ISSN: 2706 - 5928

Revista de la ESCUELA SUPERIOR DE GUERRA NAVAL

Explorando la repetición de sucesos a través de decisiones aleatorias en los Juegos de Guerra

El crimen organizado transnacional como amenaza estratégica para el Perú: riesgos, implicancias y desafíos para el Sector Defensa

Evolución de las operaciones antisuperficie

Inteligencia artificial y su consideración en el desarrollo militar como avance tecnológico

De las alertas al análisis: la importancia de una Central de Inteligencia donde la IA acelera pero el analista proyecta

Desafíos en el ejercicio del Comando y Control en Operaciones Navales aplicados en la Marina de Guerra del Perú

La guerra como fenómeno social: aportes desde la sociología y la inteligencia estratégica

Dominio marítimo del Perú, seguridad y gobernanza oceánica: evolución normativa, institucional y desafíos

Ciberdefensa: Una opción para reforzar las capacidades de Ciberseguridad en el Perú

REVISTA DE LA ESCUELA SUPERIOR DE GUERRA NAVAL

Edición: 2025, Vol.22, N°3
Callao - Perú.

Revista de la Escuela Superior de Guerra Naval

Marina de Guerra del Perú
Jr. Sáenz Peña, 590, La Punta, Callao
Web: www.esup.edu.pe

Portada:
Corrección de texto: Calm. (r) Raúl Vásquez Alvarado
Diseño y diagramación: Lic. Sheylla Castillo Cárdenas
Traducción: Lic. María Antonella Aguilar Idone

Issn: 2706 - 5928 (Digital)
Hecho en el depósito legal en la Biblioteca Nacional del Perú Nº 2010 - 07839
Edición: 2025, Vol.22, N°3
Periodicidad: Semestral
URL: revista.esup.edu.pe/ojs/
Correo electronico: revista.esup@esup.edu.pe

La *Revista de la Escuela Superior de Guerra Naval* fue establecida en 1993 con el objetivo de promover la realización de trabajos de investigación sobre temas de interés relacionados con asuntos marítimos y navales.

CONTENIDO

PALABRAS DEL DIRECTOR

Contralmirante
Kurt Böttger Garfias
Director de la Escuela Superior de Guerra Naval
https://orcid.org/0009-0008-0374-2559
DOI: https://doi.org/10.35628/resup.v16i2.169

Llegamos al final del año académico 2025 de la Escuela Superior de Guerra Naval, año de especial importancia para este Centro Académico de posgrado, tanto por la celebración del nonagésimo quinto aniversario de su creación como por la aprobación del proyecto de inversión para la construcción de un campus completamente nuevo, con tecnología educativa de punta para todos nuestros programas de estudios.

La edición que me permito presentar en esta ocasión aborda temas relacionados a las operaciones navales, inteligencia estratégica, inteligencia artificial y juegos de guerra, entre otros sobre asuntos militares en general.

Es siempre satisfactoria la participación de nuestros exalumnos en esta Revista, al escribir sobre temas del ámbito de la seguridad y defensa nacional, lo que contribuye con la gestión académica de esta Escuela de posgrado y que espero sea del beneplácito de nuestros lectores.

Atte.
Contralmirante
Kurt BÖTTGER Garfias
Director de la Escuela Superior de Guerra Naval


MARINA DE GUERRA DEL PERÚ
AGNITIO OMNIA VINCET
ESCUELA SUPERIOR DE GUERRA NAVAL

Año 2025, Vol. 22, Nº 3, pp. 08 - 32.
DOI: https://doi.org/10.35628/resup.v16i2.170

Explorando la repetición de sucesos a través de decisiones aleatorias en los Juegos de Guerra

Exploring the Repetition of Events through Random Decisions in Wargames

Recibido: 25 de septiembre de 2025 | Aceptado: 03 de diciembre del 2025

Marco Mujica Caballero
https://orcid.org/0009-0006-6789-6878

Máster en Ciencias (M. Sc.) en "Innovation and Strategic Management" por Salve Regina University, Newport, RI, EE.UU. y licenciado en Ciencias Marítimas Navales por la Escuela Naval del Perú. Es calificado en Guerra de Superficie y Sistemas de Armas. Obtuvo el primer puesto en el Programa Básico de Estado Mayor por la Escuela Superior de Guerra Naval. Graduado del programa Naval Staff College, Class of 2023 del U.S. Naval War College, Newport. Docente de la asignatura "Maritime Operation Center-MOC" del Programa Básico de Estado Mayor. En el año 2024, se desempeñó como Battle Watch Captain (BWC) en el MOC durante el ejercicio multinacional UNITAS Chile. Asimismo, participó en el ejercicio de guerra de minas navales "Nusret", estándar OTAN, llevado a cabo en el mar Egeo, Turquía.

Email:marcomujicac@gmail.com

Resumen: Los juegos de guerra son una disciplina clave en la toma de decisiones, caracterizada por la incertidumbre, la interdependencia de las decisiones y la información imperfecta. A diferencia de juegos como el ajedrez, donde la información es perfecta, los juegos de guerra implican escenarios donde los participantes deben gestionar información limitada y temporal para tomar decisiones bajo incertidumbre. El uso de métodos científicos como la simulación de Monte Carlo y el análisis de bases de datos históricas permite optimizar las decisiones, reducir riesgos y mejorar la previsibilidad a través de la simulación y el análisis de datos preexistentes. Los *wargamers* pueden explorar diferentes

cursos de acción, identificar patrones y adaptar sus estrategias y tácticas según sea el caso, en función de escenarios cambiantes. El artículo explora cómo estos métodos de análisis aplicados en los juegos de guerra y su similitud con el ajedrez pueden mejorar la calidad de la toma de decisiones y aumentar las probabilidades de éxito.

Palabras clave: toma de decisiones, métodos cuantitativos y cualitativos, simulación de Monte Carlo, análisis de bases de datos, registros históricos, ajedrez aplicado, matriz de apoyo a la decisión (DSM), progresiones regresivas en la guerra.

Abstract: *Wargames are a key discipline in decision-making, characterized by uncertainty, the interdependence of decisions, and imperfect information. Unlike games such as chess, where information is perfect, wargames involve scenarios where participants must manage limited and temporal information to make decisions under uncertainty. The use of scientific methods such as Monte Carlo simulations and the analysis of historical databases helps optimize decisions, reduce risks, and improve predictability through simulation and the analysis of previous data. Wargamers can explore different courses of action, identify patterns, and adapt accordingly their strategies and tactics, based on changing scenarios. The article explores how these analytical methods applied in wargames and their similarity with chess can improve decision-making quality and increase the chances of success.*

Keywords: *decision-making, quantitative and qualitative methods, Monte Carlo simulation, database analysis, historical records, applied chess, decision support matrix (DSM), regressive progressions in war.*

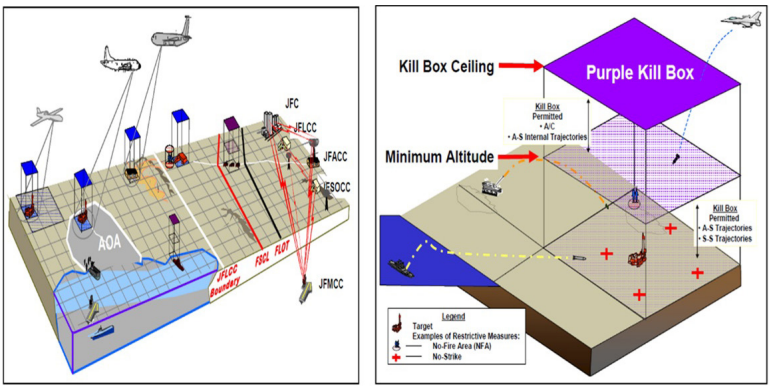
1. INTRODUCCIÓN

Los juegos de guerra constituyen un área sumamente interesante, que combina tanto la teoría como la práctica, donde la toma de decisiones puede marcar la diferencia entre el éxito y el fracaso. Estos juegos se caracterizan por la incertidumbre, el análisis de diferentes cursos de acción y la interdependencia entre las decisiones de los wargamers o actores involucrados; donde las decisiones no solo son cambiantes, sino fluyen a través de la fricción y niebla propia de la guerra, obligando a lidiar a los *wargamers* con situaciones complejas, donde disponen de información imperfecta y limitada, tratando de optimizar y adaptar los cursos de acción bajo condiciones de incertidumbre. Por ende, los juegos de

guerra permiten mejorar la calidad y reflexión de las técnicas para la toma de decisiones, innovando soluciones con diferentes perspectivas.

Cuando la información es perfecta, todos los actores tienen acceso completo al estado del juego en todo momento, lo que permite decisiones basadas en un conocimiento absoluto de las posiciones y movimientos del oponente, como ocurre en el ajedrez. En contraste, en los juegos de guerra la información es imperfecta, generando una natural incertidumbre debido a que la ubicación de algunas unidades del adversario, capacidades e intenciones del mismo se desconocen, obligando a los *wargamers* a tomar decisiones basadas en información temporal, engañosa, incompleta e imperfecta. Por tal motivo, es necesario el análisis previo, en tiempo de paz, de factores cuantitativos a través de probabilidades, procesos deductivos y manejo de inteligencia parcial[1], donde el análisis estadístico y de datos juega un papel crucial, permitiendo la obtención de información precisa y objetiva para tomar decisiones fundamentadas. La utilización de métodos cuantitativos no solo optimiza la toma de decisiones, sino que también permite la reflexión, el desarrollo de pensamiento crítico, la evaluación de riesgos, el rediseño de tácticas y la mejora de la interoperabilidad de los medios en todo el espectro de las operaciones navales. Esto permite afrontar de manera más eficaz la compleja guerra naval, enfrentando desafíos como la sorpresa y la información imperfecta a lo largo de todo el proceso del "kill chain", especialmente en las etapas críticas de identificación y clasificación, que juegan un papel crucial en el desenlace de los hechos en los "kill boxes", como se observa en la Figura 1.

FIGURA 1
Ubicaciones representativas de los Kill Boxes



Fuente:Air Land Sea Application (ALSA) Center. (2005). FM 3-09.34 Kill Box Tactics and Multiservice Procedures.

[1] **Inteligencia parcial** se refiere a la información incompleta o limitada que se tiene sobre una situación antes de tomar una decisión.

La relevancia de los métodos cuantitativos se evidencia con particular claridad en los incidentes del USS *Stark* (1987) y el USS *Vincennes* (1988). En el primer caso, la inadecuada priorización y clasificación de amenazas impidió la interceptación oportuna de dos misiles Exocet disparados por un avión iraquí, lo que ocasionó severas pérdidas humanas y materiales. En el segundo, la excesiva confianza en sensores y procedimientos de identificación derivó en la trágica confusión de un Airbus A300 iraní con un caza F-14, culminando en el derribo de una aeronave comercial y la muerte de 290 personas. Estos episodios ponen de relieve cómo la ausencia de un enfoque analítico sólido para la evaluación de riesgos, la validación cruzada de datos y la toma de decisiones bajo incertidumbre puede conducir a consecuencias irreparables.

En este contexto, los métodos cuantitativos adquieren una importancia crítica dentro de la *kill chain*, particularmente en los eslabones de detección, identificación y clasificación de blancos, que constituyen los puntos más vulnerables a la sorpresa y al error humano. La adecuada integración de análisis probabilísticos, modelos de validación de información y herramientas de apoyo a la decisión incrementa la precisión en la transición de *"find, fix, track"* hacia *"target, engage, assess"*, reduciendo la fricción en entornos operacionales saturados. Asimismo, dentro de los *kill boxes*, donde convergen múltiples plataformas y dominios, la dimensión cognitiva del comandante y su *team* se convierte en un multiplicador decisivo: la velocidad y la claridad de juicio resultan tan determinantes como las capacidades tecnológicas de la fuerza.

En función de esta perspectiva del suscrito, Clausewitz (1976) afirmaba que "el propósito de la teoría es educar la mente del futuro comandante" (p. 141); en este caso, en relación directa con la repetición de sucesos a través de decisiones aleatorias en los juegos de guerra, recordándonos que la teoría no dicta acciones automáticas, sino que fortalece el pensamiento estructurado y crítico de quienes deben decidir bajo presión. Así, el empleo de métodos cuantitativos no solo optimiza el proceso de toma de decisiones en la *kill chain*, sino que también contribuye a reducir la probabilidad de error, a mejorar la interoperabilidad en los *kill boxes* y a reforzar la objetividad de las decisiones en escenarios caracterizados por la sorpresa táctica, la presión del entorno operacional y la información fragmentada (Mujica, 2025).

Asimismo, el análisis estadístico permite procesar grandes volúmenes de datos relacionados con el comportamiento de las organizaciones de tarea, la meteorología, las condiciones del mar, movimientos del adversario, las características de sensores y armas a utilizar, entre otras. Esta información es crucial para evaluar

la mejor estrategia o táctica a seguir, optimizando la distribución de recursos, el tiempo de reacción y la maniobra a realizar. Además, la capacidad de analizar los datos de manera eficiente ayuda a predecir los movimientos de las fuerzas adversarias, anticipando sus movimientos y permitiendo una mayor capacidad de respuesta. Es así que los métodos estadísticos también se utilizan para la creación de modelos predictivos que simulan diversas situaciones. Estos modelos permiten a los wargamers evaluar el impacto de distintas decisiones en condiciones controladas y prever los resultados de diferentes tácticas sin el riesgo de un enfrentamiento real. Además, este tipo de simulaciones facilita la identificación de puntos débiles, permitiendo ajustar la planificación y la ejecución de forma preventiva, mejorando y moldeando un criterio estandarizado en la toma de decisiones.

