UNIVERSIDAD DE LA DEFENSA NACIONAL
FACULTAD DE LA ARMADA
ESCUELA DE GUERRA NAVAL

CURSO DE COMANDO Y ESTADO MAYOR (CUCOM)
ESPECIALIZACIÓN EN CONDUCCIÓN TÁCTICA Y OPERACIONAL NAVAL (ECTON)

TRABAJO INTEGRADOR FINAL

Las operaciones de información en el comando del espacio común marítimo como parte de una estrategia A2/AD.

Autor: CF (ACH) Juan Pablo Castro Brahm

Profesora: Victoria San Martín

Tutor: Juan Battaleme

Lugar y Fecha: Buenos Aires, 29 de octubre de 2021

Resumen

Las operaciones de información han sido estudiadas y aplicadas principalmente en el dominio terrestre de los conflictos armados, siendo la Guerra entre Rusia y Georgia en el año 2008 el primer conflicto bélico en que se reconoció públicamente su utilización. En este conflicto, las fuerzas militares rusas admitieron que, junto con el empleo tradicional de sus medios, realizaron una serie de ciberataques –como parte de las operaciones de información– sobre sistemas e instituciones civiles y militares georgianos, afectando directamente el ciclo de toma de decisiones del adversario. Lo anterior les permitió contar con el tiempo, iniciativa y libertad de acción requerida para triunfar en el conflicto.

Pese a existir principalmente ejemplos históricos de su aplicación en conflictos bélicos terrestres, sus propiedades y características permiten su empleo en la totalidad de los dominios de la guerra y a través de todo el rango de las operaciones militares, en donde se incluye el ciberespacio, el dominio marítimo y su espacio común.

Es en este espacio común -vital para el desarrollo y prosperidad de los Estados y no definido por líneas fronterizas fijas- que las grandes potencias han fijado su interés geopolítico, generando disputas por su comando, control y posterior proyección de fuerzas. De esta forma, los Estados rivereños han debido desarrollar –desde los tiempos en que los griegos se defendieron de la invasión de los ejércitos de Xerses en 480 AC hasta la actualidad– estrategias de antiacceso y negación de área con el propósito de evitar que fuerzas adversarias progresen hacia territorio propio.

El presente trabajo tiene como objetivo general proponer potenciales aplicaciones de las operaciones de información en el comando del espacio común marítimo como parte de una estrategia de antiacceso y negación de área. Lo anterior, tiene como resultado el cumplimiento de la hipótesis investigativa, sustentado en que al ser el espacio común marítimo un área de disputa vital entre Estados, las operaciones de información pueden ser aplicadas como parte de la estrategia de A2/AD para aumentar la capacidad de control y defensa en dicho espacio, por medio de la realización de ciberoperaciones como fuegos operacionales no letales.

Palabras Claves: Operaciones de información; capacidades relacionadas con la información; ciberoperaciones; espacio común; antiacceso y negación de área.

Contenido

Listado de Tablas

Listado de Figuras

Listado de acrónimos y abreviaturas

A2/AD : *Anti-Access/Area Denial*.

CGE : Condición Geográfica Esencial.

CSG : *Carrier Strike Group.*

CO : *Cyber Space Operations*.

COA : *Course of Action*.

C3 : *Command, Control and Communications*.

DIME : *Diplomatic, Information, Military, and Economic.*

DoD : *Department of Defense*.

EFD : Estado Final Deseado.

EMP : *Electromagnetic Pulse.*

FE : *Fires Element.*

FF.AA. : Fuerzas Armadas.

GPS : *Global Positioning System*.

IEEE : Instituto Español de Estudios Estratégicos.

IO : *Information Operations.*

IP : *Internet Protocol*.

IRC : *Information Related Capabilities*.

JP : *Joint Publication.*

LCM : Línea de Comunicaciones Marítimas.

LOE : *Line of Effort.*

LOO : *Line of Operations.*

MIDFIELD : Military, Informational, Diplomatic, Financial, Intelligence, Economic, Law, and Development.

MOC : Maritime Operation Center.

NWC : *Naval War College*.

OODA : Observe, Orient, Decide and Act.

OE : *Operational Environment.*

OPP : *Operational Planning Process*.

TA : *Target Audience.*

TAA : *Target Audience Analysis.*

USMC : *United States Marine Corps*.

USNAVY : *United States Navy*.

ZEE : Zona Económica Exclusiva.

Introducción

El presente trabajo investigativo trata sobre cómo aplicar las operaciones de información en el comando del espacio común marítimo como parte de una estrategia A2/AD. Lo anterior, en atención a la vital importancia que tiene para los Estados –y, también para actores regulares y no regulares– en términos de desarrollo y prosperidad, el poder acceder y controlar los espacios comunes, y, por sobre todo, al espacio común marítimo. Esto, en atención a la gran cantidad de recursos minerales e ictícolas que posee, y, también, a la conectividad requerida en la actualidad, tanto en términos económicos, sociales y financieros –desarrollada por medio del uso del ciberespacio a través de cables de fibra óptica que recorren los océanos–, como lo proporcionado por sus líneas de comunicaciones para el transporte marítimo y proyección de fuerzas militares en todo el mundo. Esta dependencia entre el espacio común marítimo y el ciberespacio, hace que las operaciones de información tomen un rol preponderante en la aplicación de sus capacidades relacionadas, para de esta manera poder acceder y controlar los espacios comunes marítimos como parte de la estrategia A2/AD.

Por otra parte, la relevancia de la presente investigación radica en el poder e influencia que tiene la información y sus capacidades relacionadas durante el proceso de toma de decisiones. En un escenario globalizado, la oportunidad de manipular y acceder a la información se manifiesta desde el momento en que ésta fue creada, almacenada, transmitida y modificada, hasta el instante en que es recibida y procesada por diversas organizaciones, afectando en tiempo real al proceso de toma de decisiones de un adversario o probable adversario. Adicionalmente, los resultados del presente trabajo de investigación permiten integrar conceptos y contenidos de asignaturas impartidas durante el desarrollo del Curso de Comando y Estado Mayor (CUCOM), tales como Relaciones Internacionales, Evolución del Pensamiento Naval, Arte Operacional en el Mar, Planificación de Operaciones Navales y Conducción de Fuerzas Navales.

De esta manera, la pregunta investigativa establecida para el cumplimiento de los objetivos planteados es ¿Cómo pueden ser aplicadas las operaciones de información en el comando del espacio común marítimo como parte de una estrategia A2/NA? Para responderla, se utiliza una metodología de investigación de tipo bibliográfica, mediante el análisis de información que se ha escrito al respecto, tanto en fuentes primarias como secundarias, empleando principalmente para ello publicaciones y reglamentos empleados

por las fuerzas armadas de Estados Unidos y libros y artículos escritos por diversos autores.

El objetivo general de la presente investigación es proponer potenciales aplicaciones de las operaciones de información en el comando del espacio común marítimo como parte de una estrategia A2/NA, siendo cuatro sus objetivos específicos, a saber: analizar el concepto de empleo de las operaciones de información en el desarrollo de las operaciones militares; describir las características específicas de los espacios comunes marítimos con relación a su empleo y control; definir las principales formas de utilizar la estrategia A2/AD para defender los espacios comunes marítimos; y determinar la aplicabilidad de las operaciones de información para el comando del espacio común marítimo. Asimismo, se plantea como supuesto investigativo que, siendo el espacio común marítimo un área de disputa donde la soberanía de un Estado puede verse afectada, las operaciones de información pueden ser aplicadas como parte de la estrategia de A2/AD para aumentar la capacidad de control y defensa en dicho espacio, por medio de la realización de ciberoperaciones como fuegos operacionales no letales.

De esta manera, el trabajo investigativo se desarrolla en tres capítulos. En el primero de ellos, se conceptualizan los espacios comunes y se analiza especialmente al espacio común marítimo, abarcando desde su importancia para el desarrollo de los Estados hasta lo relacionado a su comando y a lo requerido para su empleo y control. También, da a conocer la adaptación de las estrategias de A2/AD que las grandes potencias han debido realizar para poder acceder, emplear y controlar el espacio común marítimo. Finalmente, alude al ciberespacio como espacio común, describiendo en forma detallada sus características, formas de empleo, importancia y diferencias con los otros espacios comunes.

En el capítulo dos, se aborda la estrategia de A2/AD para la defensa de los espacios comunes marítimos, describiendo la forma en que ha sido aplicada desde sus orígenes, hasta cómo las principales potencias del mundo la implementan en la actualidad. Asimismo, se analiza cómo las acciones de A2/AD realizadas en el ciberespacio complementan la estrategia de antiacceso y negación de área ejecutada en el mar.

Finalmente, en el capítulo tres se analizan las operaciones de información, desde su conceptualización hasta cómo se relacionan con el proceso de toma de decisiones y la forma en que los comandantes las integran –por medio de sus capacidades

relacionadas– en el arte y diseño operacional para el cumplimiento de los objetivos de las campañas militares. Del mismo modo, se analizan a las ciberoperaciones como herramienta de las operaciones de información, ya que en base a sus características y efectos se pueden emplear como fuegos operacionales no letales para afectar el ciberespacio adversario. A su vez, se determina la aplicación de las operaciones de información en el comando del espacio común marítimo como parte de la estrategia A2/AD.

Capítulo 1: Empleo y control de los espacios comunes marítimos

Este capítulo aborda principalmente lo relacionado al espacio común marítimo y sus características, comenzando con la definición y luego con la conceptualización de los espacios comunes. Posteriormente, analiza en detalle al espacio común marítimo, haciendo hincapié en la vital importancia que tiene para los Estados, en términos de desarrollo y prosperidad. Luego, describe lo relacionado al comando del espacio común marítimo, referente a lo requerido para su empleo y control, así como también las dependencias que genera. Al mismo tiempo, manifiesta cómo las grandes potencias han adaptado sus estrategias para contrarrestar las amenazas surgidas sobre este espacio. Finalmente, alude al ciberespacio como espacio común, detallando sus características, formas de empleo, importancia y diferencias con los otros espacios comunes.

1.1 Los espacios comunes

Previo a comenzar con la descripción de los espacios comunes marítimos, es conveniente precisar el concepto de espacio común. Según lo señalado por Alexander Kutt en su artículo publicado por el Instituto Español de Estudios Estratégicos (IEEE), se define espacio común –*global commons*– desde el punto de vista del derecho internacional, como “aquellos espacios que no forman parte de ningún Estado concreto y sobre los que, por tanto, ningún Estado puede ejercer derechos soberanos” (Kutt, 2015, pág. 4), pudiendo ser utilizado por cualquier tipo de entidad pública o privada y también por cualquier Estado.

De la misma manera, en el sitio web *Global Commons Alliance* se señala que existen dos definiciones para el concepto de espacios comunes, estando ellas orientadas en términos geopolíticos y económicos. La primera, está relacionada a los recursos económicos potenciales que se encuentran más allá de la jurisdicción nacional, y la segunda, con cómo los recursos compartidos pueden ser utilizados en exceso por algunos actores a expensas de otros, independientemente de la jurisdicción nacional (Global Commons Alliance, 2021).

No obstante las distintas definiciones sobre los espacios comunes, su acceso y empleo resultan vitales en términos económicos y militares para las grandes potencias –como también para todos los actores que se beneficien de ellos– ya que por medio del control de dichos espacios los grandes Estados pueden mantener su influencia en la economía global, en la política internacional y en las rutas de transporte. Por consiguiente, para las

grandes potencias resulta imperativo acceder, dominar y emplear, así como negar su acceso y utilización de estos espacios comunes a un adversario o potencial adversario. De esta manera, tal como lo indica Kutt, “resulta evidente que cualquier enfrentamiento que se produzca en un futuro deberá desarrollarse necesariamente y de manera primordial en el ámbito de los espacios comunes, dado que es precisamente en el dominio de estos espacios donde residen los fundamentos de la hegemonía internacional” (2015, pág. 4).

Para finalizar, cabe destacar lo señalado por Hasim Turker en su artículo denominado *New Cold War at Global Commons: A New U.S. Naval Strategy for the Great Power Competition Era,* publicado en el sitio web *The Geopolitics*, en relación a que estos espacios involucran a los océanos, el espacio exterior y el ciberespacio, destacando entre ellos a los océanos como primus inter pares (2021).

1.2 El espacio común marítimo

Los espacios marítimos han jugado un rol preponderante en el desarrollo y prosperidad de la humanidad. Los océanos y mares siempre han sido un espacio común en donde las civilizaciones, comunidades, actores estatales y no estatales han competido por su acceso y control debido a la importancia estratégica que poseen.

