could include:

- Require flag officers to visit one ship or squadron each month—just to listen—regardless of their geographic location or position. Keep track.
- Find time in the schedule for "CO's time" under way and empower the CO to use that session as he or she sees fit. Resist the urge to require a report on what they did out there.
- Expand the sabbatical program to allow a better balance a family and career. Most senior officers retire at a pretty young age anyways, so a couple years to recharge could pay huge returns. This policy is also likely to help keep female officers in for a career.

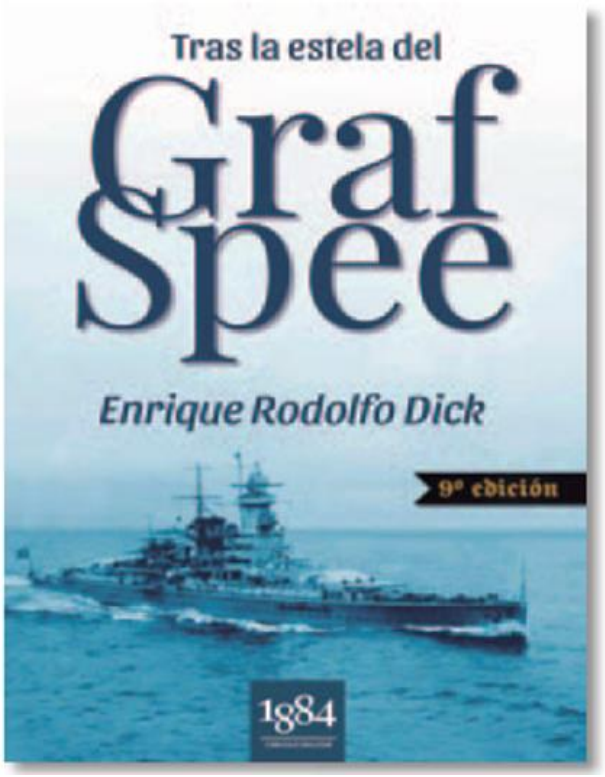
At the individual deckplate level, empower and support sailors to try new ideas without being afraid to fail, and promote them when they succeed. The best solution to your toughest problem may reside in the chief petty officer mess or on the mess decks—they are just waiting to be asked.

Back to the title—Is there a SWO culture? Unequivocally yes. But culture is more than words in a dictionary. It is a set of shared experiences by a group of people that no one else can understand unless they belong to that group. It's a personal connection with generations of seafaring mariners. It's watching the sun come up over the horizon like it only does at sea; it's jumping in for a swim call, knowing that the nearest land is thousands of miles away. It's feeling the salt spray in your face as four 25,000 horsepower engines accelerate a 10,000-ton ship to approach within 100 feet of an oiler for an underway replenishment—without batting an eye. It's the excitement of sailing into a new harbor at sunrise as an ambassador of peace and goodwill, but also with the unmistakable message of brute strength. It is the camaraderie that only the members of a fire attack team can experience in a smoke-filled space, or by the bridge team on a starry midwatch. These are the things that make surface warfare unique and these are the things that will bind us together in a culture of excellence going forward. I am immensely proud of the SWO community; its values, goals, and actions endowed me with a life well spent and a satisfaction second to none.

Culture describes a group, but a group is made up of individuals, so the responsibility for a change in culture rests equally on your shoulders, regardless of what insignia is attached to them. Surface warfare is at the core of the Navy—it is not a consolation prize. It's up to you—when you walk down that pier to work in the morning, don't look down at your shoes—look up at that magnificent warship that is your waterfront office with the best view in town, and appreciate it for the marvel that it is. And when someone asks you what you do for a living, embrace your culture; puff out your chest and say, "I'm surface warfare officer and a Mauna Kea sailor, and I drive ships!

# Libro Recomendado

## Tras la estela del Graf Spee – Novena Edición- 2018




**Formato**: LIBRO

**Autor**: Enrique Rodolfo Dick.

**Idioma**: ESPAÑOL

**Editorial**: 1884, Círculo Militar

**ISBN:** 9789874112194

**Encuadernación:** Tapa blanda

**Número de páginas**: 480

## Reseña del libro

Los lectores habrán de recibir con satisfacción esta nueva edición de una obra que ya podemos llamar clásica. El texto ha conservado el carácter histórico y la sensibilidad de la crónica familiar. La corrección en la escritura y el vuelo literario se mantienen con respecto a ediciones anteriores, y a ello se suma material gráfico sumamente atractivo.

El autor narra con los lineamientos de una novela la vida de su padre, tripulante del Graf Spee. Con rigor histórico y conocimiento de características y de tradiciones marineras, nos ilustra sobre las batallas realizadas por el navío en los albores de la Segunda Guerra Mundial, su hundimiento frente a Montevideo, el suicidio del Capitán Landgsdorff y las peripecias que vivieron sus hombres, internados en la Argentina, convertidos, luego, en prisioneros de guerra, y su regreso a Alemania.

La narración continúa con los últimos años en la Argentina, donde se establece y forma una familia que mantiene su respeto por su antecesor y que recuerda, año a año, la epopeya del acorazado Admiral Graf Spee, el honroso comportamiento de su comandante y el destino de sus tripulantes.

Enrique R. Dick es General del Ejército argentino, posee antecedentes de excelencia en lo profesional, es Magíster en Ingeniería Aeronáutica, Doctor en Historia, académico en el Instituto Nacional Sanmartiniano y miembro del Instituto de Historia Militar y del grupo de Historia Militar de la Academia Nacional de la Historia.

# Escuela de Guerra Naval

## Instituto de Postgrados de la Armada Nacional

# CENTRO DE EDUCACIÓN CONTINUA

- ❑ Negociación II — 5/8 al 9/8
- ❑ Negociación III — 12/8 al 16/8
- ❑ Mediación — 19/8 al 23/8

14 a 17 hs.

Escuela de Guerra Naval
Lido SN esquina Copacabana
esgue@armada.mil.uy

**Militares:** Uniforme de Servicio o Sport Formal
**Civiles:** Sport Formal