En tal sentido, este artículo abordará dos enfoques metodológicos científicos: el análisis mediante simulaciones de Monte Carlo y el uso de bases de datos preexistentes, con el objetivo de predecir y analizar las mejores decisiones posibles dentro de un entorno dinámico y altamente impredecible. En este contexto, se explorará cómo los métodos de análisis empleados en los juegos de guerra pueden optimizar la toma de decisiones y minimizar los riesgos, proponiendo que las acciones emprendidas sean las más adecuadas en cada escenario específico. Dado que la toma de decisiones implica inherentemente riesgos, acciones, reacciones y consecuencias, es crucial llevar a cabo un análisis detallado antes de actuar. Este análisis previo es fundamental para gestionar los potenciales escenarios y mitigar los resultados no deseados.

2. DESARROLLO

En los juegos de guerra, las decisiones tomadas en cada etapa impactan directamente los resultados futuros. Estas decisiones se comprenden mejor a través de los horizontes de planificación (Planning Horizons), gestionando la información, el riesgo asociado tanto a la fuerza como a la misión, y al timing oportuno para su implementación.

Mediante un análisis constante y sistemático del entorno operacional, es posible superar las brechas identificadas, adaptando las decisiones y los cursos de acción, y evaluando los factores internos y externos que influyen en la conducción de las operaciones navales.

Estos tres horizontes de planificación son:

- Operaciones actuales o concurrentes (Current Operations - COPS): Enfocadas en la ejecución inmediata de operaciones en curso. Su objetivo es monitorear, coordinar y ajustar acciones en tiempo real. Analogía con el ajedrez: Representan al jugador en la primera o segunda jugada, observando cada movimiento del oponente y tomando decisiones tácticas inmediatas para proteger sus piezas o capitalizar una ventaja, con información clara y perfecta.
- Operaciones futuras (Future Operations - FOPS): Enfocadas en el "¿qué pasaría si?". Valoran efectos, riesgos y reorientan operaciones según sea necesario. Buscan anticiparse a la evolución del entorno operacional y preparar respuestas ágiles. Analogía con el ajedrez: Corresponden al jugador que está pensando en la cuarta o quinta jugada adelante, identificando posibles movimientos del oponente y sus consecuencias, y preparando reacciones o maniobras de engaño.
- Planes futuros (Future Plans): Enfocados en el "¿qué sigue?". Incluyen planificación y evaluación de planes a largo plazo (MOC, 2013).Analogía con el ajedrez: Equivalen al jugador que diseña una estrategia integral de la partida, como controlar el centro del tablero, desarrollar una combinación a largo plazo o preparar un ataque posicional que definirá el rumbo del juego.

En tal sentido, en el horizonte de operaciones actuales o concurrentes (COPS), la toma de decisiones es principalmente reactiva y enfocada en la ejecución táctica, donde el rendimiento o *performance* (MOP[2]) y la efectividad (MOE[3]) se evalúan en tiempo real, demandando respuestas rápidas, precisas y ajustadas a la dinámica naval operativa inmediata. En el caso de las operaciones futuras (FOPS), las decisiones adquieren un carácter anticipatorio, mediante el análisis de escenarios hipotéticos (asumiendo supuestos), la valoración de riesgos y la constante adaptación de los planes operativos, a través de los FRAGORD[4] , permiten mantener la agilidad ante eventos inciertos o disruptivos.

Por su parte, en los planes futuros (FUPLANS), la toma de decisiones se orienta hacia la proyección estratégica de largo plazo, integrando el estudio de tendencias emergentes y amenazas futuras para desarrollar estrategias robustas, sostenibles y alineadas con los objetivos a gran escala. La integración efectiva

[2] MOP (Measure of Performance)

[3] MOE (Measure of Effectiveness)

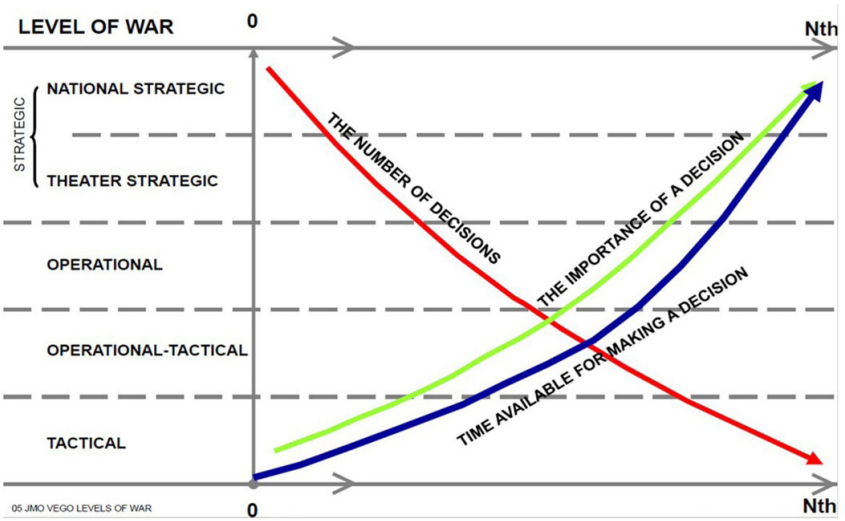
[4] FRAGORD (Fragmentary Order) es un tipo de orden militar que proporciona actualizaciones o cambios a una orden de operación previamente emitida (OPORD). Los FRAGORD se emiten típicamente cuando hay la necesidad de aclarar, ajustar o modificar un plan existente debido a nueva información, desarrollos o cambios en el entorno operacional.

de estos tres horizontes permite a los "decision makers" abordar con equilibrio tanto las demandas inmediatas como las incertidumbres a futuro. En este contexto, resulta fundamental tomar decisiones informadas a su medida y eficaces en cada horizonte, evaluando información que con frecuencia es incompleta, ambigua, engañosa o incierta, lo que obliga a los wargamers a ejercer un juicio crítico bajo presión y en condiciones de restricciones temporales y operativas. Por ello, la coordinación entre los tres horizontes de planificación se convierte en un factor clave para garantizar decisiones coherentes, adaptativas, resilientes y sostenibles en entornos altamente dinámicos y complejos. Sin embargo, este proceso está condicionado por la incertidumbre inherente a los conflictos, las capacidades del adversario y a las restricciones operativas y temporales, lo que obliga a decidir con información frecuentemente incompleta, imprecisa o engañosa. Por ello, el juicio y el pensamiento crítico, la flexibilidad y la capacidad de adaptación son esenciales.

Según este contexto, podemos mencionar al estratega británico Liddell Hart, quien en su libro Thoughts on war, define la guerra como ciencia y arte ligado a la sociología, enfatizando la explotación del elemento humano (human domain) en la guerra, en relación directa a la toma de decisiones, transversal a los otros dominios. Esto se asocia directamente, como menciona el Profesor Milan Vego, en función de las tres principales variables dependientes: el número de decisiones, la importancia de las decisiones y el tiempo disponible para tomar una decisión, como se aprecia en la Figura 2, la toma de decisiones en función de los niveles de la guerra.

FIGURA 2

Toma de decisiones en función de los niveles de la guerra.



Fuente: Milan Vego, Joint Operational Warfare, Theory, and Practice, 2013.

De igual manera, la figura muestra cómo varían las tres variables dependientes en la toma de decisiones a lo largo de los niveles de la guerra, desde el nivel estratégico hasta el táctico. A nivel táctico, los comandantes toman muchas decisiones en un corto período de tiempo, pero su impacto es limitado a situaciones específicas. En algunos casos puntuales, puede llegar a tener un impacto directo y exponencial en el nivel estratégico. Asimismo, a medida que se avanza hacia los niveles operacionales y estratégicos, la cantidad de decisiones disminuye, pero su importancia aumenta significativamente, debido a que pueden afectar el rumbo de toda una campaña u operación mayor.

De forma simultánea, por lo general, el tiempo disponible para analizarlas y tomarlas se amplía, permitiendo una planificación más detallada. En esencia, la figura ilustra cómo la toma de decisiones en la guerra cambia dependiendo del nivel, con decisiones rápidas y numerosas en el campo de batalla, y decisiones más trascendentales, pero menos frecuentes, en la conducción estratégica de una campaña u operación mayor. Como se aprecia en la figura, por lo general la dinámica de la toma de decisiones en los juegos de guerra se estructura en torno a varios factores, de los cuales destacan:

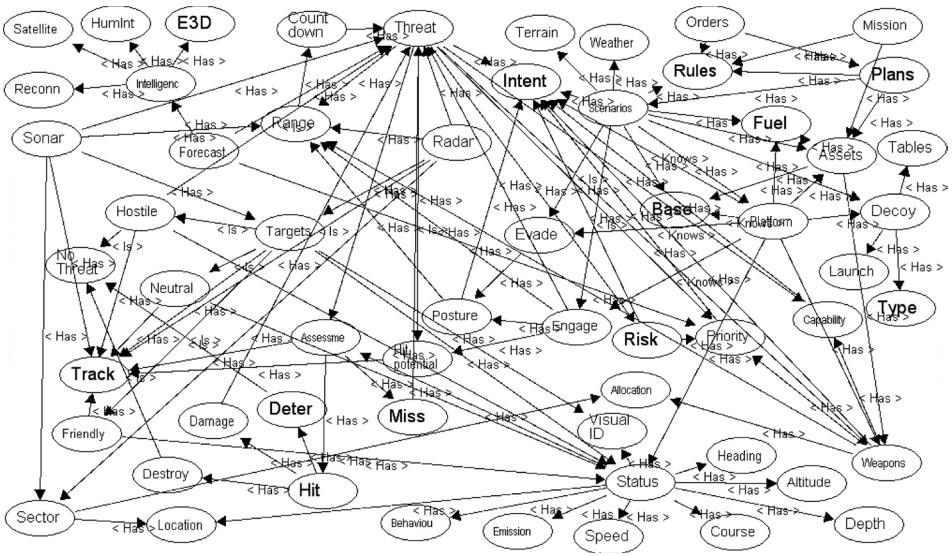
a. Tiempo: La curva azul en la imagen muestra que a medida que se asciende en los niveles de la guerra (de táctico a estratégico), el tiempo disponible para la toma de decisiones aumenta. En el nivel táctico, las decisiones deben tomarse en segundos o minutos debido a la inmediatez del combate, mientras que en el nivel estratégico, los líderes pueden disponer de mayor tiempo para evaluar información y planificar.
b. Cantidad de decisiones: La curva roja, que representa la cantidad de decisiones, disminuye a medida que se avanza hacia niveles más altos. Es decir, a nivel táctico y operacional se deben tomar muchas más decisiones en comparación con los niveles más estratégicos. Esto refleja cómo, en los niveles de la guerra más bajos (como en el campo de batalla), los "decision makers" toman muchas más decisiones en un corto periodo de tiempo. En este contexto, es esencial entrenar, agilizar la capacidad de análisis y optimizar la toma de decisiones, proporcionando experiencias a través de simulaciones o juegos de guerra a los "decision makers". De esta manera, se puede reducir el riesgo y garantizar que las acciones sean las más adecuadas en cada situación específica.

c. Escalabilidad: La curva verde muestra que la importancia de las decisiones crece a medida que se sube en los niveles de la guerra. En el nivel táctico, las decisiones afectan eventos localizados, mientras que, en el nivel estratégico, una sola decisión puede influir en toda la guerra o en la política nacional. Esto ilustra la escalabilidad del impacto de las decisiones: a medida que se asciende en la jerarquía, las decisiones se vuelven menos frecuentes, pero su alcance y consecuencias aumentan exponencialmente.

A la dinámica de los factores previamente mencionados en la toma de decisiones se suma el factor operacional: el espacio. En el ámbito marítimo, las operaciones navales son implacables, exigentes, solitarias y ponen a prueba los límites de cada comandante (Benson, 2019). Este entorno está marcado por múltiples elementos interrelacionados que constituyen variables y procesos cruciales en la adopción de decisiones tácticas en los distintos niveles de una organización de tarea, como se aprecia en la Figura 3. En este contexto, los comandantes asumen una responsabilidad absoluta al decidir tanto de manera instintiva como deliberada. Sin embargo, algunas de estas decisiones pueden derivar en resultados adversos, lo que refleja las dificultades inherentes a la toma de decisiones en operaciones navales.

FIGURA 3

Toma de decisiones en un entorno complejo de múltiples variables.



Fuente: Distributed situation awareness in collaborative systems

Hay muchos ejemplos en la historia, sobre todo de la Segunda Guerra Mundial, que resaltan los desafíos de la toma de decisiones militares. El almirante Arleigh Burke reflexionó sobre su experiencia en combate y mencionó que:

> "Todos los hombres que han estado en combate, comprenden y saben que uno de los requisitos fundamentales para ganar batallas es contar con comandantes que sepan tomar decisiones, usar su fuerza, tengan la iniciativa, el conocimiento necesario para tomar las medidas adecuadas cuando las cosas salen mal y que estén dispuestos a asumir la gran responsabilidad de liderar a sus hombres en la batalla. Los hombres que luchan con habilidad, vigor y un profundo sentido del deber, deben contar con comandantes competentes que sean inspiradores". (Benson, 2019)

Ahora bien, al analizar la toma de decisiones en el ajedrez, es evidente que cada elección puede alterar drásticamente el curso de la partida. Por ello, es fundamental contar con herramientas analíticas que permitan evaluar múltiples opciones de forma sistemática y rigurosa.