La importancia del espacio común marítimo radica principalmente en la gran diversidad de recursos naturales y minerales que yacen bajos sus aguas y su lecho marino, así como por ser la principal vía de transporte de mercancías y de carga entre los diferentes mercados globales. De la misma forma, es vital para materializar la conectividad global requerida en la actualidad, ya sea de personas o de data. Prueba de ello es lo referido en la estrategia marítima conjunta de Estados Unidos, la que incorporando a la Armada, Guardia Costera e Infantería de Marina, pone de manifiesto que el 90% del comercio mundial se realiza vía marítima y el 95% de las comunicaciones internacionales se lleva a cabo mediante el uso de cables submarinos, facilitando $5.4 trillones de dólares del comercio anual y $10 trillones de dólares en transacciones financieras por día (United States Navy, 2020, pág. 3).

La imagen que a continuación se presenta permite dimensionar lo enunciado en el párrafo precedente en relación al comercio y tráfico marítimo. Esta imagen se obtuvo del portal *Marine Traffic*, sitio web que permite obtener en tiempo real la cantidad de embarcaciones que se encuentran navegando alrededor del mundo.

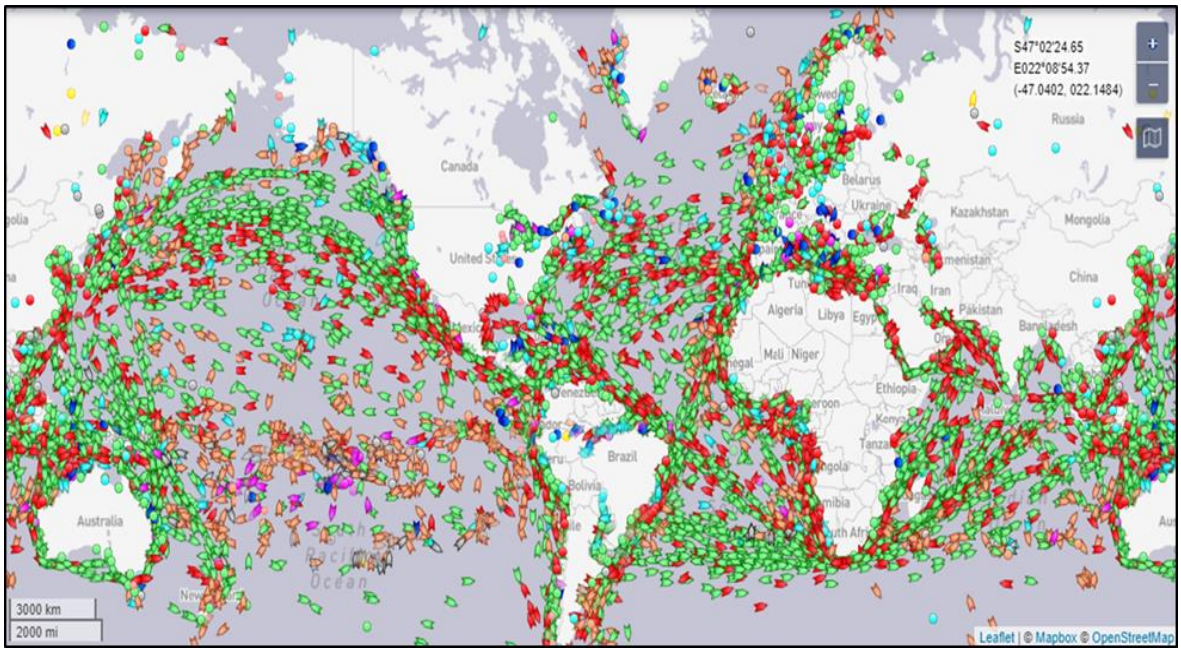

Figura 1: Tráfico marítimo mundial. Fuente: www.marinetraffic.com

Del mismo modo, la siguiente imagen obtenida del portal *Submarine Cable Map* permite cuantificar la totalidad de cables submarinos que existen en la actualidad, así como también los que serán instalados en los próximos meses. Este mapa, permite obtener de forma interactiva la información de todos los cables submarinos que hay desplegados en el mundo.

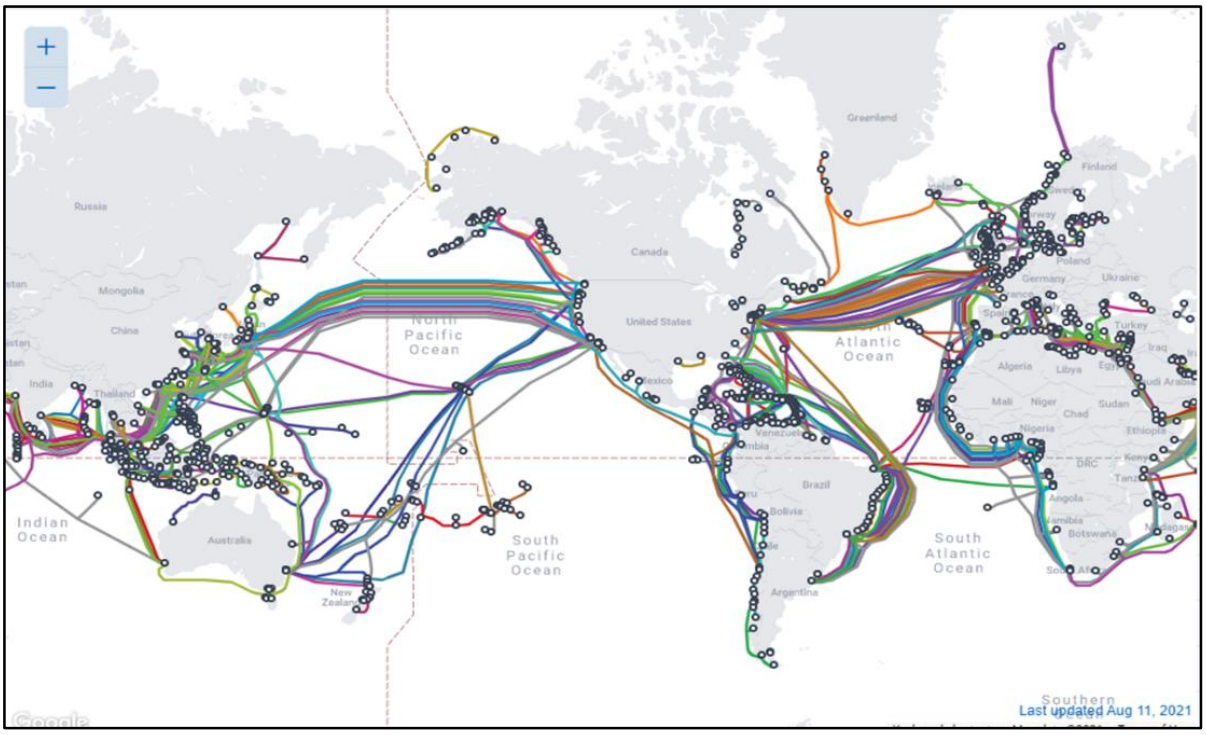

Figura 2: Cables submarinos en la actualidad. Fuente: www.submarinecablemap.com

Lo señalado anteriormente resalta la vital importancia que adquiere para las grandes potencias o para cualquier Estado ser capaz de acceder y emplear los espacios marítimos comunes en beneficio propio, independientemente de la condición geográfica esencial[1] que éstos posean o del poder que ostenten como potencia. De esta manera, es en este espacio común –no definido por líneas fronterizas fijas, rico en recursos naturales y vital para el comercio y conectividad mundial– donde las grandes potencias han fijado su interés geopolítico, generando disputas por su comando, control y posterior proyección de fuerzas.

Merece la pena subrayar lo que sostiene Kutt en relación a que Estados Unidos reconoce que gracias al dominio y control que ejercen sobre los espacios comunes, sobre todo del marítimo, han podido obtener la libertad de acción necesaria en varios teatros de operaciones de forma simultánea. De esta manera, han sido capaces de desplegar sus fuerzas terrestres en cualquier escenario mundial y dotarse de bases navales en las costas de todos los océanos (2015, pág. 7).

1.3 Comando del espacio común marítimo y la estrategia *all domain access*

Del análisis del artículo *The Command of the Commons* (Posen, 2003, págs. 5-6), se puede interpretar que el comando de los espacios marítimos es ejercido por el Estado o actor que posea el control del mar. A su vez, que dicho comando no significa que otros Estados o actores no puedan utilizar estos espacios en tiempos de paz, ni tampoco desarrollar fuerzas que los protejan, o, incluso, explotar sus recursos. Por el contrario, el comando del espacio común marítimo se relaciona con el hecho de que quien lo posea –junto con los otros espacios comunes– lo utiliza militarmente a su favor. Asimismo, significa que quien ostente este control puede amenazar y disuadir en forma creíble a otros actores o Estados para que no lo utilicen e, incluso, hacerles tomar conciencia de que en caso de disputar dicho comando y los recursos que existieran en el espacio común marítimo en controversia les significaría enfrentarse en un conflicto armado. De esta forma, el bando perdedor requeriría de un gran esfuerzo para recuperar sus

[1] El Manual de Estrategia de la Academia de Guerra Naval de la Armada de Chile (Solís, 2004, págs. 22-23), establece que la condición geográfica esencial (CGE) señala el grado de dependencia que posee un Estado de las líneas de comunicaciones marítimas (LCM). La determinación de dicho grado resulta de un estudio de los factores político, económico, estratégico y geográfico aglutinado por la influencia de las LCM. De esta manera, se identifican las siguientes CGE: Insular (depende de modo vital de las LCM), Bloque Continental (no depende de las LCM) y Marítimo Continental (depende parcialmente de las LCM).

capacidades perdidas en el conflicto, mientras que las fuerzas vencedoras preservarían y consolidarían el control del espacio marítimo en disputa después del combate.

De igual forma, Posen plantea que el Estado u actor que ejerza el comando del espacio común marítimo posee un factor militar clave para el posicionamiento de sus fuerzas y proyección de su poder en todo el mundo. Asimismo, debilita a sus adversarios al negarles el acceso a recursos naturales y líneas de comunicaciones marítimas (LCM), permitiéndole a quien comande desarrollar y explotar otras fuentes de poder propias, así como también el poder económico y militar de sus aliados.

Lo señalado en los párrafos precedentes tiene relación con lo escrito por Juan Battaleme en su artículo *Cambiando el statu quo de la Geopolítica Internacional: el acceso a los espacios comunes y las estrategias de negación de espacio y antiacceso* (Battaleme, 2015), ya que de dicho artículo se desprende que el comando del espacio común marítimo conlleva la obtención de una ventaja militar con respecto al que no posee dicho control, pudiendo ser aprovechada en beneficio de las fuerzas que ostentan la superioridad durante periodos de conflicto, permitiéndoles hacer uso de este espacio común para proyectar poder por medio de sus fuerzas navales en cualquier región del planeta, controlando su acceso y negando su uso. De la misma manera, da a entender que esta prerrogativa puede ser beneficiosa en tiempos de paz, ya que le permite al Estado al que pertenecen dichas fuerzas, disponer de este espacio común para desarrollar su comercio mediante el uso de las LCM. Al mismo tiempo, sostiene que actores con menores capacidades militares y tecnológicas se ven beneficiados del uso de ese espacio común marítimo, pero a la vez se hacen dependientes de las capacidades militares y tecnológicas de la fuerza más poderosa.

De acuerdo con lo que sostiene Kutt, Estados Unidos se ha mantenido en el tiempo como potencia mundial gracias a su gran desarrollo económico, el cual ha sido posible producto del control y del comando que ha ejercido sobre los espacios comunes: los océanos, el espacio exterior y el ciberespacio. Sin embargo, este autor también señala que pese a que en la actualidad dicho país continúa dominado los espacios marítimos, esta situación podría cambiar debido al auge de nuevas potencias y actores (2015, pág. 3).

A propósito de la irrupción de estos nuevos actores regulares y no regulares y la proliferación y disponibilidad de armamento de largo alcance –con la subsecuente secuela de no poder acceder y emplear de forma ilimitada los océanos del mundo en

tiempos de conflicto– fue que en 2020 Estados Unidos actualizó su estrategia marítima promulgada el año 2015. Esto se entiende, a su vez, porque se podría ver desafiado tanto su rol hegemón en el comando del espacio común marítimo como el balance de poder existente en regiones claves y el orden mundial que hoy se conoce.

Tal como se mencionó en el comienzo del presente capítulo, dicha estrategia marítima conjunta en su última versión incorpora a las tres ramas de la defensa norteamericana que tienen directa relación con el mar. Lo anterior, a fin de enfrentar esta nueva amenaza con el máximo de sus capacidades navales, aeronavales, marítimas y de infantería de marina, generando un poder naval integrado capaz de operar y acceder a todos los dominios de la guerra[2] a través de los océanos del mundo, asegurando de esta manera el comando del espacio común marítimo. Lo referido anteriormente –sobre el propósito de la estrategia marítima norteamericana y a la importancia que tienen los espacios comunes para Estados Unidos– es reforzado por el Reglamento Conjunto de Operaciones Marítimas de las FFAA *Joint Maritime Operations JP 3-32*, la que indica que "debido a que el acceso a los espacios comunes es crítico, esta estrategia introduce una quinta función: acceso a todos los dominios" (JP 3-32 , 2020, pág. 7).

Esta estrategia marítima de *all domain access* identifica a China y Rusia como las dos principales amenazas para su rol hegemón en el control del mar, ya que ambos intentan ejercer el control sobre los recursos naturales marinos y restringir el acceso a los océanos, repercutiendo negativamente en la seguridad, desarrollo y prosperidad de

[2] Dominios de la guerra: El diccionario de términos militares promulgado por el Departamento de Defensa (DOD) de las fuerzas armadas de Estados Unidos (Department of Defense (DOD), 2018) establece 5 dominios de la guerra, a saber: aéreo, marítimo, terrestre, espacio y ciberespacio.

- Dominio aéreo: La atmósfera, comenzando en la superficie de la Tierra, extendiéndose hasta la altitud donde sus efectos sobre las operaciones se vuelven insignificantes.
- Dominio marítimo: Los océanos, mares, bahías, estuarios, islas, zonas costeras y el espacio aéreo por encima de éstos, incluidos los litorales.
- Dominio terrestre: El área de la superficie de la Tierra que termina en la marca de agua más alta y superponiéndose con el dominio marítimo en el segmento terrestre del litoral
- Dominio espacial: El área por encima de la altitud donde los efectos atmosféricos sobre los objetos en el aire se vuelven insignificantes.
- Ciberespacio: Un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnología de la información y datos residentes, incluida internet, redes de telecomunicaciones, sistemas informáticos y sistemas integrados, procesadores y controladores.

Cabe destacar, que aun cuando el DOD no ha aprobado la promulgación de un sexto dominio de la guerra, existen ciertos autores que sí lo establecen. Dentro de ellos está Lauren Elkins, quien en su artículo denominado *The 6th Warfighting Domain* publicado en el sitio web *Over the Horizon: Multi-Domain Operations & Strategy* define que "el dominio humano es el sexto dominio de la guerra, y será el dominio más decisivo en la guerra del futuro" (Elkins, 2019).

todas las naciones. Entre estos dos actores, se prioriza al país asiático debido a su auge económico, desarrollo de sus capacidades tecnológicas-militares y su actitud agresiva en dominar los espacios marítimos comunes regionales. A su vez, la estrategia marítima norteamericana menciona que China ha implementado una estrategia nacional incompatible con el derecho internacional, junto con "corroer la gobernanza marítima internacional, negar el acceso a los centros logísticos tradicionales, inhibir la libertad de los mares y controlar el uso de chokepoints[3] claves" (United States Navy, 2020, pág. 3).

De la misma manera, la estrategia marítima conjunta de Estados Unidos señala que China ha militarizado las zonas marítimas en disputa y subsidiado estatalmente a su flota pesquera, la que depreda y extrae los recursos ictícolas vitales de aquellas naciones que son incapaces de defender sus propias Zonas Económicas Exclusivas (ZEE). Es por esto, que junto con desarrollar una fuerza naval moderna y balanceada capaz de operar y establecer superioridad en todos los dominios de la guerra, establece como factor clave la formación de alianzas y coaliciones para controlar los espacios marítimos en conflicto. De esta forma, obtener la libertad de maniobra necesaria para atacar a las fuerzas adversarias y "defender a los aliados de la agresión y contrarrestar la coerción y la subversión" (pág. 9). Lo señalado anteriormente, ratifica lo señalado por Battaleme en relación a la dependencia militar y tecnológica que el actor más débil requiere generar con el otro actor de mayor poder para poder proteger sus intereses vitales que se ven amenazados.

Así como la estrategia marítima *all domain access* de Estados Unidos refiere a la competición que existe entre actores estatales por controlar los espacios marítimos comunes para acceder a los recursos naturales, minerales e ictícolas que poseen dichos Estados, también se refiere al uso que le han dado los actores no estatales a las áreas marítimas. En ella, enfatiza que "los extremistas violentos y las organizaciones criminales aprovechan la debilidad de la gobernanza en el mar, la corrupción en tierra y los vacíos

[3] Chokepoint: Según el sitio web *Marine Insight*, el término *chokepoint* – también denominado *cuello de botella* – se refiere a un punto de congestión natural a lo largo de dos pasajes navegables más amplios e importantes, los que por ser canales de transporte naturalmente estrechos tienen un alto tráfico marítimo debido a sus ubicaciones estratégicas. Este portal web establece los siguiente chokepoints como los más importantes del mundo: Estrecho de Málaca, Golfo de Hormuz, Canal de Suez, Canal de Panamá, Estrecho del Bósforo, los tres estrechos daneses que unen el mar Báltico con el mar del Norte y el Estrecho de Bab el-Mandeb (Marine Insight, 2019).
Relacionando la importancia del control de los espacios marítimos comunes con los *chokepoints*, la publicación conjunta JP 3-32 *Joint Maritime Operations*, indica que los adversarios pueden intentar controlar el uso de estos *cuellos de botellas* "restringiendo el acceso o interrumpiendo el paso de las fuerzas navales amigas o la navegación mercante" (U.S Joint Staff, págs. I-5).

en la conciencia del dominio marítimo" (United States Navy, 2020, pág. 5) dejando a los Estados vulnerables a la coerción generada por la piratería, el tráfico de drogas, la trata de personas y otros actos ilícitos. De esta forma, y, con el propósito de evitar que fuerzas regulares o irregulares adversarias accedan y empleen a su favor estos espacios marítimos comunes, los Estados ribereños han debido desarrollar estrategias de antiacceso y negación de área (A2/AD) que abarquen todos los espacios comunes, incluyendo aquellas medidas que protejan contra las amenazas que se desarrollan en el ciberespacio.

1.1 El ciberespacio como espacio común.

El ciberespacio es definido por Alison Russell –en su libro *Strategic A2/AD in Cyberspace*– como "la red de comunicaciones moderna que sustenta el intercambio y los servicios de información global… refuerza el orden económico global y es esencial para todos los elementos del poder nacional[4]" (Russell, 2017, pág. 1). Asimismo, dicho autor manifiesta que el ciberespacio está presente en muchos lugares y situaciones, siendo mucho más grande y complejo que el internet por sí solo, dando la impresión de que está en todas partes. De la misma forma, Russell sostiene que el ciberespacio puede ser utilizado en todos los aspectos, pasando de un empleo cotidiano en la vida diaria de las personas, a ser utilizado por fuerzas militares o paramilitares para el desarrollo de sus operaciones.

Como se mencionó en el comienzo del presente capítulo, el ciberespacio está comprendido –según lo señalado en el artículo escrito por Turker (2021)– dentro de la definición del concepto de espacios comunes y, como tal, es un espacio que no está bajo la soberanía de ningún Estado en particular. De igual forma, también puede ser empleado por cualquier tipo de entidad y actor, siendo éstas instituciones públicas, privadas, militares y dichos actores regulares o irregulares. Asimismo, cabe destacar la vital importancia que tiene el ciberespacio como principal espacio común disponible en

[4] Los instrumentos del poder nacional –conocidos también por la sigla DIME– son el conjunto de instrumentos con que cuenta un Estado para el logro de sus objetivos políticos y estratégicos. Estos instrumentos son diplomático, información, militar y económico. Sin embargo, tal como lo indica la publicación de estrategia conjunta de las FFAA de Estados Unidos *Strategy*, en la actualidad estos elementos del poder nacional han sido complementados con una gama más amplia de opciones que le otorgan mayores alternativas de fuentes de poder a los Estados, siendo estos el informativo, financiero, inteligencia, legal y desarrollo. De esta forma, la nueva sigla que incorpora todos los elementos del poder nacional en la actualidad se conoce como MIDFIELD (militar, informativo, diplomático, financiero, de inteligencia, económico, legal y de desarrollo) (Joint Chieff of the Staff, 2018, págs. 1-17).

la actualidad, tanto para el establecimiento de la comunicación y traspaso de información internacional como para la ejecución de transacciones financieras a nivel global.

De esta manera, el ciberespacio al poseer características propias de suma importancia, y, a su vez, presentar características similares a los otros espacios comunes –ambas vitales para el desarrollo y prosperidad de los Estados– también está sujeto a la competencia de las grandes potencias del mundo por su control y comando. De esta manera, según lo expresado por Kutt en su artículo publicado por el IEEE “el país que consiga controlar el ciberespacio comandará también sobre el resto de global commons” (2015, pág. 18). Ejemplo de lo anterior es lo indicado por la estrategia marítima conjunta de Estados Unidos, la que sostiene que Rusia en caso de un conflicto puede amenazar con ataques cibernéticos contra las principales capitales del mundo o atacar los cables de comunicaciones submarinos, repercutiendo severamente en la economía global (United States Navy, 2020, pág. 4).

Sin embargo, a pesar de las similitudes existentes entre el ciberespacio con los otros espacios comunes –señalado en los párrafos precedentes– Russell plantea que el ciberespacio difiere de los otros dominios de la guerra en tres aspectos. El primero de ellos, es que el ciberespacio fue creado por humanos y dejará de existir y funcionar cuando éstos dejen de interactuar y de mantener, mientras que los otros dominios podrían existir sin la acción humana. El segundo, guarda relación con que el ciberespacio atraviesa e interactúa directamente con los otros dominios, mientras que los otros interaccionan entre sí, pero sin alcanzar una dependencia entre ellos. Finalmente, el tercer aspecto compara los aspectos geográficos de los dominios, en donde el ciberespacio se diferencia del resto, ya que la topografía del ciberespacio cambia y se modifica constantemente por la interacción humana, siendo especialmente difícil protegerse y defenderse de los ataques (Russell, pág. 2).

Como conclusiones del presente capítulo, se puede señalar que los espacios comunes son las áreas que involucran a los océanos, el espacio exterior y el ciberespacio que no están bajo la soberanía de ningún estado en particular, siendo vital para los Estados emplearlos en términos económicos y militares. Asimismo, se pudo determinar que la importancia del espacio común marítimo radica en los recursos naturales que posee y porque permite desarrollar el comercio y la conectividad global. También, se estableció que el comando de los espacios comunes marítimos es ejercido por el Estado o actor que posea el control del mar, pudiendo también ser utilizado en beneficio de otros

Estados o actores de menor poder. De la misma manera, se demostró que Estados Unidos –ante la irrupción de nuevas amenazas– aumentó sus capacidades militares al promulgar una estrategia de defensa conjunta, permitiéndole acceder y operar en todos los dominios de la guerra y asegurar el control y comando del espacio común marítimo. Finalmente, se pudo determinar que el ciberespacio –como espacio común– es esencial para el funcionamiento de los Estados y que posee tanto características similares como también distintas a los otros espacios comunes.

Capítulo 2: Las estrategias de Antiacceso y Negación de Área para la defensa de los espacios comunes marítimos

El presente capítulo aborda la estrategia de A2/AD para la defensa de los espacios comunes marítimos, comenzando la conceptualización histórica del A2/AD y luego con su definición actual, analizando también los conceptos que la componen, describiendo sus ventajas y limitaciones, así como también, los elementos que la caracterizan. Luego, se describe cómo las principales potencias del mundo aplican y contrarrestan la estrategia de A2/AD en defensa de estos espacios. Finalmente, se analiza la forma en que la estrategia de A2/AD –realizada en el ciberespacio– complementa las acciones de antiacceso y negación de área ejecutadas en el mar.