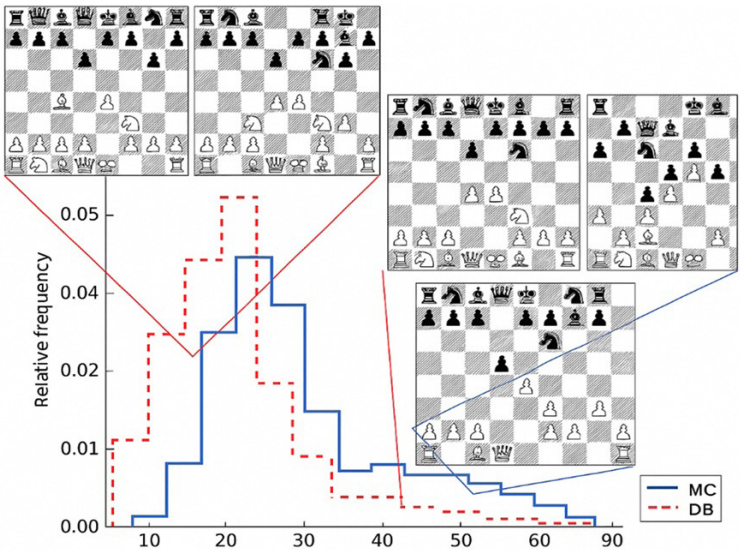
En este contexto, los métodos de simulación y el análisis de datos o registros históricos desempeñan un papel clave. Un ejemplo destacado es la simulación de **Monte Carlo (MC)**, ampliamente utilizada en juegos de guerra para modelar escenarios bajo condiciones de incertidumbre y que también se aplica en el ajedrez para explorar distintas secuencias de movimientos y sus posibles desenlaces. Tal como se aprecia en la Figura 4, se presenta un análisis comparativo de la "longitud de los caminos" (en plies) entre pares aleatorios de estados de ajedrez, contrastando dos enfoques: **Monte Carlo (MC)**, basado en simulaciones aleatorias, y **Database (DB)**, sustentado en registros históricos de partidas reales. En el eje vertical se representa la distribución de frecuencias de dichas longitudes, lo que permite observar que algunos "cursos de acción" son más recurrentes que otros. En particular, el enfoque DB refleja las tendencias empíricas del juego humano, mientras que el enfoque MC ofrece una perspectiva más amplia y no restringida de los "cursos de acción" posibles, permitiendo así evidenciar tanto los **EMLCOA**[5] (Cursos de acción más probables) como los **EMDCOA**[6] (Cursos de acción más peligrosos), y con ello, las relaciones recíprocas entre ataque y defensa, que estructuran la dinámica del juego.

[5] EML = Enemy Most Likely (COA).

[6] EMD = Enemy Most Dangerous (COA)

FIGURA 4

Distribución de las longitudes de los caminos entre pares aleatorios de estados de ajedrez



Fuente: Atashpendar, A., Schilling, T., & Voigtmann, T. (2016). Sequencing Chess. Distribution of path lengths between randomly selected pairs of chess positions.

Esta visualización facilita la identificación de patrones de comportamiento y la evaluación de riesgos y oportunidades, al analizar las trayectorias más frecuentes o efectivas. De manera similar a los juegos de guerra, el uso de simulaciones en ajedrez no solo mejora la comprensión de la dinámica del juego, sino que también optimiza la toma de decisiones. Esto se logra al permitir anticipar eventos y elegir el curso de acción más favorable y robusto. Además, la efectividad de este proceso es directamente proporcional al número de repeticiones de sucesos realizadas con decisiones aleatorias. Este enfoque de análisis basado en bases de datos, al utilizar registros históricos de decisiones previas tomadas en situaciones similares, permite optimizar la calidad y la reflexión en la toma de decisiones.

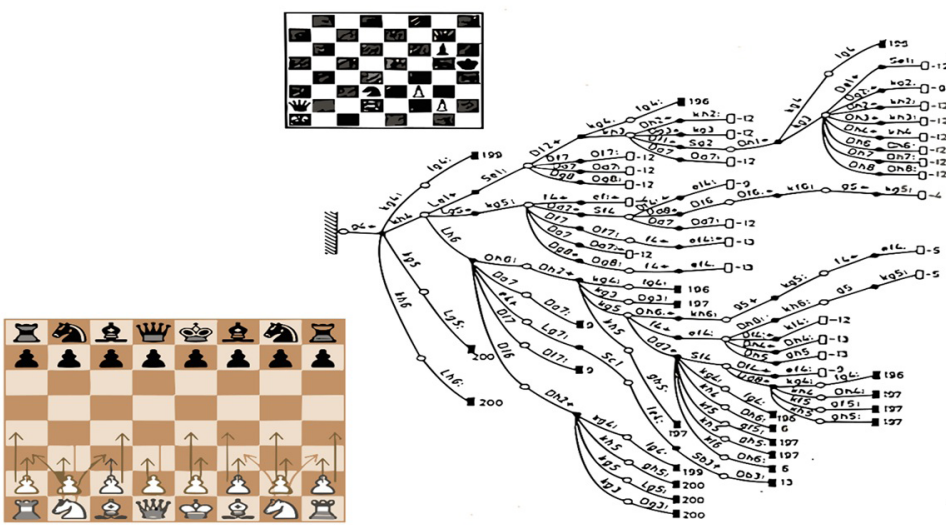
Este método se centra en estudiar decisiones del pasado para identificar patrones y comportamientos previos, lo que permite prever posibles escenarios en situaciones futuras similares empleando progresiones regresivas, que han demostrado ser buenas prácticas; mientras que las simulaciones de Monte Carlo emplean técnicas que utilizan la aleatoriedad para resolver problemas matemáticos, de optimización o evaluación, explorando una amplia gama de escenarios erráticos. Estas simulaciones son especialmente útiles cuando no se puede obtener una solución exacta debido a la complejidad del sistema o la falta de un modelo determinista, obteniendo una amplia distribución de situaciones y

desenlaces, siendo no aplicable una distribución normal en la campana de Gauss. Esto depende bastante de cómo se formuló el problema en el escenario del juego de guerra y de las distribuciones de probabilidad de los eventos que se estén modelando, por lo general por el White cell[7] .

Como se aprecia en la Figura 5, en relación directa a los patrones y comportamientos previos, la siguiente figura representa un árbol de decisiones que modela el desarrollo de una partida de ajedrez, la cual la podemos asociar a un curso de acción ramificado (Multiple Courses of Action with Multiple Branches), donde cada rama simboliza una posible jugada y su impacto en la evolución de la partida. Este tipo de representación es crucial en la toma de decisiones de los juegos de guerra, debido a que permite visualizar cómo una elección de un curso de acción en un momento determinado puede derivar en múltiples ramificaciones secuenciales, mostrando algunos escenarios favorables y otros desfavorables. La estructura del árbol de decisiones vincula los métodos de simulación de Monte Carlo, comúnmente utilizados para evaluar escenarios en condiciones de incertidumbre mediante simulaciones aleatorias, con datos históricos y registros. Además, incorpora evaluaciones que asignan valores a cada decisión,

FIGURA 5

Ramificación de las decisiones y sus posibles consecuencias



Fuente: Diagrams for Dynamic Space.

[7] White Cell: es un equipo de control y coordinación utilizado principalmente durante ejercicios de juegos de guerra y simulaciones en diferentes escenarios. (MOC, 2013)

que se materializa en un movimiento (en función de los factores gobernantes). Este enfoque permite un análisis más estructurado basado en patrones, el cual, generalmente, refleja la comprensión y las lecciones aprendidas a lo largo de las decisiones de cada curso de acción.

Por tal motivo, la integración de los métodos de Monte Carlo y análisis basado en bases de datos (DB) permite llevar a cabo análisis exhaustivos y robustos en la toma de decisiones. Cada uno de estos enfoques tiene ventajas específicas y es aplicable en distintos contextos, lo que potencia la capacidad de tomar decisiones. A continuación, se detallan los principales beneficios de su combinación:

- Mejora en la previsibilidad: La simulación de Monte Carlo ofrece una visión amplia de los posibles resultados futuros, al explorar diversas combinaciones de eventos. Por otro lado, el análisis de bases de datos proporciona una visión detallada y precisa sobre decisiones pasadas. Combinados, estos métodos aumentan significativamente la capacidad para prever los resultados con mayor certeza.
- Análisis comparativo: La comparación entre las decisiones tomadas por el wargamer y las de su oponente permite evaluar la efectividad de las tácticas empleadas. Este análisis facilita la identificación de áreas de mejora y la adaptación de tácticas para ganar una ventaja considerable.
- Optimización continua: Estos métodos permiten ajustar las decisiones de manera dinámica, a medida que se recopilan más datos durante el desarrollo de los juegos de guerra. Esto facilita una mejora constante en la flexibilidad y la adaptación ante nuevas circunstancias.
- Reducción de incertidumbre: Al combinar simulaciones y análisis históricos, se disminuye considerablemente la incertidumbre en el proceso de toma de decisiones. Esto proporciona una base más sólida para tomar decisiones y aumenta la confianza en la elección de los mejores cursos de acción.
- Adaptación a cambios en el entorno: La flexibilidad de estos métodos permite ajustar las decisiones conforme varían las condiciones del entorno o el comportamiento del adversario. Esta adaptabilidad es esencial para mantener la ventaja competitiva y reaccionar de manera efectiva, tomando la iniciativa ante situaciones inesperadas.

Esto va de la mano con lo que Clausewitz sostenía, que el alcance del azar en la guerra debería y podría reducirse al mínimo mediante el empleo de la doctrina operativa y táctica correcta. En función de la teoría, poner todo en orden sistemático, de forma clara y exhaustiva, y rastrear cada acción hasta una causa adecuada y convincente (Howard & Paret, 1989, p. 577), como parte del profundo entendimiento de las progresiones regresivas en la historia (casos de estudio) y de su impacto directo, en relación con la geografía en las distintas guerras. (Mujica, 2023)

En este mismo sentido, el análisis sustentado en bases de datos históricas, que emplea registros, destaca la idea de que la historia es cíclica. Esta perspectiva, conocida como la "Ley de los Ciclos", sostiene que los eventos y patrones del pasado tienden a repetirse de manera continua a lo largo del tiempo. Ray Dalio propone que todos los sistemas, incluidos los económicos y políticos, están sujetos a estos ciclos naturales de expansión y contracción. Esta perspectiva ofrece una herramienta valiosa para entender y predecir las tendencias históricas. Sin embargo, es importante señalar que, aunque los ciclos son similares, cada uno es único y está condicionado por factores complejos y circunstanciales.

En su libro “Principles for Dealing with the Changing World Order”, ofrece un enfoque integral sobre los ciclos históricos de poder y riqueza, proporcionando una visión profunda de cómo las potencias globales han experimentado ascensos y declives a lo largo del tiempo. A través de su análisis, Ray Dalio identifica diversos factores que influyen en estos ciclos, como la deuda externa, las fluctuaciones económicas, y la interacción entre el orden interno y externo de las naciones-estado, en un contexto de creciente globalización (Dalio, 2021). Este enfoque resulta ideal para la elaboración de progresiones regresivas y prospectivas de escenarios, las cuales permiten formular escenarios para la realización de los juegos de guerra, comprendiendo el análisis global e interconectado de los factores internos y externos, como los movimientos políticos, económicos y geopolíticos, que afectan el dinamismo de las decisiones. Este enfoque permite anticipar cambios en la dinámica mundial y abordar las tensiones internacionales con mayor preparación y perspectiva estratégica, operacional y táctica.

De igual forma, se resalta la importancia de comprender estos patrones históricos para tomar decisiones informadas en el presente y anticipar con mayor claridad los posibles escenarios futuros. De esta manera, ofrece herramientas clave para navegar en un mundo cada vez más incierto. Un ejemplo fundamental es la diversificación de activos, asociada con la gestión de recursos en los juegos de guerra. La idea de distribuir adecuadamente los recursos para enfrentar múltiples

amenazas y escenarios posibles se convierte en una herramienta esencial. En este sentido, la diversificación permite mitigar los riesgos derivados de eventos impredecibles y aprovechar las fluctuaciones económicas de manera estratégica, ayudando en la adecuada determinación de la estructura y magnitud de fuerzas, un concepto clave para el diseño de armas combinadas[8].

Otro principio importante es el uso de reglas sistemáticas de toma de decisiones. Al definir previamente cómo actuar frente a diferentes escenarios, ***los wargamers*** **pueden optimizar su capacidad de tomar decisiones con rapidez, claridad y objetividad, evitando que factores emocionales o de pánico interfieran en el proceso.**

Este enfoque se aplica directamente en los juegos de guerra, donde la capacidad de tomar decisiones rápidas y eficaces en el nivel táctico puede marcar la diferencia entre el éxito y el fracaso, con un criterio común y uniforme en los *teams* de combate, resaltando el papel del TAO (Tactical Action Officer) en un proceso táctico. Asimismo, la mentalidad flexible y resiliente es otro principio esencial que requieren los *wargamers* para la toma de decisiones, permitiendo adoptar una actitud de aprendizaje continuo y estando dispuestos a ajustar las tácticas según las condiciones cambiantes del entorno operacional y en función directa de las nuevas tecnologías emergentes.