2.1 Conceptualización de la estrategia antiacceso y negación de área

La estrategia de antiacceso y negación de área –conocido en la actualidad con el acrónimo A2/AD por sus siglas en inglés– ha sido empleada desde los principios de la humanidad, siendo su primer registro escrito de utilización lo realizado por los griegos para evitar la invasión de su territorio por parte del emperador persa Xerxes en el año 480 AC. Según lo mencionado por Alison Russel en su libro *Strategic A2/AD in Cyberspace* (2017), las fuerzas invasoras persas superaban ampliamente en número y medios a las griegas, por lo que para derrotarlas, los helénicos utilizaron la estrategia de antiacceso y negación de área mediante el empleo integrado de sus fuerzas navales junto con sus islas como barreras naturales y *chokepoints*. De esta forma, destruyeron y neutralizaron a las unidades que proveerían de suministros logísticos a las fuerzas del gran ejército de Xerxes antes de alcanzar las costas griegas, obligando a las fuerzas terrestres persas que amenazaban con invadir Grecia a retirarse del área en disputa. Por consiguiente, tal como lo expresa Russel “el poder de la estrategia antiacceso le permitió a la fuerza más débil evitar que la fuerza más poderosa utilizara sus recursos en el teatro de operaciones“ (pág. 11).

Del mismo modo al propósito buscado por los griegos casi 500 años AC, la concepción moderna de la estrategia A2/AD está orientada a negarle a un adversario la capacidad de acceder y llevar sus capacidades operativas a una región en disputa, y, a su vez, evitar que el atacante opere libremente dentro de esta área y maximice sus capacidades. Es decir, el propósito de la estrategia A2/AD es “negarle al adversario la capacidad de entrar al área y maniobrar libremente dentro del espacio de batalla” (pág. 3).

Relacionado a la definición actual de la estrategia A2/AD, Dave Shunk en su artículo *Area Denial & Falklands War Lessons Learned*, escrito en la revista *Small Wars Journal* (Shunk, Small Wars Journal, 2014), menciona al conflicto de Malvinas como la primera guerra moderna en donde se utilizó esta estrategia. Shunk señala que la Fuerza Aérea Argentina desencadenó su plan de denegación de área al concentrar su ataque sobre las unidades de superficie –tanto de combate como transportes de tropas y elementos logísticos– que se encontraban en la Bahía de San Carlos, por sobre las fuerzas terrestres ya desembarcadas. Así, combinando en sus tácticas el ataque de aeronaves de combate –equipadas con misiles anti-superficie Exocett AM-39 y bombas convencionales– junto con el ocultamiento brindado por la geografía, las FFAA argentinas repercutieron directamente en el tempo[5] de las operaciones que se habían previsto para las fuerzas terrestres británicas. Merece la pena subrayar lo referido por Shunk en relación al ataque al buque de transporte *Atlantic Conveyor*, ya que su pérdida afectó la flexibilidad estratégica e "interrumpió totalmente la campaña de las fuerzas terrestres británicas". De esta manera, por medio del ejemplo del conflicto de Malvinas, se puede demostrar que desde los tiempos en que los griegos defendieron su territorio de una invasión se ha mantenido como tendencia[6] en la estrategia A2/AD, la modernización de las capacidades tecnológicas y militares utilizadas por las fuerzas, tanto en su precisión, alcance y letalidad. Asimismo, ha sido constante[7] en el tiempo, por parte del bando más débil, el uso de la geografía a su favor como también el ataque sobre los medios de transporte logísticos que apoyan al desarrollo de las operaciones de la fuerza de mayor poder militar.

La estrategia A2/AD –como su acrónimo bien lo señala– está compuesta de dos conceptos, que, si bien son distintos, son complementarios entre sí: antiacceso y negación de área. De acuerdo a lo planteado por Russel, el primero de ellos se refiere a

[5] Tempo es el ritmo de la acción militar. Controlar o alterar el ritmo es necesario para retener la iniciativa. El comandante operacional ajusta el tempo para maximizar las capacidades propias. El tempo tiene significado militar sólo en términos relativos. Cuando el tempo sostenido propio excede la habilidad del oponente de reaccionar, las fuerzas propias pueden mantener la iniciativa y tienen una ventaja marcada. Fuente: Módulo 3. Conducción táctica y operacional de fuerzas navales. Asignatura de Arte Operacional en el Mar. Unidad Temática N°9. Escuela de Guerra Naval 2021.

[6] Tendencia: son los factores que cambian de una época a otra en una dirección, y que también pueden deducirse de la historia naval. Son generalmente provocados por las nuevas tecnologías, y se aplican en el mar tanto a nivel operacional como a nivel táctico. Fuente: Módulo 3. Conducción táctica y operacional de fuerzas navales. Asignatura de Conducción de Fuerzas Navales. Unidad Temática N°3. Escuela de Guerra Naval 2021.

[7] Constante: Son los modos operacionales que resultaron más útiles y que se deducen de la historia de las operaciones navales; y permanecen vigentes. Fuente: Módulo 3. Conducción táctica y operacional de fuerzas navales. Asignatura de Conducción de Fuerzas Navales. Unidad Temática N°3. Escuela de Guerra Naval 2021.

la habilidad de acordonar un área y controlar su entrada, negándole efectivamente a un adversario poder acceder a una zona en disputa. Ejemplo de lo anterior es el bloqueo naval, ya que previene que embarcaciones accedan a un área marítima en particular, pero no controla necesariamente el uso que dicha embarcación haga dentro del área. Por su parte, el segundo concepto tiene relación a la habilidad de disminuir, degradar o evitar que el adversario obtenga la libertad de acción necesaria para ejecutar sus operaciones dentro del área en disputa. Una zona de exclusión marítima[8] es un ejemplo, ya que el propósito de su establecimiento es neutralizar a las embarcaciones que ingresen para evitar su accionar en el interior del espacio marítimo controlado. En síntesis, el "antiacceso afecta el movimiento hacia un teatro, mientras que la negación de área afecta el movimiento dentro de un teatro" (pág. 3).

Si bien la estrategia A2/AD es utilizada, generalmente, como método de defensa de una fuerza más débil, esta condición no es excluyente. Sin embargo, al ser defensiva y combinar tanto el uso de la geografía con la tecnología, junto con su implementación alejada del territorio o zona a proteger, permite al actor cuyo poder de combate[9] es menor, a evitar un enfrentamiento directo en contra del bando más poderoso. De esta forma, la ventaja de este tipo de estrategia es que una fuerza no tiene que ser más fuerte que otra para obtener la victoria, sino que tiene que ser lo suficientemente poderoso para evitar que el contendor logre acceder a un área y la utilice a su favor para alcanzar sus objetivos. Del mismo modo, Sam Tangredi indica en su artículo *Antiaccess Warfare as Strategy* –escrito para la revista *Naval War College Review* (2018)–que, a lo largo de la historia, la mayor parte de los Estados o actores que utilizaron la estrategia A2/AD nunca derrotaron a sus oponentes que ostentaban un poder de combate superior "porque los costos parecen demasiado altos cuando un evento u otras preocupaciones de mayor interés ocurren en otra parte" (pág. 6).

De la misma forma que la estrategia A2/AD presenta ventajas, también exhibe limitaciones. Esta refiere a que su utilización exclusiva como método defensivo no permitirá derrotar al bando adversario, sino que solo lo inmovilizará, lo hará abandonar

[8]Zona de exclusión: Definido por el Diccionario de Términos Militares del Departamento de Defensa de las FFAA de Estados Unidos, como una zona establecida por un organismo sancionador para prohibir actividades específicas en un área geográfica específica, con el fin de persuadir a las naciones o grupos de modificar su comportamiento para satisfacer los deseos del organismo sancionador o enfrentar la imposición continua de sanciones, o uso o amenaza de la fuerza (Department of Defense (DOD), 2018, pág. 83).

[9] Poder de combate: Definido como los medios totales de fuerza destructiva y/o disruptiva que una unidad militar puede aplicar contra el oponente en un momento dado (Department of Defense (DOD), 2018, pág. 42)

el área y desistir de su intento. Por consiguiente, para que una fuerza adversaria sea derrotada, es necesario que ocurran en forma simultánea otros eventos fuera de las operaciones propias de antiacceso y negación de área.

En relación a lo anterior, Tangredi plantea que la estrategia A2/AD posee cinco elementos que la caracterizan, de los cuales dos se atañen a los eventos externos que requiere esta estrategia para que su utilización sea efectiva (pág. 4). El primero de ellos, guarda relación a la importancia crítica que tiene el empleo de la información e inteligencia como parte de la estrategia A2/AD, para que por medio de la utilización de ambos, se logre afectar el proceso de toma de decisiones de los líderes adversarios y disuadir en los niveles de conducción estratégico y operacional. El segundo elemento, está relacionado con lo determinante que resultan los eventos extrínsecos que suceden en otras áreas o regiones y que afectan al A2/AD en el área en disputa en particular. Estos eventos, acciones o medidas, pueden ser materializados mediante el empleo de los otros instrumentos del poder nacional, siendo éstos los campos de acción diplomático, económico y de la información.

Los otros tres elementos característicos de la estrategia A2/AD, señalados por Tangredi son: en primer lugar, la importancia de la geografía como elemento preponderante que más influye en el tiempo y facilita el desgaste en combate de las fuerzas del oponente; en segundo lugar, el dominio marítimo como el espacio predominante entre todos los dominios de la guerra en donde se materializa el antiacceso y negación de área; y, en tercer lugar, la percepción de superioridad estratégica del oponente.

2.2 Estrategia de A2/AD en el espacio común marítimo

El dominio marítimo es el espacio en donde confluyen por naturaleza los elementos componentes no externos de la estrategia A2/AD, ya que las características y formaciones geográficas que posee –estrechos, istmos, cadenas de islas, islas desoladas, *chokepoints*, entre otros– favorecen la implementación de medidas antiacceso y de negación de área.

Las estrategias de A2/AD que se realizan en este espacio común –también conocidas según Russel con el nombre de control del mar[10], superioridad marítima[11], de bloqueo y de proyección del poderío naval[12]–, están enfocadas a acceder a los espacios comunes marítimos para hacer uso del mar en beneficio propio y controlar las LCM, negándole esta posibilidad al adversario. Para lograrlo, el sitio web *Missile Defence Advocacy Alliance* señala en su artículo que la componente antiacceso de la estrategia A2/AD utiliza aviones de ataque, buques de guerra y misiles balísticos y de crucero diseñados especialmente para atacar objetivos claves. De la misma manera, indica que la parte negación de área de dicha estrategia emplea medios más defensivos, como los sistemas de defensa aérea y marítima (MDAA, 2018).

Tal como señala Battaleme, "si los 'accesos a' son la clave en el presente siglo, la contracara de ello es el anti-acceso, y su 'socio' la negación de área" (2015, pág. 22). Esta necesidad de acceder y negar los accesos a los espacios comunes marítimos –para de esta manera obtener o impedir la obtención de recursos naturales y vías de conectividad globales vitales para el desarrollo y prosperidad de las grandes potencias– se ve materializado en la actualidad, principalmente, en la relación de competencia que existe entre las estrategias de A2/AD de Estados Unidos y China.

Con respecto a China, el sitio web referenciado anteriormente destaca que dicho Estado "ha emergido como una potencia regional asertiva en el Asia-Pacífico con poderosas capacidades A2/AD", disuadiendo a Estados Unidos por medio de su capacidad de misiles balísticos y de crucero, junto con sistemas de defensa aérea y marítima. Estos sistemas de defensa de última tecnología, se encuentran emplazados haciendo uso de las características geográficas de la región en disputa, concentrándose en las cadenas

[10] Control del mar: La condición en la que uno tiene libertad de acción para usar el mar para sus propios fines en áreas específicas y por períodos de tiempo específicos y, cuando sea necesario, para negar o limitar su uso al enemigo. El control del mar incluye el espacio aéreo sobre la superficie y el volumen de agua y el fondo del mar (United States Navy, 2020, pág. 27).
Por otra parte, las operaciones de control del mar son definidas como el empleo de fuerzas para destruir las fuerzas navales enemigas, suprimir el comercio marítimo enemigo, proteger las rutas marítimas vitales y establecer la superioridad militar local en áreas marítimas vitales (Department of Defense (DOD), 2018, pág. 203)

[11] Superioridad marítima: grado de dominio de una fuerza sobre otra que permite la conducción de operaciones marítimas por parte de la primera y sus fuerzas terrestres, marítimas y aéreas relacionadas en un momento y lugar determinados sin interferencia prohibitiva de la fuerza opuesta (United States Navy, 2020, pág. 26).

[12] Proyección del poder naval: Definido por Russel como la capacidad de proyectar el poder naval cualquier parte del mundo, incluso para poder contrarrestar las medidas A2/AD emprendidas por otras fuerzas que quieran restringir el movimiento cerca de las aguas territoriales o, por el contrario, imponer esas condiciones a los adversarios con el fin de limitar su capacidad para utilizar el espectro completo de capacidades (Russell, 2017, pág. 13).

de islas alrededor de Taiwán y el Mar de China Meridional, siendo capaces de alcanzar tanto instalaciones en tierra aposentadas en la región –entre ellas las ubicadas en las islas de Guam y Okinawa– como a los Grupos de Ataque de Portaaviones[13] que intenten acceder a sus espacios marítimos a grandes distancias.