En ese sentido, la dimensión cognitiva se configura como un pilar de la supervivencia, dado que la velocidad y la claridad de juicio son tan determinantes como las capacidades propias de la plataforma. En concordancia con esta perspectiva, Clausewitz (1976) mencionaba que "el propósito de la teoría es educar la mente del futuro comandante" (p. 141), insistiendo en que la teoría no prescribe manuales de acción, sino que perfecciona el pensamiento estructurado y crítico de quienes deben decidir bajo presión. (Mujica, 2025, p. 56).

En conjunto, estas herramientas ofrecen un marco poderoso para entender y adaptarse a un entorno global en constante cambio. El conocimiento de los ciclos históricos no solo ayuda a tomar decisiones más informadas, sino que también proporciona las bases para navegar en los retos del futuro con mayor certeza. Al integrar estas herramientas en los juegos de guerra, los wargamers pueden formular decisiones más eficaces, basadas en una comprensión profunda de los ciclos históricos, los escenarios cambiantes y la interacción e interoperabilidad de los elementos de tarea de una fuerza naval.

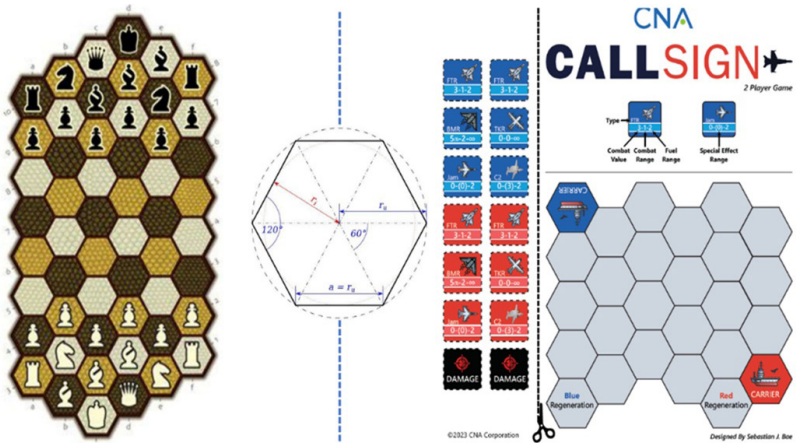
[8] Mujica Caballero, M. (2025). Aproximación a una metodología híbrida para el diseño de fuerzas navales: una guía de Planeamiento Estratégico para la defensa basada en prospectivas de escenario, considerando amenazas y capacidades. Revista de Marina, (2025, núm. 2)

Por lo tanto, el ajedrez, al igual que en juegos de guerra, permite la capacidad de anticipar las consecuencias de cada acción en particular. La combinación de simulaciones, datos históricos y modelos de decisión permite optimizar la identificación de los cursos de acción con mayor probabilidad de éxito, evitando aquellos que conducen a situaciones desventajosas. Este enfoque no solo mejora la comprensión táctica del juego, sino que también ofrece valiosas lecciones aplicables a contextos más amplios, como la planificación operativa y la determinación de la concepción estratégica, donde la evaluación sistemática de múltiples escenarios y cursos de acción es crucial para una toma de decisiones efectiva.

En este caso, se presenta en la Figura 6 la similitud entre el ajedrez y los juegos de guerra, destacando el papel del hexágono como una figura geométrica idónea, ampliamente utilizada en la representación de los ejercicios sobre la carta o Table-Top Exercise (TTX), como: Kriegsspiel, Operational Wargame System, War at Sea, Littoral Commander, Indo- Pacific, Cyber combat game, Naval Kriegsspiel, Malign[9] ; y sus sistemas de movimiento. Si bien su estructura optimiza la movilidad y el equilibrio entre direcciones, el hexágono por sí solo no define un juego de guerra. La verdadera esencia de los juegos de guerra radica en la dinámica de toma de decisiones, el análisis de escenarios y la adaptación a los cambios constantes; elementos que también se reflejan en el ajedrez.

FIGURA 6

Similitud entre el ajedrez y los juegos de guerra.



Fuente: Internet, adaptación propia.

[9] Mujica Caballero, M. (2023). Juegos de Guerra: una poderosa herramienta prospectiva, analítica y didáctica. Revista de la Escuela Superior De Guerra Naval, 20(2), 26-43. Recuperado a partir de https://revista.esup.edu.pe/RESUP/article/view/160

En cambio, la Figura 7 presenta un ejercicio más complejo que el expuesto en la Figura 6, materializado sobre la carta o Table-Top Exercise (TTX), basado en un escenario específico denominado "Falklands-Malvinas, 1982," por su creador Operational Wargame System. Este sistema de juego de guerra simula las operaciones militares ocurridas durante el conflicto de las Malvinas, utilizando fichas que representan aviones, buques y otros elementos militares distribuidos en un mapa hexagonal. Este mapa refleja la disposición y composición de las organizaciones de tareas, así como sus movimientos. Este tipo de ejercicio permite la reconstrucción de hechos históricos y la formulación de hipótesis sobre eventos con desenlaces alternativos, promoviendo el análisis y la evaluación de diversas posibilidades. A través de este enfoque, los wargamers desarrollan un pensamiento crítico mediante discusiones profesionales, explorando nuevas tácticas y enfoques innovadores. Esta experiencia inmersiva, tanto en escenarios históricos como hipotéticos, fomenta la creatividad y la innovación táctica o estratégica, según sea el caso. Los TTX, en el contexto de la andragogía, permiten que los wargamers aprendan de manera didáctica, asumiendo una mayor responsabilidad en su propio proceso de aprendizaje y toma de decisiones a través de resolución de problemas, que aborde situaciones prácticas e históricas, estrechamente vinculadas a la conducción de una fuerza naval.

FIGURA 7

Simposio de Juegos de Guerra, Operational Wargame System, Falklands-Malvinas, 1982

Fuente: Escuela Superior de Guerra Naval, 2023.

En este contexto, la "Decision Support Matrix" (DSM) constituye una herramienta fundamental para los TTX, debido a que se articula con los dos enfoques anteriormente argumentados: Monte Carlo (MC), basado en simulaciones aleatorias, y Database (DB), sustentado en registros históricos. Su relevancia radica en que ofrece un marco sistemático para evaluar múltiples opciones de decisión, algo esencial cuando se deben considerar numerosas variables, tales como tácticas, recursos disponibles, tiempo, riesgos y efectos esperados en relación con las tareas y objetivos previstos. De este modo, la DSM facilita que los participantes en un TTX sigan un proceso de toma de decisiones más estructurado y objetivo, permitiendo analizar alternativas no solo en función de la repetición de sucesos con decisiones aleatorias, sino también de su efectividad para alcanzar los objetivos establecidos.

Además, permite visualizar de forma clara los posibles efectos secundarios de cada decisión, como el impacto en otras tareas o en la relación de comandos, lo que mejora la capacidad de anticiparse a consecuencias no deseadas. Por estos motivos, la clave del DSM es que no solo ayuda a formular decisiones durante un evento, sino que también fomenta la reflexión crítica sobre cada opción y sus consecuencias. En estos ejercicios, se presentan varios "puntos de decisión", momentos específicos donde se anticipan decisiones cruciales que afectarán el desarrollo de la misión. Estos puntos de decisión están relacionados con eventos críticos, como la aparición de una amenaza no programada por el targeting o la pérdida de una capacidad operacional esencial para el cumplimento de la misión, y se apoyan en los CCIR[10] (Requerimientos Críticos de Información del Comandante), que son requisitos de información que el comandante necesita para tomar decisiones rápidas y efectivas. Entre estos requisitos encontramos los PIR[11](Requerimientos Prioritarios de Información), que son esenciales para comprender al adversario y el entorno operacional; y finalmente, los FFIR[12] (Requerimiento de información de fuerzas amigas), que se centran en el estado de operatividad, composición, disposición y las capacidades de las fuerzas propias en relación con los factores operacionales: Fuerza, Espacio y Tiempo.

Es así que el Decision Support Matrix (DSM) organiza las decisiones tácticas mediante estructuras estandarizadas, entre las que destaca el DRAW-DDA-NG[13] (Defender, Reforzar, Atacar, Retirar, Retrasar, Desviar, Abortar, No-go). Este es

[10] CCIR: Commander's Critical Information Requirements

[11] PIR: Priority Intelligence Requirement

[12] FFIR: Friendly Forces Information Requirement

[13] **DRAW-DDA-NG: Defender, Reinforce, Attack, Withdraw, Delay, Divert, Abort, No-go.**

un acrónimo que se utiliza con frecuencia en la planificación militar para describir las posibles decisiones tácticas que un comandante puede tomar en respuesta a las acciones del adversario, directamente relacionado con el DSM. Las decisiones tácticas esenciales pueden ser descritas de la siguiente forma:

- **Defender**: Mantener la posición y defenderla de los ataques enemigos.
- **Reforzar**: Enviar más fuerzas o recursos para fortalecer una posición o unidad que está en peligro o bajo ataque.
- **Atacar**: Lanzar un ataque para tomar la iniciativa o destruir al enemigo.
- **Retirar**: Retirarse de la posición para evitar más pérdidas o para reorganizar las fuerzas.
- **Retrasar**: Retrasar las acciones del enemigo, normalmente para ganar tiempo o evitar que tomen una posición favorable.
- **Desviar**: Cambiar el objetivo o la misión de manera intencional para confundir al enemigo, hacer que gaste recursos o atención en una dirección equivocada.
- **Abortar**: Detener de manera abrupta una acción o misión en curso debido a un cambio en las circunstancias, una amenaza o la imposibilidad de lograr los objetivos de la misión.
- **No-go**: Esta decisión implica que no se debe proceder con la acción o misión planeada debido a que existen condiciones que hacen imposible o inviable su realización, como factores logísticos, tácticos o condiciones no favorables.

En este contexto, el *Decision Support Matrix* se complementa perfectamente con la comprensión de la geometría del teatro[14] , representada en la carta o TTX. Juntas, estas herramientas son fundamentales en la planificación y ejecución de operaciones navales en el dominio marítimo. La geometría del teatro se centra en elementos clave de cualquier área de operaciones, como las posiciones, distancias, bases de operación, objetivos físicos, puntos decisivos y las líneas de comunicación.

Por su parte, el Decision Support Matrix ayuda a estructurar decisiones tácticas esenciales, expuestas anteriormente. Al combinarse con la geometría del teatro, ambas permiten evaluar las opciones disponibles según la disposición en el entorno operacional y las dinámicas propias del campo de batalla, lo que brinda a los comandantes la capacidad de adaptarse rápidamente a las condiciones del terreno y a las acciones del adversario. Esta sinergia no solo maximiza la

[14] Geometría del Teatro (Theater Geometry), College of Maritime Operational Warfare, U.S. Naval War College,2021

efectividad de las decisiones, sino que también permite generar múltiples cursos de acción, cada uno evaluado según criterios críticos como tiempo, recursos, impacto en la misión y riesgos para la fuerza. Así, los comandantes pueden tomar decisiones informadas y ajustar tácticas y estrategias, según sea el caso, de manera eficiente a lo largo del desarrollo de las operaciones navales, garantizando que las decisiones sean las más adecuadas para el contexto específico.

En tal sentido, se presenta el siguiente cuadro, como ejemplo, materializando lo explicado en el presente artículo.

TABLA 1
Matriz de apoyo a las decisiones

	CCIR	**Opciones de decisión**	**Criterios de apoyo a la toma de decisiones**	**Ubicación**
1	Detección de campo minado en el estrecho (choke point) A. Situación del Control de zonas críticas.	**1A:** El CTF 182 transita por el estrecho B en lugar del estrecho A	Efectos sobre otras tareas asignadas al CTF 182	NAI 3
		1B: Reasignar la tarea al CTF 183	Tiempo previsto para despejar el estrecho B	
		1C: Retrasar la operación hasta que se despeje el estrecho A	Efectos del retraso en la operación, conectores de superficie no disponibles	
2	Condiciones climáticas adversas que afectan las operaciones	**2A:** Retrasar la misión hasta que mejore el tiempo (No-go)	Impacto en el matriz de sincronización	NAI 5
		2B: Ajustar el COA para evitar la zona afectada	Mayor consumo de combustible y logística. Reevaluar la geometría del teatro.	
		2C: Continuar con las operaciones aumentando el riesgo a la fuerza y misión	Impacto severo en las operaciones para el cumplimiento de la misión	

3	Situación y capacidades del enemigo	**3A:** Análisis de las capacidades de combate del enemigo	Evaluar la disposición de las fuerzas enemigas, su localización y el tipo de armas que emplea	NAI 2
		3B: Despliegue de fuerzas para contrarrestar al enemigo	Necesidad de concentrar fuerzas en áreas críticas para neutralizar la amenaza	NAI 1
		3C: Desviar al enemigo, hacia una dirección equivocada	Impacto en la capacidad de respuesta del enemigo	NAI 2
4	Situación del control local del mar	**4A:** Establecer control temporal en áreas críticas	Evaluar el impacto en la libertad de maniobra y los recursos disponibles	NAI 5,8
		4B: Reforzar la presencia en áreas disputadas para asegurar rutas de navegación	Aumentar la cantidad de elementos de tarea en el área D	
		4C: Continuar con la misión bajo condiciones de alto riesgo en el área	Evaluar la viabilidad de las operaciones y el riesgo del no-go de la misión	

5	El CTF pierde una capacidad operativa crítica	**5A:** Reasignar fuerzas para restaurar la capacidad.	Efecto en el CTF desde la que se reasignó la capacidad.	NAI 1, 3, 4, 7, 9
		5B: Reasignar la tarea a una CTF con la capacidad.	Capacidad de otro CTF para aceptar la tarea.	
		5C: Solicitar asistencia del comando de apoyo.	Capacidad de un comando de apoyo para asumir la tarea.	
6	Fallo de las comunicaciones en la Fuerza de Tarea	**6A:** Intentar restaurar los sistemas de comunicación principales.	Tiempo estimado para restaurar los sistemas.	NAI 1,2, 3, 4, 7, 9
		6B: Cambiar a métodos de comunicación secundarios o alternativos.	Confiabilidad de las comunicaciones de respaldo. Matriz de riesgo a la fuerza y a la misión: RAC (Calculating the Risk Assessment Code)	
		6C: Reasignar las funciones de C2 a una unidad con comunicaciones intactas.	Impacto en la interoperabilidad	

7	Submarino enemigo detectado cerca del convoy	**7A:** Desplegar elementos de tarea de guerra antisubmarina (ASW) para localizarlo y rastrearlo.	Probabilidad de detectar y neutralizar el submarino. RCP > 2.5:1	NAI 2
		7B: Cambiar la ruta del convoy para evitar la amenaza.	Impacto en la matriz de sincronización y en el cumplimiento de la misión.	
		7C: Aumentar la protección de la escolta del convoy	Disponibilidad de unidades de escolta	

Fuente: Joint Military Operations' seminar, Naval Staff College, U.S. Naval War College, 2023.

Finalmente, la relación entre la teoría y la práctica (simulación aplicada) en el ajedrez y en los juegos de guerra destaca la importancia de estructurar el pensamiento del que tomará las decisiones. Como señalaba Clausewitz, la teoría no es un manual rígido de acción, sino una herramienta para formar mentes capaces de analizar múltiples escenarios y tomar decisiones informadas bajo incertidumbre, educando a la mente para enfrentar la incertidumbre con pensamiento crítico y estructurado[15] .

La combinación de modelos probabilísticos, datos históricos y simulaciones refuerza esta capacidad, permitiendo no solo anticipar posibles desenlaces, sino también mejorar continuamente la toma de decisiones, maximizando las oportunidades de éxito y minimizando los riesgos. Esto implica también el de comprender el nivel de competencias, conocimiento y experiencia de cada *decision-maker*, donde los comandantes se entrenan y capacitan para tomar decisiones y asignar tareas en consecuencia.

[15] Michael Howard and Peter Paret (1989), On War, Carl von Clausewitz, Princeton University Press. Page 141.

En última instancia, en el campo de batalla o en el tablero de ajedrez, el éxito depende no solo de la teoría, sino de la capacidad de aplicarla con criterio y visión.

3. CONCLUSIONES

La toma de decisiones en juegos de guerra requiere adaptabilidad y manejo de la incertidumbre, donde los wargamers deben tomar decisiones basadas en información imperfecta, entrenándose con simulaciones y datos históricos, para prever posibles resultados y reducir los riesgos.

El uso combinado de simulaciones y análisis histórico mejora la previsibilidad y la capacidad de adaptación, permitiendo predecir escenarios futuros y ajustar decisiones en función de cambios constantes en el entorno.

La teoría aplicada en la práctica fortalece la capacidad de tomar decisiones informadas, dando un enfoque crítico y estructurado, basado en simulaciones y análisis previos, siendo esencial para maximizar el éxito y minimizar riesgos en contextos de incertidumbre, constituyendo un factor clave las perspectivas e interpretaciones[16] de los "wargamers".

Es esencial comprender la prospectiva de escenarios, haciendo una retrospectiva de acontecimientos en base a una correlación de datos, a fin de generar patrones en sucesos futuros, explotando directrices junto con factores potencialmente causales de acciones, reacciones y consecuencias ligados directamente a un enfoque analítico mixto (cuantitativo y cualitativo).

[16] Mujica Caballero, M. (2024). Perspectivas e interpretaciones en torno a los Juegos de Guerra a partir de la visión de Sun Tzu y Clausewitz. Revista De La Escuela Superior De Guerra Naval, 21(1), 81-89. Recuperado a partir de: https://revista.esup.edu.pe/RESUP/article/view/190

Referencias

Air Land Sea Application (ALSA) Center. (2005). FM 3-09.34 Kill Box Tactics and Multiservice Procedures | Public Intelligence. Publicintelligence.net. https://publicintelligence.net/fm-3-09-34-kill-box-tactics-and-multiservice-procedures/

Atashpendar, A., Schilling, T., & Voigtmann, T. (2016). Sequencing chess. EPL (Europhysics Letters), 116(1), 10009. Retrieved from: https://doi.org/10.1209/0295-5075/116/10009

Benson, J. W. (2019, December 23). Prepare for Decision-Making at Sea. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/2019/december/prepare-decision-making-sea

Dalio, R. (2021). Principles for dealing with the changing world order. Simon & Schuster.

Daniel J. Hughes (1995), Moltke on the Art of War: Selected Writings

Hanley, J. T. (2023). The US Navy and the National Security Establishment: A Critical Assessment. Lynne Rienner Publishers.

Hart, L. (1944). Thoughts on war. Faber.

Michael Howard and Peter Paret (1989), On War, Carl von Clausewitz, Princeton University Press.

Milan Vego (2020), General Naval Tactics: Theory and Practice.

Mujica Caballero, M. (2023). Juegos de Guerra: una poderosa herramienta prospectiva, analítica y didáctica. Revista De La Escuela Superior De Guerra Naval, 20(2), 26-43. Recuperado a partir de https://revista.esup.edu.pe/RESUP/article/view/160

Mujica Caballero, M. (2024). Perspectivas e interpretaciones en torno a los Juegos de Guerra a partir de la visión de Sun Tzu y Clausewitz. Revista De La Escuela Superior De Guerra Naval, 21(1), 81-89. Recuperado a partir de: https://revista.esup.edu.pe/RESUP/article/view/190

Mujica Caballero, M. (2025). Aproximación a una metodología híbrida para el diseño de fuerzas navales: una guía de Planeamiento Estratégico para la defensa basada en prospectivas de escenario, considerando amenazas y capacidades. Revista de Marina, (2025, núm. 2)

Mujica Caballero, M. (2025). Explorando la susceptibilidad, vulnerabilidad y recuperación de las plataformas de superficie ante amenazas de misiles de crucero anti-buque (ASCM). Revista de Marina, (2025, núm. 3)

Norman Friedman (2017), Winning a future war, Wargaming and victory in the Pacific War

Roger Harris Hill (1968), How the Influence of Wargaming on the Schlieffen Plan

Rubel, R. C. (2018, December 12). Then What? Wargaming the Interface Between Strategy and Operations. Center for International Maritime Security. https://cimsec.org/then-what-wargaming-the-interface-between-strategy-and-operations-pt-1/

Salmon, P. M., Walker, G. H., Stanton, N. A., & Baber, C. (2006). Distributed situation awareness in collaborative systems: A case study in the energy distribution domain. Ergonomics, 49(12-13), 1288–1311. https://doi.org/10.1080/00140130600612762

Trent Hone (2018), Learning War: The Evolution of Fighting Doctrine in the U.S. Navy, 1898–1945.

U.S. Navy. (2013). NTTP 3-32.1: Maritime Operations Center (April 2013). U.S. Department of the Navy.

Whitney, V. (2019, May 27). Diagrams for Dynamic Space - Measuring the Great Indoors - Medium. Medium; Measuring the Great Indoors. Retrieved from: https://medium.com/measuring-the-great-indoors/diagrams-for-dynamic-space-896e67e8ed8

Año 2025, Vol. 22, Nº 3, pp. 33 - 43.
DOI: https://doi.org/10.35628/resup.v16i2.171

El crimen organizado transnacional como amenaza estratégica para el Perú: riesgos, implicancias y desafíos para el Sector Defensa

The transnational organized crime as a strategic threat to Peru: risks, implications, and challenges for the Defense Sector

Recibido: 22 de septiembre del 2025 | Aceptado: 03 de diciembre del 2025

Anshella Lizbeth Díaz Macedo
https://orcid.org/0009-0008-5556-407X

Abogada con dieciséis años de ejercicio profesional. Magíster en Derecho Constitucional y Administrativo, egresada de la Maestría en Derecho Registral y Notarial por la Universidad de San Martín de Porres y del Doctorado en Derecho por la Universidad Privada Antenor Orrego. Cuenta con especialización en Técnicas de Litigación Oral por la Universidad Western – California, San Diego, EE. UU. Ha ejercido funciones en el sector público y privado en áreas vinculadas a la función pública, la gestión administrativa y el control gubernamental. Es docente universitaria en la Escuela Nacional de Control de la Contraloría General de la República y ha sido docente invitada en la Universidad del Pacífico, la Universidad Nacional del Santa y la Universidad César Vallejo.
Actualmente labora en la Contraloría General de la República, en la Subgerencia de Coordinación Parlamentaria. Combina su labor profesional con la investigación y docencia, consolidándose como especialista comprometida con el desarrollo del Derecho y la mejora institucional.
Email:anshellad@gmail.com

Resumen: La criminalidad organizada transnacional (COT) representa una seria amenaza para la seguridad global y el desarrollo sostenible. Este fenómeno complejo abarca diversas actividades ilícitas que trascienden las fronteras nacionales, incluyendo el tráfico de drogas, la trata de personas, el lavado de dinero, el tráfico de armas, la ciberdelincuencia y la explotación de recursos naturales, entre otros. La COT se caracteriza por la existencia de estructuras jerárquicas, la búsqueda de beneficios económicos y la capacidad de corromper instituciones estatales y privadas.

Este artículo analiza la naturaleza multifacética de la COT, examinando sus principales manifestaciones, los factores que facilitan su expansión (como la globalización, los avances tecnológicos y las desigualdades socioeconómicas), y su impacto en la estabilidad política, la economía y la sociedad. Se exploran las

estrategias y los mecanismos de cooperación internacional implementados para combatir este flagelo, así como los desafíos y las limitaciones que aún persisten en la lucha contra las redes criminales transnacionales. El objetivo principal es definir correctamente la problemática de la seguridad, ofrecer una comprensión integral de la COT y proponer recomendaciones para fortalecer las respuestas a nivel nacional e internacional.

Palabras clave: Crimen organizado transnacional, defensa nacional, gobernabilidad, Marina de Guerra del Perú, seguridad nacional, socialismo del siglo XXI, soberanía.

Abstract: *Transnational organized crime (TOC) poses a significant threat to global security and sustainable development. This complex phenomenon encompasses various illicit activities that transcend national borders, including drug trafficking, human trafficking, money laundering, arms trafficking, cybercrime, and the exploitation of natural resources, among others. TOC is characterized by hierarchical structures, the pursuit of economic gain, and the ability to corrupt state and private institutions.*

This article analyzes the multifaceted nature of TOC, examining its main manifestations, the factors that facilitate its expansion (such as globalization, technological advancements, and socioeconomic inequalities), and its impact on political stability, economy, and society. It explores the strategies and mechanisms of international cooperation implemented to combat this scourge, as well as the challenges and limitations that still persist in the fight against transnational criminal networks. The main objective is to correctly define the security problem, provide a comprehensive understanding of TOC, and propose recommendations to strengthen responses at national and international levels.

Keywords: *Transnational organized crime, defense sector, governance, Peruvian Navy, national security, socialism of the 21st Century, sovereignty.*

1. INTRODUCCIÓN

En el actual escenario geopolítico regional, el crimen organizado transnacional (COT) ha adquirido una dimensión estratégica que desborda los márgenes clásicos de la criminalidad común, convirtiéndose en un factor desestabilizador de la seguridad nacional y de la gobernabilidad de los Estados. El Perú, por su posición geográfica, condición de país bioceánico y su rol dentro de los corredores logísticos de América del Sur, se enfrenta crecientemente a dinámicas delictivas

de carácter transnacional que ponen a prueba no solo sus capacidades policiales, sino también los instrumentos de defensa del Estado.

Organizaciones criminales como el Tren de Aragua, diversos carteles vinculados al narcotráfico y estructuras dedicadas al tráfico de personas, armas, minería ilegal, contrabando y pesca ilegal, configuran un ecosistema delictivo que opera de manera articulada, flexible y con alta capacidad de corrupción institucional. Este fenómeno trasciende el ámbito interno y, en algunos casos, es propiciado indirectamente por regímenes hostiles, insertándose dentro de estrategias de guerra asimétrica y amenazas híbridas, orientadas a debilitar las estructuras soberanas mediante la descomposición del orden interno.

En este contexto, el Sector Defensa y, particularmente, la Marina de Guerra del Perú enfrentan el desafío de actualizar su doctrina, capacidades operativas y estructuras de inteligencia para contribuir de manera efectiva a la neutralización de estas amenazas, dentro de los marcos legales y constitucionales vigentes.

El presente artículo tiene como objetivo analizar la configuración del crimen organizado transnacional como amenaza estratégica para el Perú, evaluando sus manifestaciones operativas y su vinculación con dinámicas geopolíticas regionales, y proponiendo recomendaciones concretas orientadas tanto al Sector Defensa como al fortalecimiento de la función específica que le compete a la Marina de Guerra en el ámbito marítimo y costero.

2. ANÁLISIS

2.1. Conceptualización del crimen organizado transnacional (COT)

El crimen organizado transnacional (COT) representa una de las expresiones más complejas de la criminalidad global contemporánea. Se caracteriza por estructuras flexibles, adaptativas y altamente descentralizadas, capaces de operar simultáneamente en múltiples jurisdicciones. Estas redes criminales trascienden las fronteras nacionales aprovechando los vacíos legales, las debilidades institucionales, las asimetrías económicas y los conflictos sociales de los Estados vulnerables.