Asimismo, menciona que en cuanto a la componente antiacceso, China se basa en misiles balísticos y de crucero, capaces de atacar objetivos tanto en tierra como en el mar con un alto grado de precisión, y, a su vez, aptos para eludir la mayoría de los sistemas de defensa antimisiles. Estos misiles –cuyos alcances varían entre 1500 y 500 km– pueden ser lanzados por buques de combate, aeronaves de ataque y submarinos. Por su parte, para desarrollar la negación de área, China sustenta su estrategia en el empleo de aviones de combate y una vasta red de plataformas de defensa aérea y de misiles producidos por su industria militar, negándole a Estados Unidos la capacidad de emplear su poder aéreo-marítimo y el uso de sus misiles crucero en la región.

Por su parte –tal como se señaló en el capítulo I– Estados Unidos prioriza en su estrategia marítima conjunta el desafío presentado por China ante el de otros actores. En ella señala que "China es el único rival con el potencial económico y militar combinado para presentar un desafío integral a largo plazo para Estados Unidos" (United States Navy, 2020, pág. 9). De esta manera, dicha estrategia focaliza los esfuerzos y orientaciones de sus FF.AA en generar fuerzas capaces de operar en todos los dominios de la guerra –*all domain access*– para contrarrestar el desafío planteado por China a nivel mundial y fortalecer la disuasión regional en el Indo-Pacífico. Esto queda demostrado cuando declara: "si nuestros adversarios eligen el camino de la guerra, la Armada luchará junto al Ejército, la Fuerza Aérea, la Fuerza Espacial, nuestros aliados y nuestros socios para negar los objetivos del enemigo y destruir las fuerzas enemigas" (pág. 13).

[13] Según el diccionario de terminología militar conjunto de las FFAA de Estados Unidos (Department of Defense (DOD), 2018, pág. 32), un Grupo de Ataque de Portaaviones o *Carrier Strike Group* (CSG) es un grupo de tarea naval permanente que consiste en un portaaviones, un ala aérea embarcada, unidades de combate de superficie y submarinos asignados en apoyo directo, que operan en apoyo mutuo con la tarea de destruir las fuerzas aéreas, de superficie y submarinas hostiles a lo largo de la costa enemiga o proyectar su poder hacia tierra. Según el sitio web de la Fuerza Naval de Superficie de la Flota del Pacífico de la Armada de Estados Unidos ***Fuente especificada no válida.,*** la USNAVY mantiene 11 grupos de ataque de portaaviones, 10 de los cuales están basados en los Estados Unidos y uno está desplegado en Japón. Cada uno de los CSG normalmente constan de 1 portaaviones, 2 cruceros de misiles guiados, 2 buques de guerra antiaéreos y 1-2 destructores o fragatas antisubmarinos.

Para finalizar, cabe destacar que China –según lo planteado por el sitio web *Missile Defence Advocacy Alliance*– continúa con el proceso de mejorar sus capacidades de A2/AD, desarrollando sistemas de armas anti-satélites, capaces de neutralizar la capacidad satelital requerida por los sistemas de armas de las FFAA de Estados Unidos por medio de la interrupción o negación del uso del ciberespacio.

2.3 Estrategia de A2/D2 en el ciberespacio como complemento de las acciones A2/AD para la defensa de los espacios comunes marítimos.

Aun cuando el dominio marítimo es el principal espacio en donde se materializan las acciones relacionadas a la estrategia A2/AD, la interacción directa del ciberespacio con la totalidad de los dominio de la guerra, y, su inclusión dentro de la clasificación de espacio común –por ende no perteneciente a ningún Estado en particular y de libre uso, que sustenta el intercambio y servicios de información global e imprescindible para todos los elementos del poder nacional– hace que resulte imperativo considerar las acciones de antiacceso y negación de área que se ejecutan en el ciberespacio como complemento de las acciones A2/AD que se realizan en el dominio marítimo, para, de esta forma, lograr el comando de sus espacios comunes.

La información y las comunicaciones –que utilizan el ciberespacio como principal medio de propagación– son consideradas actualmente como elementos clave para obtener la victoria o la derrota en un conflicto, ya sea enfocando sus esfuerzos en la obtención de inteligencia, para engañar al adversario o afectar su proceso de toma de decisiones. De este modo, tal como lo señala Russell, “las operaciones de A2/AD en el ciberespacio no buscan manipular la información, sino más bien buscan interrumpir y prevenir el flujo o intercambio de información” (2017, pág. 4).

Según Russel, las operaciones relacionadas a la estrategia A2/AD que se ejecutan en el ciberespacio –denominadas también como *cyber A2/AD*– existen en los niveles estratégicos y tácticos. De esta forma, a las operaciones estratégicas de A2/AD las define como “la habilidad de obtener el control de la red o la infraestructura del ciberespacio y manipularla de tal manera que se niegue a un Estado la habilidad de utilizar el ciberespacio en cualquiera de sus capacidades” (pág. 4). Las *cyber A2/AD* en este nivel, no buscan afectar el funcionamiento de ningún sistema de armas o infraestructura en particular, sino que están orientadas a atacar al adversario negándole al acceso al ciberespacio en su totalidad. Es decir, mediante la ejecución de operaciones estratégicas

de A2/AD, el Estado afectado no tendría la capacidad de emplear sus capacidades asociadas con los instrumentos de su poder nacional que dependan del ciberespacio.

Por otra parte, las operaciones de A2/AD en el nivel táctico "buscan bloquear el acceso a partes específicas del ciberespacio (…) son extraordinariamente importantes porque permiten que un bando evite que el otro use recursos específicos que están conectados al ciberespacio" (pág. 22). De esta manera, y en base a que el ciberespacio posee la característica de atravesar e interactuar con todos los dominios de la guerra, las *cyber A2/AD* que se ejecutan en este nivel están orientadas a complementar las estrategias A2/AD que se desarrollen en la totalidad de los espacios comunes. Ejemplo de lo señalado anteriormente es la realización de acciones tácticas en el ciberespacio, cuyo propósito sea afectar los sistemas posicionamiento global (GPS) de las unidades de combate marítimas, terrestres y aéreas –y, por ende, el funcionamiento de sus sistemas de armas y de comando, control y comunicaciones (C3) – afectando de esta manera en las estrategias de A2/AD que se desarrollen en todos los espacios comunes y dominios de la guerra, entre ellos el espacio común marítimo.

Las operaciones de A2/D2 que se realizan en ciberespacio para la defensa de los espacios comunes, tienen que estar enmarcadas –según lo indicado por Russell– dentro de tres tipos de ataques a realizar. El primero de ellos, los ataques mecánicos, que llevados a cabo principalmente en tiempos de conflicto, incluyen acciones tales como bombardeo sobre centros de mando y control, destrucción de antenas, neutralización de satélites, entre otros. Los segundos, son los ataques realizados dentro del espectro electromagnético[14], incluyéndose entre ellos la emisión de pulsos[15] o interferencias[16] electromagnéticas sobre equipos de C3. Finalmente, el tercer tipo de ataque son los ataques digitales o *cyber attacks*, los que pudiendo ser realizados de numerosas maneras, tienen el propósito de que un equipo o sistema funcione mal o se apague completamente para inhibir el flujo de datos.

[14] Espectro electromagnético: Definido como el rango de frecuencias de radiación electromagnética desde cero hasta el infinito (Department of Defense (DOD), 2018, pág. 75).

[15] Pulso electromagnético (EMP): Definido como la radiación electromagnética generada por un fuerte pulso electrónico con el objeto de producir picos de tensión y corriente dañinos en sistemas eléctricos o electrónicos (Department of Defense (DOD), 2018, pág. 75)

[16] Interferencia electromagnética: la radiación deliberada, la re-radiación o el reflejo de energía electromagnética realizada con el propósito de prevenir o reducir la efectividad de un uso malicioso del espectro electromagnético, y con la intención de degradar o neutralizar el capacidad de combate del enemigo (Department of Defense (DOD), 2018, pág. 75).

Para que los ataques realizados en el ciberespacio –mencionados en el párrafo anterior– logren el efecto deseado mediante la ejecución de acciones de A2/AD, es importante saber identificar dónde realizar dichas acciones. De acuerdo con lo planteado por Russel, el ciberespacio está conformado por cuatro capas que son vulnerables a ser atacadas: la física, la lógica, la de información y la de los usuarios. La capa física, cuyos elementos varían desde satélites, dispositivos inteligentes, computadoras, cables de fibra óptica, entre otros. La capa lógica, la que siendo "el sistema nervioso central del ciberespacio" (pág. 6) se sustenta en los elementos de la capa física y es la responsable de transmitir los paquetes de datos[17] a sus destinos finales, a través de protocolos de internet, navegadores, sitios web y software. La capa de la información –que interactuando con la capa de los usuarios– está compuesta de códigos, textos, fotografías y otros materiales que se almacenan y transmiten por el ciberespacio. Si bien las capas de la información y de los usuarios también son vulnerables a *cyber attacks*, "sería significativamente más difícil lograr efectos estratégicos si es que se realizan ataques digitales sobre estas capas" (pág. 6). De esta manera, para que los ataques realizados en el ciberespacio –como complemento de las acciones A2/AD que se realicen en el espacio común marítimo– produzcan el efecto deseado en el dominio marítimo, deben enfocarse en afectar las capas físicas y lógicas, ya que son "la columna vertebral y el sistema nervioso central del sistema" (pág. 7).

Finalmente, cabe destacar que otra manera que tienen las *cyber A2/AD* de complementar la estrategia de antiacceso y negación de área desarrollada en el espacio común marítimo, tiene relación con el efecto disuasivo que generan las *cyber A2/AD* en el bando adversario. Esto, directamente relacionado con la dependencia que tienen los Estados del ciberespacio, ya que quien posea la capacidad de negar el acceso a este espacio común, amenazaría su economía, seguridad y estabilidad. Así, tal como señala Russel, "una amenaza creíble de esta naturaleza puede ser suficiente para disuadir un conflicto armado o forzar un curso de acción más favorable" (pág. 8).

[17] Un paquete es una unidad básica de comunicación, utilizado para la transmisión de datos a través de una red digital. Cuando los datos tienen que ser transmitidos, se descomponen en estructuras similares de datos antes de la transmisión, llamadas paquetes, que se vuelven a ensamblar al trozo de datos original una vez que llegan a su destino. La estructura de un paquete, depende del tipo de paquete que sea y del protocolo a utilizar. Por ejemplo, la transferencia de datos a través de Internet requiere desglosar los datos en paquetes IP, los que incluyen la dirección IP de las máquinas de origen y de destino de los datos **Fuente especificada no válida.**.

En su libro *Strategic A2/AD in Cyberspace*, Russel plantea que para que la disuasión mediante *cyber A2/AD* sea exitosa debe basarse en tres principios relacionados entre sí: castigo, negación y cooperación. El primero de ellos –disuasión por castigo– "ocurre cuando el actor señala que los costos infligidos en represalia por ser atacado superarían los beneficios potenciales derivados de lanzar un ataque" (pág. 60). De esta manera, el resultado logrado por este tipo de disuasión, va a depender de lo creíble que sea dicho actor de amenazar de realizar acciones ofensivas en el ciberespacio en contra del bando atacante. El segundo principio –disuasión por negación–, se refiere a las capacidades propias que posee un Estado para reducir los efectos ante acciones de *cyber A2/AD* realizados en su contra. Este tipo de disuasión se logra reduciendo sus propias vulnerabilidades de ser atacado y demostrándole al atacante que su probabilidad de éxito en al ataque que intente realizar es bastante baja. Finalmente, el tercer y último principio es la disuasión por cooperación, la que por medio de la generación de lazos e interdependencias entre los bandos, busca prevenir la realización de un ataque digital sobre un Estado en base a la relación costo-beneficio –presentada al oponente– que generaría la concretación de dicha acción.