A diferencia de las organizaciones criminales tradicionales, el COT opera bajo esquemas de negocio diversificados, articulando actividades ilícitas (narcotráfico, trata de personas, tráfico de armas, contrabando, minería ilegal, pesca INDNR [pesca ilegal no declarada y no registrada], extorsión) con actividades legales como comercio, finanzas, construcción, transporte y servicios logísticos. El denominador común de todas estas actividades es el lavado de activos, proceso

indispensable para transformar las ganancias ilícitas en recursos financieros aparentemente legítimos.

En el Perú, factores estructurales como las extensas fronteras porosas, la economía informal robusta, la debilidad institucional y la corrupción endémica han facilitado el posicionamiento operativo de estas redes criminales, convirtiendo al país en plataforma logística, productiva y financiera para múltiples organizaciones criminales transnacionales.

2.2. El COT como herramienta de guerra asimétrica

El COT ha sido incorporado por algunos actores estatales y paraestatales dentro de esquemas de guerra asimétrica y amenazas híbridas, transformándolo en un instrumento indirecto de desestabilización estratégica de Estados adversarios sin recurrir a un conflicto militar abierto.

Este fenómeno es observable especialmente en el marco geopolítico impulsado por el socialismo del siglo XXI, donde algunos regímenes autoritarios han utilizado el crimen organizado para:

- Financiar operaciones políticas y de propaganda.
- Corromper estructuras estatales de países objetivo.
- Desestabilizar democracias mediante migración forzada, desorden social y captura económica.
- Garantizar su propia supervivencia mediante economías criminales paralelas.

En este contexto, las organizaciones criminales transnacionales no solo actúan como negocios ilícitos, sino como verdaderos brazos financieros, logísticos e incluso de inteligencia al servicio de estrategias geopolíticas más amplias.

2.3. Manifestaciones en el contexto peruano

2.3.1. El vínculo estructural con el socialismo del siglo XXI

El modelo del socialismo del siglo XXI ha mutado hacia un proyecto de captura estatal funcionalmente asociado al crimen organizado. Las redes criminales proveen de recursos económicos, control territorial y protección operativa, mientras los regímenes autoritarios les ofrecen impunidad jurídica, amparo diplomático y acceso a recursos estratégicos.

El lavado de activos es el núcleo central de esta simbiosis criminal-política. Las ganancias ilícitas son blanqueadas a través de:

- Empresas fachadas.
- Transacciones inmobiliarias.
- Operaciones comerciales internacionales.
- Uso de criptomonedas.
- Transferencias bancarias multinivel.

Esto permite infiltrar sectores estratégicos de la economía formal peruana, deformando los mercados y erosionando la estabilidad institucional.

2.3.2. Infiltración institucional

El COT ha penetrado distintas capas del Estado peruano mediante:

- Captación y corrupción de autoridades judiciales, policiales, fiscales, aduaneras y migratorias.
- Financiamiento ilegal de campañas políticas.
- Penetración en sectores económicos sensibles: transporte, puertos, minería, construcción y comercio exterior.
- Cooptación de operadores financieros, legales y empresariales para facilitar el lavado de activos.

2.3.3. Penetración económica

El COT controla sectores clave mediante:

- Minería ilegal: explotación descontrolada de oro, coltán y otros recursos estratégicos en zonas críticas como Madre de Dios, Puno y la Amazonía.
- Pesca INDNR: explotación ilegal de recursos marinos frente al litoral peruano.
- Narcotráfico: articulación de la producción de hoja de coca con carteles internacionales.
- Tráfico de personas: explotación laboral y sexual de migrantes vulnerables.
- Extorsión, contrabando y tráfico de armas: que alimentan la violencia urbana y la expansión territorial de las mafias.

2.3.4. Organizaciones criminales relevantes

- El Tren de Aragua: organización criminal venezolana con presencia consolidada en varias regiones del Perú, articulada al tráfico de personas, sicariato, extorsión, narcotráfico y contrabando.
- Carteles internacionales: Cartel de Sinaloa, CJNG (México), Comando Vermelho y PCC (Brasil), con redes operativas y financieras en el Perú.
- Redes de tráfico de migrantes: organizaciones mixtas que explotan la crisis migratoria para actividades lucrativas y de control territorial.

2.4. Implicancias para el Sector Defensa

2.4.1. Expansión conceptual de la defensa nacional

El COT no es solo un fenómeno policial o judicial. Su impacto directo sobre la soberanía, la gobernabilidad y la estabilidad estratégica exige que la Defensa Nacional amplíe su marco doctrinario, reconociendo al COT como amenaza híbrida.

2.4.2. Vulnerabilidades críticas

- Fronteras abiertas y porosas.
- Presencia de zonas grises de gobernabilidad (VRAEM, minería ilegal, rutas migratorias).
- Debilitada capacidad de inteligencia financiera, cibernética y estratégica integrada.
- Alta corrupción estructural.

2.4.3. Exigencias doctrinarias

- Doctrinas multidimensionales que integren defensa convencional, inteligencia estratégica y combate al crimen transnacional.
- Fortalecimiento de la cooperación civil-militar-policial.
- Interdicción integral: marítima, fluvial, terrestre, aérea, cibernética y financiera.
- Construcción de capacidades específicas de ciberdefensa e inteligencia financiera militar.

2.4.4. Cooperación internacional

- Consolidación de patrullajes combinados regionales.
- Intercambio de inteligencia estratégica con socios hemisféricos.
- Participación activa en esquemas multinacionales de defensa hemisférica.

2.5. El rol estratégico de la Marina de Guerra del Perú

2.5.1. Defensa marítima y fluvial

- Interdicción de narcotráfico marítimo y fluvial.
- Control y neutralización de pesca INDNR.
- Interdicción de tráfico ilícito de armas y personas.
- Vigilancia efectiva de ríos amazónicos y zonas ribereñas críticas.

2.5.2. Inteligencia naval especializada

- Fortalecimiento de capacidades SIGINT (inteligencia de señales), HUMINT (inteligencia humana), IMINT (inteligencia de imágenes)

y OSINT (inteligencia de fuentes abiertas), orientadas a amenazas marítimas.
- Creación de células de inteligencia financiera naval articuladas al sistema nacional de inteligencia.

2.5.3. Cooperación regional y multinacional
- Participación en ejercicios combinados multinacionales.
- Desarrollo de interoperabilidad naval con armadas aliadas.
- Fortalecimiento de alianzas hemisféricas navales.

2.5.4. Desarrollo doctrinario naval
- Incorporación formal del COT como amenaza estratégica permanente dentro de la doctrina de defensa marítima del Estado peruano.

2.6. Referente jurídico internacional
El combate al COT exige respetar e integrar los siguientes marcos normativos:
- Convención de Palermo (ONU): principal instrumento internacional contra el crimen organizado transnacional.
- UNODC (Oficina de las Naciones Unidas contra la Droga y el Delito).
- GAFILAT: estándares regionales de combate al lavado de activos y financiamiento ilícito.
- Compromisos hemisféricos de seguridad multilateral.

3. CONCLUSIONES
El crimen organizado transnacional (COT), en el contexto geopolítico actual, ha evolucionado más allá de su expresión puramente delictiva, consolidándose como un actor estratégico no convencional que amenaza la soberanía, la estabilidad política, la seguridad económica y la gobernabilidad de los Estados. El Perú, debido a sus características geográficas, económicas e institucionales, enfrenta esta amenaza de manera particularmente aguda.

A lo largo del análisis se ha identificado que:

□ El COT no actúa de manera aislada, sino que en muchos casos opera en estrecha vinculación con proyectos de captura estatal, como los impulsados bajo el paraguas ideológico del socialismo del siglo XXI, donde el crimen organizado funge como brazo operativo, financiero y de control territorial de regímenes autoritarios y redes transnacionales de poder.

- La penetración del crimen organizado en el Perú abarca desde la corrupción institucional hasta el control de sectores económicos estratégicos, generando distorsiones profundas en el aparato estatal, las finanzas públicas y la vida social.
- El lavado de activos constituye el eje financiero transversal que permite al COT blanquear recursos ilícitos, conquistar estructuras formales, financiar proyectos políticos, expandir operaciones ilícitas y desestabilizar la economía nacional.
- La vulnerabilidad de las fronteras, la debilidad institucional, la carencia de inteligencia financiera integrada, la fragmentación interagencial y el alto nivel de corrupción política y judicial son factores que han favorecido la consolidación y expansión territorial de estas redes criminales.
- El Sector Defensa, y particularmente la Marina de Guerra del Perú, enfrentan el desafío ineludible de adaptarse doctrinaria y operativamente para enfrentar este nuevo tipo de amenaza híbrida, que exige capacidades de interdicción ampliadas, inteligencia especializada, cooperación internacional efectiva y un marco normativo actualizado.
- La dimensión transnacional de estas redes exige que el Estado peruano fortalezca sus alianzas regionales y hemisféricas, participe activamente en plataformas de inteligencia conjunta y potencie la interoperabilidad doctrinaria con sus socios estratégicos.

Neutralizar esta amenaza requiere abandonar los enfoques exclusivamente policiales o jurídicos y asumir que el crimen organizado transnacional constituye hoy uno de los principales riesgos estratégicos a la seguridad nacional, la defensa soberana y el futuro político del Estado peruano.

4. RECOMENDACIONES

El carácter complejo, híbrido y multidimensional del crimen organizado transnacional (COT) exige respuestas articuladas, sostenidas y adaptadas a la realidad estratégica del Perú. Las siguientes recomendaciones están orientadas a fortalecer la capacidad del Estado, el Sector Defensa y particularmente la Marina de Guerra del Perú, para enfrentar eficazmente esta amenaza.

A nivel del Estado peruano

Reformulación de la doctrina de Defensa Nacional ampliada

- Incorporar de forma explícita al crimen organizado transnacional como amenaza estratégica dentro de la doctrina de defensa nacional.

- Establecer legalmente un marco de defensa frente a amenazas híbridas, que permita articular capacidades militares, policiales, de inteligencia, financieras y diplomáticas.

Reestructuración legal

- Actualizar y modernizar los marcos normativos que regulan la intervención de las Fuerzas Armadas en escenarios de crimen organizado transnacional, bajo estrictos controles constitucionales y de derechos humanos.
- Fortalecer las leyes contra el lavado de activos y el financiamiento ilícito, mejorando los sistemas de detección, seguimiento y persecución penal de flujos financieros criminales.

Consolidación de la inteligencia estratégica

- Recomendar a la Dirección de Inteligencia Nacional (DINI) la implementación de un área con especialidad en crimen organizado transnacional.
- Articular capacidades de inteligencia financiera, cibernética, marítima, migratoria, aduanera y geopolítica.
- Potenciar los protocolos de intercambio de información con agencias internacionales de inteligencia y seguridad.

Fortalecimiento de la cooperación internacional

- Intensificar la participación activa en mecanismos regionales como Ameripol, UNODC, GAFILAT, entre otros.
- Establecer acuerdos bilaterales de inteligencia operativa con países aliados estratégicos (EE. UU., Colombia, Brasil, Chile, entre otros).
- Participar en programas de formación conjunta y ejercicios multinacionales de lucha contra amenazas híbridas.

A nivel del Sector Defensa

Desarrollo doctrinario específico

- Elaborar manuales doctrinarios sobre la confrontación de amenazas híbridas, particularmente en el ámbito del crimen organizado transnacional.
- Establecer protocolos de empleo conjunto civil-militar en escenarios de neutralización de redes criminales.

Formación de personal especializado:

- Capacitar oficiales y cuadros operativos en:
  - Inteligencia estratégica aplicada al crimen organizado transnacional.
  - Inteligencia financiera y seguimiento de flujos ilícitos.
  - Ciberdefensa y análisis de amenazas híbridas.
  - Interdicción marítima, fluvial y aérea de actividades criminales transnacionales.

Creación de estructuras interagenciales permanentes

- Formalizar comandos operativos conjuntos (Fuerzas Armadas, Policía Nacional, entidades judiciales, SUNAT, Migraciones, Aduanas) para planificar operaciones integradas de interdicción y neutralización de redes criminales.

Desarrollo de capacidades cibernéticas

- Crear unidades de ciberinteligencia militar con capacidad de monitoreo, detección y neutralización de operaciones criminales digitales, financieras y de lavado de activos.

A nivel de la Marina de Guerra del Perú

Fortalecimiento de la capacidad de interdicción marítima y fluvial

- Incrementar el despliegue permanente de unidades fluviales en los ríos amazónicos vulnerables.
- Modernizar la flota costera para patrullaje oceánico, combate a la pesca INDNR y neutralización del narcotráfico marítimo.
- Establecer presencia disuasiva permanente en rutas de alto tránsito criminal.

Creación de un Comando de Inteligencia Naval especializado

- Consolidar un comando naval de lucha contra el crimen organizado transnacional, con capacidades SIGINT, HUMINT, IMINT y OSINT.
- Integrar plataformas ISR (Intelligence, Surveillance and Reconnaissance) con recursos satelitales y UAV (vehículo aéreo no tripulado).

Interoperabilidad internacional

- Establecer acuerdos formales de interoperabilidad doctrinaria y tecnológica con armadas aliadas del hemisferio.
- Participar activamente en ejercicios combinados regionales enfocados en la lucha contra el crimen organizado transnacional y la protección de espacios marítimos soberanos.

Ajuste doctrinario interno

- Incorporar formalmente dentro de la doctrina naval el concepto de defensa permanente contra amenazas no convencionales, incluyendo el crimen organizado transnacional, como misión central de la Marina de Guerra.