Como conclusiones del presente capítulo, se puede señalar que la estrategia A2/AD ha sido utilizada desde la antigüedad hasta nuestros tiempos, con el propósito de negarle al adversario la capacidad de entrar a un área específica y maniobrar libremente dentro de ella, empleando para esto la geografía del área en disputa junto a sistemas de armas y de defensa. Asimismo, que para cumplir con ese objetivo, la estrategia A2/AD necesita de otros elementos ajenos a sus acciones y de una fuerza lo suficientemente poderosa –pero no necesariamente más fuerte– que la del adversario. De la misma manera, se pudo determinar que el dominio marítimo es el espacio preponderante para el desarrollo de las acciones de antiacceso y negación de área, y, cómo las grandes potencias del mundo utilizan esta estrategia en la actualidad. Por último, se pudo establecer que las acciones de A2/AD que se desarrollan en el ciberespacio, complementan la estrategia A2/AD realizada en el dominio marítimo para la protección de los espacios comunes.

Capítulo 3: Las operaciones de información y el comando del espacio común marítimo

Este capítulo aborda principalmente a las operaciones de información (IO), comenzando con su definición y las principales características del entorno en donde se desarrollan estas operaciones. Luego, se determina la forma en que se relacionan con el proceso de toma de decisiones y la manera en que afectan a la ejecución del ciclo OODA. A continuación, se analiza cómo se relacionan las IO con la creatividad y visión del comandante –arte operacional– y con la metodología y representación gráfica de las campañas militares –diseño operacional– determinando cuándo y cómo deben aplicarse estas operaciones para el cumplimiento de los objetivos de los comandantes operacionales. Posteriormente, se analizan las ciberoperaciones (CO) como parte de las capacidades relacionadas con la información (IRC), ya que en base a sus características y como herramienta de las IO, pueden ser utilizadas para afectar el ciberespacio. A continuación, se establece que las CO son consideradas fuegos operacionales no letales, y, también, cómo éstas se relacionan con el centro de operaciones marítimas[18] (MOC). Finalmente, se determina cómo pueden ser aplicadas las IO en el comando del espacio común marítimo como parte de la estrategia A2/AD.

3.1 Las operaciones de información

Según lo establecido por Lincoln en su artículo *Cyber Power in 21st Century Joint Warfare* (Lincoln, 2014), la guerra entre Rusia y Georgia ocurrida en 2008 fue el primer conflicto armado en donde se reconoce públicamente el empleo de operaciones de información (IO) y ciberoperaciones en apoyo a las operaciones militares tradicionales. En este conflicto las fuerzas militares rusas –apoyadas por medio de la realización de ciberataques– derrotaron en un corto período de tiempo a las fuerzas georgianas y se apoderaron del territorio en disputa, colapsando los sistemas de C3 de las fuerzas militares adversarias, así como de los sistemas de seguridad de las principales instituciones públicas, privadas y del gobierno georgiano.

[18]MOC: Maritime Operation Center. El MOC es un tipo de organización de un Estado Mayor, flexible, escalable y adaptable al tipo y cantidad de fuerzas y a las características de la misión, conformado por una red de personas, procesos y funciones, que permite conducir el proceso de las operaciones y apoya al comandante en su ciclo de toma de decisiones, creando conocimiento compartido para conducir la ejecución de las operaciones en el nivel operacional.

Las operaciones de información (IO) son definidas por las fuerzas conjuntas de Estados Unidos en su publicación JP 3-13 *Information Operations* (JP 3-13, 2014), como el empleo integrado durante las operaciones militares de las capacidades relacionadas con la información (IRC) junto con otras líneas de operaciones (LOO) con el propósito de influir, perturbar, corromper o usurpar el ciclo de toma de decisiones del adversario y potenciales adversarios, mientras se protege la información propia (pág. ix) .

Este empleo integrado de las IO se lleva a cabo en el denominado ambiente/entorno de la información, el cual siendo transversal a todos los dominios de la guerra, se define como "el conjunto de individuos, organizaciones y sistemas que recopilan, procesan, difunden o actúan sobre la información" (págs. ix,x). A su vez, este entorno está constituido por tres dimensiones interrelacionadas –física, de la información y cognitiva– las que continuamente interactúan con individuos, organizaciones y sistemas.

La publicación JP 3-13, señala que la dimensión física está compuesta por los sistemas de mando y control, líderes tomadores de decisiones e infraestructura que permite a los individuos y organizaciones crear efectos en el ambiente/entorno de la información. Esta dimensión incluye principalmente a las personas, instalaciones de mando y control, periódicos, unidades de procesamiento, computadoras portátiles, teléfonos inteligentes o cualquier otro objeto que esté sujeto a mediciones empíricas (2014, págs. I2-I3).

Asimismo, indica que la dimensión de la información es donde se ejerce el mando y control de las fuerzas militares y donde se transmite la intención del comandante, realizándose de esta forma las actividades de recopilación, procesamiento, almacenamiento, difusión y protección de la información. De esta manera, las acciones ofensivas y defensivas que se lleven a cabo en esta dimensión afectan el contenido y el flujo de información del ciclo de toma de decisiones del comandante.

De la misma manera, la publicación señala que la dimensión cognitiva comprende las mentes de aquellos que transmiten, reciben, responden o actúan sobre la información. Asimismo, hace referencia a cómo esta dimensión afecta al procesamiento de la información y finalmente a la toma de decisiones del grupo o líder de la organización. Estos últimos, se encuentran influenciados por diversos factores, entre ellos: creencias individuales y culturales, normas, vulnerabilidades, motivaciones, emociones, experiencias, moral, educación, salud mental, identidades e ideologías. La definición de estos factores en un entorno o ambiente de la información dado, es fundamental para

comprender cómo influir mejor en la mente del responsable de la toma de decisiones y crear los efectos deseados; de esta forma, “la dimensión cognitiva constituye el componente más importante del entorno de información” (2014, pág. I 3).

3.2 Las operaciones de información en el proceso de toma de decisiones

El proceso de toma de decisiones, también conocido como ciclo OODA, es un concepto que fue desarrollado en la década del 50 por el coronel de la Fuerza Aérea de Estados Unidos John Boyd, quien estableció un ciclo compuesto de cuatro fases, las cuales son: observar, orientar, decidir y actuar (OODA: *observe, orient, decide, act*). A su vez, indicó que este ciclo era aplicable durante el desarrollo de las operaciones de combate en el nivel táctico y también en el nivel operacional durante las campañas militares.

En la actualidad, el Cuerpo de Infantería de Marina de Estados Unidos (USMC) continúa utilizando el ciclo OODA establecido por Boyd para la ejecución de sus operaciones. Así, en el libro *Operational Art*, es indicado como el ciclo de decisión de los comandantes, el cual debe ser completado con anterioridad al del adversario para, de esta forma, cambiar la situación más rápidamente de lo que el enemigo puede seguir o reaccionar.

En la medida en que las nuevas tecnologías de información, sistemas y procedimientos permiten poner a disposición información detallada en todos los niveles de la cadena de mando, los líderes militares deberían comprender cómo estos cambios afectan los procesos de toma de decisiones durante el ciclo OODA. Asimismo, éstos deben esforzarse por obtener un ritmo de toma de decisiones más reflexivo y rápido para poder observar y actuar, ya que “el objetivo de cualquier comandante es aumentar su ritmo de toma de decisiones mientras manipula la toma de decisiones de su adversario” (USMC University, 2016, pág. 3).

Durante la ejecución del ciclo OODA, las IO se convierten en un método que influye, interrumpe, corrompe o usurpa la toma de decisiones o el mando y control de los adversarios o potenciales adversarios. Esto se logra interrumpiendo o disminuyendo la velocidad a la que funciona su ciclo OODA o alimentando la información seleccionada en ese ciclo, el cual no tiene que ser completamente roto por esfuerzos ofensivos de IO, sino que solo podría ser interrumpido durante el tiempo necesario para permitir que otras operaciones militares logren el éxito.

Dado que el ciclo OODA ayuda a crear una imagen mental estructurada y completa para los responsables de tomar de decisiones en cualquier tipo de organización, en el libro *Operational Art* se establece que toda interrupción o manipulación a este ciclo puede hacer que el comandante enemigo tome una mala decisión y cree una ventaja u oportunidad para las fuerzas propias o amigas; de esta forma, se cumpliría, el principal objetivo de las IO, el cual es influir, perturbar, corromper o usurpar la toma de decisiones del adversario y potenciales adversarios, mientras se protege la información propia.

Por ello, identificar acertadamente a los responsables de tomar decisiones en el bando oponente juega un rol preponderante en el resultado que se espera que produzcan las IO. Para lograr esta identificación e influir con éxito en los adversarios, el texto de la USMC indica que los líderes en el nivel operacional deben centrarse en comprender los procesos cognitivos del enemigo, así como en alcanzar objetivos militares físicos en el entorno operacional[19] (OE). Además, señala que para poder crear los efectos deseados en la voluntad, comprensión y capacidades del adversario o potenciales adversarios, lo más importante es convencerlos de reaccionar sin que estén conscientes de que están siendo manipulados. Finalmente, establece que para poder influir con éxito sobre el oponente o potenciales oponentes, se deben dominar aspectos de su cultura, valores y tendencias mediante el análisis del público objetivo o *target audience analysis* (TAA).

De esta manera, el TAA tiene por propósito "identificar públicos con poder, los que comprenden grupos o personas cuyas decisiones o cambios de comportamiento pueden impactar positiva o negativamente en el estado final deseado del comandante" (pág. 7). Por consiguiente, la ejecución de un detallado proceso de TAA permitirá comprender sobre quién o en contra de qué se deben direccionar los esfuerzos de las IO.

3.3 Aplicación de las operaciones de información en el arte y diseño operacional

El arte operacional es un proceso creativo que busca el hábil empleo de las fuerzas para alcanzar objetivos militares –operacionales y estratégicos– traduciendo la estrategia en acción mediante el diseño, organización, integración y conducción de campañas, operaciones mayores y acciones tácticas, determinando dónde, cuándo, y con qué propósito se realizarán operaciones. Es aplicable a todo el espectro del conflicto y en los

[19] Entorno operacional (OE): Definido como la combinación de las condiciones, circunstancias e influencias que afectan el empleo de capacidades y afectan las decisiones del comandante (Department of Defense (DOD), 2018, pág. 172).

diferentes niveles de conducción militar –estratégico, militar y táctico– y busca alcanzar los objetivos con menor costo y duración. Por medio del arte operacional, el comandante es capaz de enlazar fines, modos, recursos o capacidades con el estado final deseado (EFD).

Mientras el arte operacional es la manifestación de la visión y creatividad del comandante, el diseño operacional es la metodología por la cual el arte operacional es graficado y relatado para la planificación de campañas militares. El artículo *Arte y Diseño Operacional. Una Forma de Pensar Opciones Militares* de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas argentinas (Kenny, Locatelli, & Zarza, 2017) establece que para su realización el diseño operacional utiliza elementos tradicionales, Innovadores y circunstanciales, los que a continuación se detallan en la siguiente tabla.

ELEMENTOS DEL DISEÑO OPERACIONAL		
Tradicionales	**Innovadores**	**Circunstanciales**
• Objetivo Operacional • Misión • Esfuerzos • Maniobra • Campaña • Niebla y fricción	• Estado Final Deseado • Centro de Gravedad • Factores Críticos • Puntos Decisivos • Líneas de Operaciones • Intención del Comandante	• Momentum • Tempo • Punto Culminante • Alcance Operacional • Pausa Operacional • Enlace Operacional

Tabla 1: Elementos del diseño operacional. Fuente: Elaboración propia.

Con respecto al empleo de las IO en el diseño operacional, es importante señalar que éstas deben ser integradas desde el inicio del proceso, ya que su correcta integración permitirá emplearlas como medios y formas para alcanzar los objetivos operacionales de la campaña. Esto es corroborado por la publicación conjunta estadounidense JP 3-13 *Information Operations*, la cual indica que junto con cooperar a alguna LOE las IO deben apoyar a múltiples LOO y que en algunas ocasiones puede ser la LOO que se debe apoyar. De la misma manera, establece que “la planificación de las IO debe comenzar en la etapa más temprana del proceso de planificación de operaciones (OPP) y ser parte integral y no una adición al esfuerzo de planificación general” (JP 3-13, 2014, pág. IV 1). Por otra parte, en un artículo escrito por Blane Clark en de la revista *Military Review*, se señala que “las operaciones de información que se planean, integran y ejecutan como parte de un plan de campaña de un comando de combate en la primera fase, ofrecen opciones no cinéticas y no letales a un comandante para lograr sus metas estratégicas”

ya que generan temor, desconcierto y duda en los líderes adversarios, induciéndolos a abandonar un curso de acción (COA) específico (Clark, 2010, pág. 2).