Estas recomendaciones buscan transformar el actual paradigma de seguridad nacional hacia un modelo de defensa multidimensional, adaptado a las nuevas dinámicas estratégicas del siglo XXI, donde el crimen organizado transnacional ya no constituye un problema exclusivamente interno, sino un desafío de alcance hemisférico y de implicancias directas en la estabilidad del Estado peruano.

Referencias

- Arenas Piedrahita, A. J., Erazo Patiño, L. A., & Cujabante Villamil, X. A. (2022). Delincuencia organizada transnacional en un escenario multidimensional. En Escuela Militar de Cadetes "General José María Córdova" (Ed.), *Colombia: Avances y desafíos frente a la delincuencia organizada transnacional*. Sello Editorial Esmic.
- Center for a Secure Free Society. (s. f.). *Think tank especializado en seguridad nacional y crimen transnacional*. https://sfsociety.org
- Decreto Legislativo N.º 1249, que modifica la Ley N.º 30077, Ley contra el Crimen Organizado. Diario Oficial *El Peruano*, 07 de octubre de 2016.
- Decreto Supremo N.º 001-2017-JUS, Reglamento de la Ley contra el Crimen Organizado. Diario Oficial *El Peruano*, 05 de enero de 2017.
- Decreto Supremo N.º 017-2019-IN, que aprueba la Política Nacional Multisectorial de Lucha contra el Crimen Organizado 2019–2030. Diario Oficial *El Peruano*, 21 de agosto de 2019.
- Escalante Barreto, E. (2024, 27 de junio). *Política criminal transnacional en la lucha contra el crimen organizado*. Editorial Tirant Lo Blanch.
- Ley N.º 30077, Ley contra el Crimen Organizado. Diario Oficial *El Peruano*, 20 de agosto de 2013. https://lpderecho.pe/ley-crimen-organizado-ley-30077-actualizado/
- Ley N.º 32108, que modifica el Código Penal, la Ley 30077 y la Ley 27379. Diario Oficial *El Peruano*, 09 de agosto de 2024.
- Magaz Álvarez, R. (2011). *Crimen organizado transnacional y seguridad*. Instituto Universitario General Gutiérrez Mellado; Marcial Pons Librero.
- Naciones Unidas. (2000). *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos*. Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC).
- Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2011). *Delincuencia organizada transnacional: La economía ilegal mundializada*. Naciones Unidas.
- Peña Cabrera Freyre, A. R. (2018). *Derecho penal: Parte especial* (Tomo II, 5.ª ed.). Gaceta Jurídica.
- Prado Saldarriaga, V. (2017). *Criminalidad organizada: Concepto, evolución y desafíos*. Grijley.
- Prado Saldarriaga, V. (2019). El delito de crimen organizado y su tratamiento en la legislación peruana. En J. R. Hurtado Pozo (Ed.), *Estudios de derecho penal y procesal penal: Homenaje al profesor José Hurtado Pozo* (pp. 345–360). Instituto Pacífico.
- Rebolledo, A. *Así se lava el dinero en Venezuela*.
- Rebolledo, *A. Delincuencia organizada transnacional: El gran negocio*.
- Risquez, R. *El Tren de Aragua*.
- Rivera-Páez, S. I., Rey Pinto, E. M., & González Saiz, A. (2021). Crimen organizado transnacional y dimensiones culturales en América Latina. Escuela Superior de Guerra "General Rafael Reyes Prieto" (Sello Editorial ESDEG).
- Sain, M. F. (2017). *Qué es el crimen organizado*. Universidad Metropolitana para la Educación y el Trabajo.
- Salinas Siccha, R. (2020). La criminalidad organizada transnacional en el Perú: Desafíos para el sistema de justicia penal. *Actualidad Jurídica*, 16(212), 15–28.
- Sin Filtros. (s. f.). Plataforma digital dirigida por Maibort Petit dedicada a la difusión de temas vinculados con la geopolítica, seguridad hemisférica, política y crimen organizado transnacional.
- Vizcarra, S., Bonilla, D., & Prado, B. (2020). Respuestas del Estado peruano frente al crimen organizado en el siglo XXI. *CS*, (31), 109–138.

Año 2025, Vol. 22, Nº 3, pp. 44 - 56.
DOI: https://doi.org/10.35628/resup.v16i2.172

Evolución de las operaciones antisuperficie

Evolution of anti-surface operations

Recibido: 26 de junio de 2025 | Aceptado: 05 de diciembre del 2025

Jhonatan Velásquez Céspedes
https://orcid.org/0009-0000-7835-4667

Oficial calificado en guerra de superficie, completó el curso básico de Estado Mayor y el curso de Comando y Estado Mayor en la Escuela Superior de Guerra Naval. Ha trabajado en diversas unidades navales, incluyendo el BAP Los Héros, BAP Montero y BAP Ferré. Asimismo, se desempeñó como comandante del BAP Curaray con el grado de teniente segundo. Actualmente, ocupa el cargo de jefe de operaciones del BAP Quiñones.

Email:jhonatan.velasquez.cespedes@gmail.com

Resumen: El presente artículo tiene como objetivo analizar la evolución de las operaciones antisuperficie desde la guerra de las Malvinas en 1982 hasta la actualidad, en 2024. A lo largo de este período, se explorarán los cambios y las innovaciones tecnológicas. En relación con la parte metodológica, el artículo tiene un enfoque cualitativo, de carácter descriptivo, aplicándose el método inductivo-analítico debido a que se estudió la evolución de las operaciones antisuperficie a través de los años. Como resultado de la investigación, se presenta la evolución de las operaciones antisuperficie.

Palabras clave: táctica, táctica naval, guerra de las Malvinas, operaciones antisuperficie.

Abstract: *This article aims to analyze the evolution of anti-surface operations from the Falklands War in 1982 to the present day, in 2024. Throughout this period, technological changes and innovations will be explored. Regarding the methodological aspect, the article adopts a qualitative, descriptive approach, using the analytical inductive method to study the evolution of anti-surface*

operations over the years. As a result of the investigation, the evolution of anti-surface operations is presented.

Keywords: *tactics, naval tactics, Falklands War, anti-surface operations.*

1. INTRODUCCIÓN

A lo largo de la historia, el ser humano ha otorgado gran importancia al estudio del pasado, particularmente en el ámbito bélico y su evolución hacia la guerra moderna. Este análisis permite identificar las acciones de los conflictos, evaluar cómo influye la tecnología en diferentes épocas y establecer conexiones entre las causas, los resultados y las consecuencias de los enfrentamientos. Como afirmó Napoleón Bonaparte: "el que no conoce su historia está condenado a repetirla", lo que subraya la relevancia de comprender el pasado para orientar el futuro.

La guerra de las Malvinas en 1982 representó un hito clave en la historia militar, marcando un punto de inflexión en las tácticas navales. Este conflicto introdujo innovaciones significativas en el uso de tecnologías y estrategias, las cuales han tenido un impacto duradero en los conflictos posteriores. Este conflicto no solo evidenció la importancia de la interoperabilidad y la adaptabilidad de las fuerzas navales, sino que también puso de manifiesto el impacto de la guerra electrónica, las operaciones anfibias y el empleo de plataformas de superficie, aéreas y submarinas.

Desde entonces, la evolución de la táctica naval ha estado marcada por la incorporación de nuevas tecnologías, como la guerra cibernética y la automatización de sistemas, que han transformado la manera en que se llevan a cabo las operaciones navales. A medida que las amenazas han cambiado, las marinas del mundo han tenido que adaptarse a un entorno cada vez más complejo y dinámico, reconfigurando sus doctrinas y capacidades para enfrentar los desafíos del siglo XXI. Este análisis de la evolución de las operaciones antisuperficie desde la guerra de las Malvinas hasta la actualidad no solo revela los avances tecnológicos y las lecciones aprendidas que continúan moldeando el futuro de la guerra naval, sino que también destaca la importancia de considerar este conflicto como punto de partida para evaluar las tácticas empleadas.

En este artículo se tratará la evolución de las operaciones antisuperficie desde la guerra de las Malvinas hasta la actualidad.

2. ANTECEDENTES

Sharrett (1987) realizó una investigación titulada "The Evolution of Naval Warfare Technology and the Impact of Space Systems", donde se explica la historia de la guerra naval y la tecnología desde la antigüedad hasta la Segunda Guerra Mundial. Al analizar diferentes innovaciones tecnológicas, incluido su desarrollo, asimilación y empleo por parte de las marinas en batalla, se identificaron cinco tendencias básicas de la guerra naval, las cuales han sido influenciadas por los cambios tecnológicos. Estas tendencias son: el aumento del tamaño del área que una fuerza naval puede controlar, la resiliencia de los medios, la reducción de los tiempos de reacción, la reducción de la exposición y el riesgo de una fuerza, y el aumento de la probabilidad de destrucción del arma. Asimismo, el autor analizó algunas tendencias de la época, como es el caso de la contribución de los sistemas espaciales a las operaciones de guerra naval.

Lautenschl (1984) escribió el libro "Technology and the Evolution of Naval Warfare: 1851-2001", donde se explica que los avances tecnológicos pueden generar innovaciones tácticas; esto produciría cambios fundamentales en las capacidades de combate. Asimismo, menciona la preocupación de cómo anticipar ese cambio, especialmente si se produce de forma inesperada. Igualmente, describe que la revisión histórica proporciona estudios de casos sobre cómo la tecnología puede afectar la guerra naval y el análisis evidenciaría las tendencias básicas que podrían ser útiles para desarrollos futuros.

3. ANÁLISIS DE LAS OPERACIONES ANTISUPERFICIE DESDE 1982 HASTA 2024

En los años 80, las operaciones antisuperficie fueron destinadas a neutralizar o afectar unidades navales de superficie; se valían principalmente del empleo de plataformas de superficie, submarinas y aeronavales. Básicamente, el accionar antisuperficie se caracterizaba por el uso intensivo de los misiles antisuperficie disparados por buques y aeronaves, así como bombas lanzadas desde aeronaves. En forma secundaria o contra blancos de superficie menores se empleaba artillería.

Por otra parte, los submarinos empleaban torpedos para atacar a las unidades de superficie. En esta década todavía se encontraban en desarrollo los primeros misiles antibuque disparados desde submarinos como el Harpoon UGM-84 (U.S. Naval Institute, 2001). En términos generales, el procedimiento táctico general para atacar a una unidad de superficie por medio de buques o aeronaves era:

1) Detectar e identificar al blanco de superficie que podía ser por diversos medios, generalmente a través de exploradores aéreos.
2) Conformar un Grupo de Acción de Superficie (GASUP) en caso de realizar el ataque con unidades de superficie o vectorear aeronaves para efectuar el ataque (Freedman, 2005).
3) Realizar el ataque y evaluar los resultados del mismo. Generalmente, los ataques se realizaban al alcance de los propios sensores, haciendo su aparición en esta época los primeros misiles transhorizonte como el Otomat MK-II y el Harpoon, que podían ser disparados con información desde otra unidad que no era la lanzadora (U.S. Naval Institute, 2001).

En el caso de los submarinos, el ataque se podía efectuar de dos maneras:

1) A partir de la detección del buque por parte del submarino cuando entraba en su área de patrullaje (Rebolar, 2013).
2) Por medio del vectoreo del submarino hacia la posición conocida del blanco por medio de otras plataformas (Freedman, 2005).

Una situación especial, no concebida por las otras armadas y fabricantes de armas, fue el ataque realizado por los argentinos contra el HMS Glamorgan por medio de una instalación improvisada de misiles Exocet MM-38 basada en tierra. Esto fue algo innovador, puesto que la empresa Aerospatiale de Francia, fabricante del arma, no tenía concebido esto (Mayorga & Errecaborde, 1998). A raíz de este ingenio innovador y efectivo, diversos fabricantes de misiles comenzaron a fabricar sistemas de lanzamiento de misiles antisuperficie basados en tierra (Middlebrook, 2003).

Respecto a la defensa de los buques contra el accionar antisuperficie proveniente de las diversas plataformas, en los años 80 se contaban con las siguientes medidas:

1) Empleo de medios de guerra electrónica y disturbadores para desviar a los misiles.
2) Empleo del chaff; además las tácticas de chaff incluían la dispersión de reflectores radar para confundir los sistemas de guía enemigos mediante modalidades específicas:
    a) Despliegue seductor (Seduction): se utiliza en la fase final de seguimiento del misil enemigo, con el objetivo de desengancharlo del objetivo original. Para ello, se lanzan paquetes de chaff de alta

densidad que crean señales "más atractivas" que engañan al radar del misil, desviándolo del blanco verdadero.

b) Despliegue protectivo (Distraction): Utilizado para enmascarar al buque creando una nube que lo ocultaba del radar enemigo, dificultando la fijación de los misiles. Este método era clave durante momentos críticos, como maniobras evasivas o ataques coordinados.

c) Despliegue de saturación (Saturation): al abrumar la capacidad del radar enemigo para detectar y seguir objetivos reales, generando una gran cantidad de ecos falsos en la pantalla del radar. Consiste en tiras metálicas o metalizadas dispersas en el espacio que actúan como reflectores, creando una nube de objetivos falsos que dificultan la identificación de los blancos auténticos. Su efectividad depende de factores como la densidad de las tiras, su tamaño, que debe resonar con la frecuencia del radar, y las condiciones del viento, que pueden dispersar la nube y reducir su eficacia

En la guerra de Malvinas se pueden apreciar diversas acciones que se enmarcan en este tipo de accionar táctico:

1) El hundimiento del HMS Sheffield por medio de misiles Exocet AM-39 disparados por los aviones Super-Etendard de la Armada Argentina.
2) El ataque a los buques británicos en el estrecho de San Carlos por medio de unidades aéreas de la Fuerza Aérea y la Aviación Naval Argentina por medio de bombas.
3) El hundimiento del ARA General Belgrano por medio de torpedos del submarino HMS Conqueror, el cual fue vectoreado para la realización del ataque (Freedman, 2005).