3.4 Las ciberoperaciones como parte de las capacidades relacionadas con la información

La publicación conjunta de las FF.AA de Estados Unidos JP 3-13 indica que, mediante el empleo de las capacidades relacionadas con la información (IRC) se logra un efecto multiplicador de las IO, por medio de herramientas, técnicas o actividades que pueden afectar a cualquiera de las tres dimensiones del entorno de la información (física, cognitiva e información), afectando a la capacidad del público objetivo (TA) para recopilar, procesar o diseminar información antes y después de tomar decisiones; de esta manera, es el comandante, junto a su grupo asesor, quien debe determinar qué IRC puede aplicar sobre individuos, organizaciones o sistemas para lograr el EFD.

Las IRC establecidas y definidas por la JP 3-13 para las fuerzas conjuntas estadounidenses son: comunicaciones estratégicas, grupos de coordinación interinstitucional conjunto, asuntos públicos, operaciones civiles-militares, seguridad de la información, operaciones espaciales, operaciones de apoyo a la información militar, operaciones de técnicas especiales, operaciones conjuntas del espectro electromagnético, inteligencia, decepción militar, seguridad de las operaciones, captación del líder/actor clave y ciberoperaciones.

La publicación define a las ciberoperaciones como el empleo de las capacidades del ciberespacio, donde el propósito principal es lograr objetivos en o a través del ciberespacio. Estas capacidades, cuando apoyan el desarrollo de las IO en coordinación con otras LOO y LOE, permiten negar o manipular el ciclo OODA de un adversario o potencial adversario al realizar acciones ofensivas u ofensivas en la dimensión física, de la información y cognitiva (JP 3-13, 2014, págs. II-9).

En base al análisis de las características de las CO, descritas por las fuerzas conjuntas de Estados Unidos en su publicación JP 3-12 *Cyberspace Operations* (JP 3-12, 2018), se elaboró una tabla en donde se describe lo que estas características proporcionan –

como herramientas de las IO para afectar al ciberespacio– durante el desarrollo del proceso de las operaciones[20]:

Características ofensivas y defensivas de la IRC ciberoperaciones	
Latencia	Dificulta al adversario detectar el ataque realizado por las fuerzas propias, siendo su efecto evidenciado posterior a su ejecución.
Atribuibilidad	Permite realizar el ataque en forma anónima, sin evidenciar quién materializó la ciberinterdicción, dificultando la identificación de su originador.
Limitación del daño	Si bien el daño físico/material que producen es limitado, el ataque sobre los sistemas de comunicaciones y de mando y control de las fuerzas militares enemigas puede producir efectos operacionales y estratégicos.
Incertidumbre	Una vez que el adversario detecta que fue atacado, desconoce las repercusiones que tendrá sobre sus sistemas, ya que sus efectos pueden no ser aparentes ni verificables en primera instancia, afectando directamente a la dimensión cognitiva del enemigo.
Ubicuidad	Permite realizar los ataques de forma individual o simultánea sobre distintos objetivos desde cualquier ubicación geográfica, dentro o fuera del AROP.
No proporcionalidad	Otorga a la fuerza naval más débil la capacidad de producir daños significativos sobre fuerzas que posean mayores capacidades militares.
Diseminación	Mediante la ejecución de ciberataques como fuegos operacionales no letales, permite minimizar y controlar los daños colaterales que puede causar un ataque dirigido sobre un blanco en particular.

Tabla 2: Características ofensivas y defensivas de las CO. Fuente: Elaboración propia.

3.5 Las ciberoperaciones como fuegos operacionales no letales

Para el logro de sus objetivos operacionales y estratégicos, los comandantes de estos niveles utilizan las denominadas *funciones operacionales o conjuntas*, las que según lo establece la publicación *Joint Operations* de las FFAA de Estados Unidos, se definen como capacidades y actividades relacionadas agrupadas para ayudar a los comandantes del nivel operacional a integrar, sincronizar y dirigir operaciones conjuntas. Las funciones

[20] El proceso de las operaciones consiste en planificar, preparar, ejecutar, evaluar, una operación naval de nivel operacional o táctico, para el logro de los objetivos estratégicos, operacionales o tácticos establecidos por los niveles correspondientes de conducción militar. Fuente: Módulo 3. Conducción táctica y operacional de fuerzas navales. Asignatura de Conducción de Fuerzas Navales. Unidad Temática N°1. Escuela de Guerra Naval 2021.

operacionales son: inteligencia, movimiento y maniobra, mando y control, sostenimiento, protección y fuegos (JP 3-0, 2017, págs. III-1).

Con respecto al empleo de las CO como fuegos operacionales, Crowell indica, en su artículo escrito para el *Naval War College,* que la IRC ciberoperaciones, –al realizarse en las profundidades operacionales y estratégicas de las defensas del enemigo–, puede considerarse como fuego operacional, ya que genera un impacto decisivo durante el transcurso y en el resultado de una campaña. Al mismo tiempo, facilita la maniobra operacional propia siendo parte de las opciones no cinéticas y no letales con que cuentan los comandantes para cumplir sus objetivos operacionales y estratégicos (Crowell, 2016, pág. 18).

De la misma manera, la publicación conjunta de las Fuerzas Armadas de Estados Unidos *Joint Fire Support JP 3-09* (JP 3-09, 2019) –que proporciona los principios y orientaciones fundamentales para la planificación, ejecución y evaluación de los fuegos de apoyo operacionales o conjuntos– establece que el fuego de apoyo operacional es el "fuego conjunto que apoya a las fuerzas aéreas, terrestres, marítimas, espaciales, ciberespaciales y de operaciones especiales a mover, maniobrar y controlar el territorio, el espacio aéreo, el espacio, el ciberespacio, el espectro electromagnético y los espacios marítimos claves e influir en las poblaciones" (pág. vii). Igualmente, la JP 3-09 refiere que las capacidades relacionadas con los fuegos de apoyo operacionales incluyen –no de forma exclusiva– las capacidades aire-superficie, superficie-superficie, control del espacio ofensivo, ataques electrónicos, IRCs, ciberoperaciones y las armas no letales (pág. x).

Cabe destacar que dentro de la estructura de un MOC existe una célula dedicada a planificar, preparar y coordinar los fuegos operacionales. Esta célula, denominada *Fires Element* (FE), posee en forma paralela un grupo especialmente conformado para materializar el comando y control de las CO como fuegos operacionales de apoyo, denominado *Cyberspace Fires C2*, cuyo propósito es coordinar la planificación e integración de estos fuegos en la maniobra operacional (págs. II-16, II-22).

En síntesis, mediante la planificación, integración y sincronización de la IRC ciberoperaciones en el desarrollo de una operación naval mayor[21] como fuego

[21] Operación Naval Mayor: Serie de acciones navales tácticas de mayor o menor envergadura, relacionadas entre sí, llevadas a cabo por fuerzas navales diversas o incluso con fuerzas de otras armas, en términos de espacio y tiempo

operacional no letal dentro de una LOO o LOE, el comandante del nivel operacional puede crear las condiciones requeridas en el OE marítimo, que le permitan a sus comandantes subordinados obtener la libertad de acción requerida para el cumplimiento de la misión, pudiendo ser ésta –entre otras– la de impedir el acceso a una área marítima propia a una fuerza adversaria.

3.6 Aplicabilidad de las operaciones de información en el comando del espacio común marítimo como parte de la estrategia A2/AD.

Las IO emplean el ciberespacio como principal espacio para utilizar sus IRC en la estrategia A2/AD, entre ellas la IRC de ciberoperaciones. De este modo, y, en atención a que el ciberespacio sustenta la conectividad y las transacciones comerciales y financieras del mundo, junto con que las acciones realizadas en dicho espacio afectan transversalmente a todos los dominios de la guerra –afectando a los sistemas de C3 de las unidades e instalaciones militares–, es que resulta fundamental aplicar las IO en la estrategia de A2/AD que se desarrolle para obtener el comando del espacio común marítimo.

De esta manera, y tomando en consideración las características de las IO, es que las IO deben ser aplicadas como parte de la estrategia A2/AD desde la primera etapa del proceso de las operaciones, realizando un acabado TAA para identificar al actor, líder o sistema de C3, y, también, determinando sobre cual capa del ciberespacio se realizarán las IO. De esta forma, se afecta el proceso de toma de decisiones del adversario y también las dimensiones física, cognitiva y de la información, reafirmando así lo señalado por Alexander Kutt, en relación a que “el país que consiga controlar el ciberespacio comandará también sobre el resto de global commons” (2015, pág. 18)

Haciendo referencia a lo señalado por Russell (2017), la principal forma de aplicar las IO en el comando del espacio común marítimo como parte de la estrategia A2/AD es mediante la realización de ataques digitales o *cyber attacks* en el ciberespacio. Asimismo, que para que estas ciberoperaciones permitan el cumplimiento de los objetivos planteados, deben focalizarse en afectar las capas físicas y lógicas del ciberespacio, ya que ambas están estrechamente relacionadas al sustentarse la capa lógica en los elementos de la física.

dados para alcanzar un objetivo operacional (a veces un objetivo estratégico limitado) dentro de un teatro de operaciones marítimo.

En base a lo enunciado precedentemente, es que deben centrarse los esfuerzos de las *cyber A2/AD* en atacar la principal vulnerabilidad de la capa física. Esta es, según Russell, la que presentan los cables de fibra óptica submarinos, ya que éstos son vulnerables –en su capa física– tanto en sus nodos y servidores que centralizan el procesamiento de los paquetes de datos, como también, al atravesar los espacios marítimos sin ningún tipo de protección. De la misma forma, también son vulnerables –en su capa lógica– los sistemas operativos que gestionan las longitudes de onda de los cables de fibra óptica cuando llegan a tierra. En el mismo sentido, Russell plantea que no existen fuerzas navales dedicadas a la protección de los cables, y, también, que sólo existe una poca cantidad de empresas que los reparen por medio de sus buques, estando sus servicios agendados con años de antelación. Asimismo, dicho autor señala que otra vulnerabilidad de la capa física son los satélites, ya que pueden ser atacados digitalmente desde cualquier lugar geográfico –aduciendo a la característica de *ubicuidad* de las ciberoperaciones. De esta manera, se afectan las capacidades de C3 del adversario antes de acceder al espacio común marítimo o reduciendo su capacidad de maniobra dentro de dicho espacio (págs. 5,6,29).

Otra forma en que se pueden aplicar las IO en el comando del espacio común marítimo como parte de la estrategia A2/AD, es mediante la afectación del dominio cognitivo del adversario, generado mediante el efecto disuasivo que generan las cyber A2/AD. Así, el Estado atacante al verse –creíblemente– amenazado de la realización de *cyber attacks* sobre los instrumento de su poder nacional que dependan del ciberespacio, pude desistir de su accionar o cambiar su curso de acción.

Finalmente, cabe destacar, que tanto las *cyber A2/AD* realizadas –como fuegos operacionales no letales– sobre los cables de fibra óptica submarinos y sobre los satélites, como también el efecto disuasivo que generan dichas acciones –como parte de las aplicaciones de las IO en la estrategia A2/AD– pueden ser realizadas por fuerzas que posean sólo el suficiente poder para desarrollar estas acciones, no siendo necesariamente más fuertes que sus adversarios.

Como conclusiones del presente capítulo, se puede señalar que las IO son realizadas para afectar el ciclo de toma de decisiones del adversario mientras se protege la información propia, y que la dimensión cognitiva es la más importante del entorno de la información. De la misma manera, se pudo determinar que la ejecución de IO durante el desarrollo del ciclo OODA del adversario afecta su proceso de toma de decisiones y

protege el propio y, también, que estas operaciones se relacionan con el arte y diseño operacional al ser parte de las LOE y LOO. A su vez, se pudo concluir que por medio del empleo de las IRC se logra un efecto multiplicador de las IO para afectar las dimensiones del entorno de la información, y que la IRC ciberoperaciones permite lograr los objetivos operacionales a través del uso de las capacidades del ciberespacio. Del mismo modo, se estableció que las CO son consideradas como fuegos operacionales no letales y que se relacionan con el MOC por medio de un grupo especialmente conformado para incluirlas en la maniobra operacional. Finalmente, se determinó que la principal forma de aplicar las IO en el comando del espacio común marítimo, como parte de la estrategia A2/AD, es por medio de la realización de ataques digitales sobre las vulnerabilidades que presentan las capas físicas y lógicas del ciberespacio, y, también, por medio de la disuasión que generan las *cyber A2/AD*.

Conclusiones

Durante el desarrollo del presente trabajo de investigación se logró cumplir con los cuatro objetivos específicos establecidos, conducentes al objetivo general de la investigación, definido como p*roponer aplicaciones de las IO en el comando del espacio común marítimo como parte de la estrategia A2/AD*. De esta forma, en base al supuesto investigativo de que siendo el espacio común marítimo un área de disputa donde la soberanía de un Estado puede verse afectada, las operaciones de información pueden ser aplicadas como parte de la estrategia de A2/AD para aumentar la capacidad de control y defensa en dicho espacio, por medio de la realización de ciberoperaciones como fuegos operacionales, afectando el ciclo de toma de decisiones del adversario, se ha llegado a las siguientes conclusiones:

Mediante el desarrollo del Capítulo 1, *Empleo y control de los espacios comunes marítimos*, se pudo señalar que los espacios comunes son las áreas que involucran a los océanos, el espacio exterior y el ciberespacio que no están bajo la soberanía de ningún estado en particular, pudiendo ser explotados por cualquier tipo de actor o entidad. Asimismo, que para las grandes potencias –y también para los que se benefician de ellos– resulta vital poder acceder a estos espacios para emplearlos en términos económicos y militares.

De la misma manera, se determinó que la importancia del espacio común marítimo radica en los recursos naturales que presenta, así como también, por ser el principal espacio para desarrollar el comercio y la conectividad global. También, se afirmó que para las grandes potencias –sean ribereñas o no– es esencial acceder y emplear estos espacios marítimos en su propio beneficio, ya sea económico o militar.

A su vez, se estableció que el comando de los espacios comunes marítimos es ejercido por el Estado o actor que posea el control del mar, otorgándole una ventaja militar por sobre quien no lo posee y la capacidad de posicionar y proyectar sus fuerzas navales en todo el mundo, controlando su acceso y negando su uso. Al mismo tiempo, se determinó que Estados o actores con menores capacidades pueden hacer uso y beneficiarse de estos espacios comunes marítimos, generando una dependencia militar y tecnológica del bando más débil para con el más fuerte. También, se demostró que las FFAA de Estados Unidos –como actor hegemón del comando de los espacios comunes- actualizó su estrategia de defensa al ver amenazados el acceso y control a los océanos, para por

medio de la unión de las capacidades de su armada, infantería de marina y servicio de guardacostas poder acceder a todos los dominios de la guerra y mantener el comando del espacio común marítimo.

Finalmente, se pudo determinar que el ciberespacio como espacio común es esencial para el funcionamiento de los Estados y posee las mismas características que los otros espacios comunes, generando disputas entre las grandes potencias del mundo por su control y comando al ser un espacio vital para la economía y conectividad mundial. También, se demostró que difiere en tres aspectos: en que fue creado y puede ser destruido por el ser humano; en que se relaciona transversalmente con los otros dominios y en que su topografía cambia constantemente.

Las conclusiones enunciadas anteriormente, permitieron cumplir con el segundo objetivo específico del presente trabajo de investigación, correspondiente a *describir las características específicas de los espacios comunes marítimos con relación a su empleo y control.*

Con respecto al cumplimiento del tercer objetivo específico, *definir las principales formas de utilizar la estrategia A2/AD para defender los espacios comunes marítimos,* este fue alcanzado mediante la obtención de las siguientes conclusiones del Capítulo 2, *Las estrategias de Antiacceso y Negación de Área para la defensa de los espacios comunes marítimos*:

Se pudo establecer, mediante la conceptualización de la estrategia de A2/AD, que ésta ha sido utilizada –con el propósito de negarle al adversario la capacidad de entrar a un área específica propia y maniobrar libremente dentro del espacio de batalla– desde los tiempos de los griegos hasta en la actualidad. Esto a través del cumplimiento de la tendencia en el tiempo de la modernización de las capacidades tecnológicas y militares utilizadas por las fuerzas, asimismo, de la constante histórica del uso de la geografía a favor del bando defensor, como también el ataque sobre la logística del atacante. Asimismo, se pudo concluir que la ventaja de este tipo de estrategia es que una fuerza tiene que ser lo suficientemente poderosa –no más fuerte– para cumplir con su propósito. Por otro lado, la desventaja que presenta es que si se utiliza como método defensivo exclusivo no permitirá derrotar al bando adversario, ya que necesita de elementos fuera de las operaciones propias de antiacceso y negación de área.

Con respecto a la estrategia de A2/AD en el espacio común marítimo, se pudo demostrar –mediante tendencias y constantes– las formas en que las principales potencias del mundo utilizan esta estrategia para defender sus espacios comunes marítimos. También, se pudo concluir que por medio de las acciones realizadas en la estrategia A2/AD en el ciberespacio, se pueden complementar las formas de utilización de las actividades de antiacceso y negación de área realizadas para la defensa de los espacios comunes marítimos. Esto, debido a la vital importancia que posee el ciberespacio como espacio común para los Estados, y a que las acciones que se realicen en él afectan transversalmente a todos los dominios de la guerra. Además, se pudo establecer que estas acciones complementarias –realizadas en los niveles estratégico y táctico– deben desarrollarse en las capas físicas y lógicas del ciberespacio. De la misma manera, se pudo establecer otra forma de utilizar las *cyber* A2/AD en las actividades de antiacceso y negación de área realizadas en el dominio marítimo, siendo ésta a través del efecto disuasivo que generan las ciberoperaciones en el bando adversario.

Finalmente, mediante el desarrollo del Capítulo 3, *Las operaciones de información y el comando del espacio común marítimo*, se cumplieron los objetivos parciales 1 y 4, definidos como *analizar el concepto de empleo de las IO en el desarrollo de las operaciones militares* y *determinar la aplicabilidad de las IO para el comando del espacio común marítimo*, respectivamente.

Con respecto al primer objetivo, se definió que las operaciones de información (IO) son el empleo integrado –durante las operaciones militares– de las capacidades relacionadas con la información (IRC), siendo su propósito influir, perturbar, corromper o usurpar el ciclo de toma de decisiones del adversario mientras se protege la información propia. Asimismo, que su entorno está compuesto por tres dimensiones: la dimensión física –integrada por sistemas, infraestructuras de C3 e individuos–; la dimensión de la información –donde se realizan las actividades de recopilación, procesamiento, almacenamiento, difusión y protección de la información–, y, finalmente, la dimensión cognitiva –que comprende las mentes de aquellos que transmiten, reciben, responden o actúan sobre la información, siendo el componente más importante del entorno de información. También, se pudo determinar que la ejecución de IO durante el desarrollo del ciclo OODA afecta el proceso de toma de decisiones del adversario –interrumpiendo o disminuyendo la velocidad a la que funciona su ciclo– y permite proteger el ciclo de las fuerzas propias.

De la misma manera, se determinó que las IO se emplean desde el comienzo del proceso de las operaciones, al integrarse con el arte y diseño operacional por medio de las IRC como medios o formas de una o más LOO o como una LOE en particular. A su vez, se pudo concluir que la IRC ciberoperaciones logra los objetivos operacionales a través del uso de las capacidades del ciberespacio. También, se estableció que las CO son empleadas como fuegos operacionales no letales, ya que se planifican en el nivel operacional y las consecuencias de sus acciones se reflejan en los niveles operacionales y estratégicas del adversario. Asimismo, porque generan un impacto decisivo tanto durante el transcurso de las operaciones militares, como en el resultado de una campaña. Por otra parte, se indicó que las CO son planificadas, preparadas y coordinadas –como fuegos operacionales– en el MOC por medio de un grupo especialmente conformado para ello.

Del mismo modo, para el cumplimiento del cuarto objetivo específico, se pudo determinar que la principal forma de aplicar las IO en el comando del espacio común marítimo como parte de la estrategia A2/AD, es por medio de ataques digitales –también llamados *cyber attacks*– sobre las capas físicas y lógicas del ciberespacio. De esta manera, las cyber A2/AD deben focalizarse en afectar las principales vulnerabilidades de estas capas, siendo estas los cables de fibra óptica submarinos y los satélites. Asimismo, se determinó que otra forma de aplicar las IO en el comando del espacio común marítimo como parte de la estrategia A2/AD, es por medio del efecto disuasivo que generan las cyber A2/AD, ya que afectando el dominio cognitivo del adversario se puede llegar cambiar el curso de acción tomado por el adversario o incluso disuadir un conflicto.

Bibliografía

Battaleme, J. (2015). Cambiando el Status Quo de la Geopolítica Internacional: El acceso a los espacios comunes y las estrategias de negación de espacio y antiacceso . *Instituto de Ciencias Sociales y Disciplinas Proyectuales. INSOD*.

Clark, B. (2010). Las operaciones de información como elemento disuasivo para el conflicto armado. *Military Review*, 2-11.

Crowell, R. (2016). *War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare.* U.S. Naval War College. NWC 2021D.

Department of Defense (DOD). (2018). *Dictionary of Military and Associated Terms.*

Elkins, L. (Noviembre de 2019). *OTHT. Over the Horizon. Multi-Domain Operations & Strategy*. Obtenido de https://othjournal.com/2019/11/05/the-6th-warfighting-domain/

Global Commons Alliance. (09 de Agosto de 2021). *Global Commons Alliance. A plan for the planet*. Obtenido de https://globalcommonsalliance.org/global-commons/

Joint Chieff of the Staff. (2018). *Strategy.*

Kenny, A., Locatelli, O., & Zarza, L. (2017). *Arte y Diseño Operacional. Una forma de pensar operaciones militares.* Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Kutt, A. (2015). La importancia de dominar los globals commons en el siglo XXI. *Instituto Español de Estudios Estratégicos*. Obtenido de http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM29-2015_Global_Commons_XXI_Alexander_Kutt.pdf

Lincoln, E. (2014). Cyber Power in 21st-Century Joint Warfare. *JFQ 74, 3rd Quarter 2014*.

Marine Insight. (2019). *Marine Insight*. Obtenido de https://www.marineinsight.com/marine-navigation/what-are-maritime-chokepoints/

Marine Traffic. (19 de Agosto de 2021). *Marine Traffic*. Obtenido de https://www.marinetraffic.com/en/ais/home/centerx:-17.1/centery:21.9/zoom:2

MDAA. (24 de Agosto de 2018). *China's Anti-Access Area Denial*. Obtenido de Missile Defense Advocacy Alliance: https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/china/china-anti-access-area-denial/

Posen, B. (2003). *Command of the Commons. The Military Foundation of U.S Hegemony.*

Russell, A. (2017). *Strategic A2/AD in Cyberspace.* New York: Cambridge University Press.

Shunk, D. (Diciembre de 2014). Area Denial & Falklands war lessons learned - Implications for land warfare 2030-2040: After the Army´s theater arrival - The coming complex fight. *Small Wars Journal*. Obtenido de https://smallwarsjournal.com/jrnl/art/area-denial-falklands-war-lessons-learned-implications-for-land-warfare-2030-2040-after-the

Shunk, D. (2014). *Small Wars Journal*. Obtenido de https://smallwarsjournal.com/jrnl/art/area-denial-falklands-war-lessons-learned-implications-for-land-warfare-2030-2040-after-the

Solís, E. (2004). *Manual de Estrategia.* Viña del Mar: Academia de Guerra Naval.

Staff, U. J. (2014). *JP 3-13 "Information Operations".*

Submarine Cable Map. (19 de Agosto de 2021). *Submarine Cable Map*. Obtenido de https://www.submarinecablemap.com/

Tangredi, S. (2018). Antiaccess Warfare as Strategy. *Naval War College Review, 71*.

Turker, H. (9 de Enero de 2021). *The Geopolitics*. Obtenido de https://thegeopolitics.com/new-cold-war-at-global-commons-a-new-u-s-naval-strategy-for-the-great-power-competition-era/

U.S Joint Staff. (2014). *JP 3-13.* Estados Unidos.

U.S Joint Staff. (2014). *JP 3-13 "Information Operations".* Estados Unidos.

U.S Joint Staff. (2017). *JP 3-0.*

U.S Joint Staff. (2018). *JP 3-12.*

U.S Joint Staff. (2019). *JP 3-09.*

U.S Joint Staff. (2020). *JP 3-32 .*

U.S. Joint Staff. (2013). *JP 3-12 "Cyberspace Operations".*

United States Navy. (2020). *Advantage at Sea. Prevailing with Integrated All-Domain Naval Power.*

United States Navy, U. (2020). *Advantage at Sea. Prevailing with Integrated All Domain Naval Power.* Estados Unidos. Obtenido de https://assets.documentcloud.org/documents/20429439/triservicestrategy.pdf

USMC University. (2016). *Module 8903. "Operational Art". Lesson 7.*

USNAVY. (2013). *NWP 5-01 "Navy Planning".*