4. EVOLUCIÓN DE LAS OPERACIONES ANTISUPERFICIE DESDE LA GUERRA DE LAS MALVINAS (1982) HASTA EL AÑO 2024

Periodo de 1982 a 2000

El empleo de misiles Exocet desde plataformas terrestres durante la guerra de las Malvinas en 1982 marcó un punto de inflexión tanto tecnológico como táctico en la guerra antisuperficie. Los ataques con estos misiles, lanzados desde tierra por fuerzas argentinas, lograron hundir o dañar varios buques de la Royal Navy británica, lo que provocó importantes cambios en las doctrinas navales para enfrentar misiles antibuque y mejoró significativamente las capacidades de defensa naval (Mayorga & Errecaborde, 1998). También, desde el punto de vista

tecnológico, uno de los cambios más destacados fue la integración de misiles en plataformas terrestres. El Exocet, originalmente diseñado para ser lanzado desde aeronaves y buques, fue adaptado para ser disparado desde vehículos terrestres improvisados. Este uso novedoso demostró que los misiles antibuque no estaban limitados a plataformas navales o aéreas, lo que expandió el concepto de guerra antisuperficie y subrayó la vulnerabilidad de los buques frente a ataques desde tierra.

Además, el éxito del Exocet incentivó el desarrollo de tecnologías de contramedidas electrónicas (ECM), con los buques de guerra empezando a equiparse con sistemas más avanzados para interferir con los radares de misiles entrantes y desviar su trayectoria mediante señuelos (Coli, 2007).

Por otro lado, la experiencia también impulsó mejoras en los sistemas de defensa antimisiles. A raíz de los ataques en Malvinas, las armadas del mundo comenzaron a equipar sus buques con sistemas avanzados de defensa antimisiles como los sistemas CIWS (Close-In Weapon Systems) y lanzadores verticales de misiles, diseñados para interceptar misiles como el Exocet antes de que alcanzaran sus objetivos (Ventura, 2000). Esto fortaleció la capacidad defensiva de los buques ante la creciente amenaza de misiles antibuque.

En el ámbito táctico, uno de los cambios clave fue la adopción de tácticas de dispersión. Tras la experiencia en Malvinas, las flotas navales comenzaron a dispersarse más en lugar de concentrarse en áreas estrechas o en grupos grandes, con el fin de reducir su vulnerabilidad a los ataques coordinados de misiles. Además, los buques mantuvieron maniobras de movimiento constante, como en décadas anteriores, lo que dificultaba que los radares enemigos pudieran localizarlos con precisión (Lombardo, 1989).

Otro ajuste en las tácticas antisuperficie fue el fortalecimiento de la defensa de área, especialmente ante ataques aéreos y de misiles costeros. La coordinación estrecha con aeronaves de patrulla marítima y cazas permitió establecer una defensa en capas más robusta, optimizando la detección temprana de misiles o torpedos y facilitando su neutralización antes de que alcancen a los buques. Además, la incorporación de sistemas avanzados de alerta temprana y radares de mayor alcance en los buques mejoró notablemente su capacidad de reacción, permitiendo el despliegue rápido de contramedidas o maniobras evasivas (Coli, 2007).

Otro aspecto crucial que surgió a raíz de la experiencia de Malvinas fue la necesidad de mejorar la resistencia estructural de los buques. El incendio del HMS Sheffield, provocado por el impacto de un misil Exocet, demostró la

vulnerabilidad de los materiales tradicionales en los buques de guerra. Además, los buques de guerra se construían principalmente con materiales tradicionales como el acero y el aluminio. El acero se utilizaba para la estructura y el casco debido a su resistencia, mientras que el aluminio era común en superestructuras por su ligereza. Sin embargo, el aluminio era inflamable a altas temperaturas y, en combinación con revestimientos de materiales plásticos y otros compuestos inflamables utilizados en interiores, resultaba en una vulnerabilidad crítica frente a incendios. El HMS Sheffield mostró que estos materiales, aunque comunes en ese momento, ofrecían poca resistencia ante el calor extremo generado por el impacto de misiles como el Exocet, provocando la rápida propagación de incendios y el fallo de sistemas.

En respuesta, las nuevas generaciones de buques respondieron a los riesgos de incendio mejorando sus materiales y sistemas de seguridad. Se incorporaron materiales resistentes al fuego y sistemas automáticos de extinción en áreas críticas, como la sala de máquinas y los compartimentos de mando. Además, se perfeccionó el compartimentaje de los buques para contener el daño en una sección y evitar su propagación a otras áreas, incrementando así las posibilidades de supervivencia en caso de ataque.

Por otra parte, el papel de los helicópteros y aviones de despegue vertical, como el Harrier, ganó mayor relevancia tras la guerra de Malvinas. Para optimizar las operaciones aéreas, se rediseñaron las cubiertas de vuelo y los hangares de los buques de guerra, reconociendo que los helicópteros eran fundamentales en misiones de guerra antisuperficie, reconocimiento, búsqueda y rescate, así como en guerra antisubmarina.

En operaciones antisuperficie, el binomio buque-helicóptero permitió extender el alcance de vigilancia y detección al operar a mayores distancias, lo que facilitó el monitoreo de áreas alrededor de la fuerza naval y la detección anticipada de amenazas, dándole a los buques la ventaja de responder antes de que el enemigo pudiera acercarse. Equipados con misiles antibuque y torpedos ligeros, los helicópteros comenzaron a ejecutar misiones de intercepción y ataque a distancia, neutralizando embarcaciones hostiles sin exponer al buque a la línea de fuego, lo cual resultaba particularmente útil contra lanchas rápidas y buques de superficie (Vego, 2020).

Durante los años 90, las operaciones antisuperficie se enfocaban en la detección temprana y el combate a distancia mediante el uso de misiles antibuque, también en el empleo de aeronaves con capacidad de ataque antisuperficie y

antisubmarino. En este contexto, los sistemas avanzados de radar y control de tiro eran esenciales para identificar y atacar objetivos con precisión. Por otro lado, la maniobrabilidad y velocidad de los buques eran cruciales para evadir ataques enemigos y posicionarse para contraatacar. De esta forma, los buques podían adaptarse rápidamente a las cambiantes condiciones del combate y maximizar su efectividad ofensiva y defensiva (Rodríguez, 2015).

Además, una de las principales tácticas ajustadas fue la dispersión de las flotas. En lugar de operar en formaciones compactas, las fuerzas navales se dispersaban en un rango de 20 a 40 millas náuticas (mn) en formaciones de protección estándar, y llegando hasta 50 mn en situaciones de alta amenaza. Esta táctica minimizaba el riesgo de que varias unidades fueran atacadas simultáneamente, al tiempo que optimizaba la cobertura de vigilancia y defensa mutua. Los sensores avanzados permitían rastrear objetivos a más de 200 mn, facilitando la detección temprana de amenazas y la efectividad en formaciones dispersas. Misiles de largo alcance como el RGM-84 Harpoon y el AGM-84E SLAM, con alcances de 80-150 mn, permitían a los buques mantener una considerable separación sin perder su capacidad ofensiva.

Periodo de 2000 a 2010

Entre el 2000 y el 2010, las operaciones antisuperficie mantuvieron la creciente amenaza de los misiles antibuque, que se habían vuelto más precisos, con mayor alcance y capacidad destructiva. Para contrarrestar estos avances, las armadas adoptaron sistemas de defensa más avanzados y ajustaron sus maniobras y operaciones de combate. Uno de los principales ajustes fue la defensa en capas, la cual avanzó considerablemente con la integración de sistemas antimisiles de diferentes alcances. En la capa de largo alcance, misiles como el Standard Missile SM-2 y SM-3, con un alcance efectivo de hasta 100 millas náuticas, interceptaban misiles enemigos en fases tempranas de vuelo, antes de que se aproximaran al objetivo. En la capa media, misiles de corto y medio alcance, como el Evolved Sea Sparrow Missile (ESSM), cubrían rangos de aproximadamente 10 a 20 millas náuticas, proporcionando una segunda línea de defensa ante misiles que lograban acercarse más. Por último, la defensa de punto se aseguraba con sistemas de corto alcance, como el CIWS Phalanx, que protegía a menos de una milla náutica mediante ráfagas de alta cadencia, interceptando amenazas en el último momento y ofreciendo una respuesta final ante ataques inminentes (Norman & Polmar, 2005).

Una operación destacada en este contexto son las operaciones antisuperficie de la OTAN en el Cuerno de África, que se centraron en la protección de rutas marítimas clave y la lucha contra la piratería en el Golfo de Adén y el océano Índico. Para ello, se emplearon sistemas de armas de corto alcance, como cañones de 20 a 30 mm y misiles de defensa cercana (SeaRAM y CIWS), con el objetivo de neutralizar amenazas inmediatas, como ataques de misiles o embarcaciones hostiles a corta distancia. Además, se utilizaron radares de última generación con capacidades de detección de múltiples capas para rastrear amenazas tanto aéreas como de superficie, lo que, junto a los sistemas de armas de precisión, permitió destruir rápidamente las amenazas sin la necesidad de un combate prolongado (Consejo de Seguridad de las Naciones Unidas, 2021).

Además, las formaciones y maniobras de las flotas se mantuvieron en disposiciones dispersas, con buques separados entre 20 y 50 millas náuticas, dependiendo de la amenaza y de las capacidades de vigilancia y defensa de cada unidad. Este grado de separación reducía la probabilidad de que múltiples buques fueran atacados al mismo tiempo por misiles enemigos, al dificultar la adquisición y el ataque simultáneo de blancos. Además, esta dispersión optimizaba la cobertura de sensores y sistemas de defensa mutua.

También, la proliferación de UAV ajustó las tácticas antisuperficie al proporcionar capacidades de vigilancia y reconocimiento en tiempo real sin exponer a tripulaciones. Los drones de vigilancia extendieron el alcance de detección de las flotas a más de 100 millas náuticas, permitiendo localizar objetivos de superficie y submarinos desde una distancia segura. Además, su integración en la defensa en capas ayudó a guiar misiles antibuque, aumentando la precisión de los ataques en áreas costeras. Las fuerzas navales adaptaron formaciones dispersas o divididas para dificultar la vigilancia continua de los drones, mientras que las operaciones de guerra electrónica se implementaron para bloquear o interferir sus comunicaciones, afectando el control y transmisión de datos (Ventura, 2000).

Periodo de 2010 a 2024

Entre 2010 y 2024, las operaciones antisuperficie se mantuvieron para contrarrestar la evolución de los misiles antibuques, implementando una defensa activa multicapa que integraba diversos sistemas de interceptores operativos en distintas fases del vuelo del misil. Los misiles de largo alcance, como el SM-6, con un alcance efectivo de hasta 240 millas náuticas, permitieron interceptar amenazas en fases iniciales y medias de vuelo, atacando los misiles enemigos

antes de que alcanzaran su fase terminal, lo que minimizaba el riesgo para las defensas internas.

Complementando esta defensa, el SeaRAM, que actúa como un sistema de defensa de punto con un alcance de aproximadamente 20 millas náuticas, se ajustó para responder a las maniobras terminales erráticas de los misiles antisuperficie modernos, que complicaban la efectividad de los CIWS convencionales. Esta combinación de misiles de largo alcance y sistemas de corto alcance garantizó una respuesta coordinada, mejorando la protección de los buques y aumentando la probabilidad de neutralizar amenazas avanzadas antes de que llegaran a sus objetivos (Nordenstahl, 2017).

Además, la incorporación de sistemas de defensa basados en inteligencia artificial (IA) se volvió fundamental en la lucha contra misiles antibuques. La IA permitió la fusión de datos de múltiples fuentes, mejorando la conciencia situacional y la capacidad de respuesta de las fuerzas navales. Estos sistemas de IA podían analizar información en tiempo real, identificar amenazas y coordinar automáticamente las respuestas defensivas, optimizando así la efectividad de los sistemas de armamento y contramedidas. Sumado a ello, se continuaron empleando maniobras evasivas y la dispersión de fuerzas para reducir la vulnerabilidad ante ataques con misiles desde tierra y submarinos.

Una operación dentro de este contexto fue la Operación Inherent Resolve (OIR), lanzada por Estados Unidos en 2014, cuyo objetivo era derrotar al grupo terrorista Estado Islámico (ISIS) en Irak y Siria. Durante esta campaña, la coalición aliada, que combinaba fuerzas terrestres, aéreas, navales y de inteligencia, llevó a cabo una serie de maniobras estratégicas tanto en el frente terrestre como en el marítimo. Los portaviones, como el USS Harry S. Truman y el USS Dwight D. Eisenhower, operaban como plataformas aéreas para misiones de bombardeo y patrullaje. En el ámbito naval, las fuerzas de la coalición emplearon tácticas de dispersión para reducir la vulnerabilidad a ataques con misiles desde la costa o submarinos enemigos, manteniendo separaciones adecuadas para dificultar su localización por misiles de crucero o sistemas de misiles lanzados desde tierra (Department of State et al., 2024)

También, la cooperación entre plataformas tripuladas y no tripuladas se mantuvo como una táctica clave para mejorar la efectividad de las operaciones antisuperficie. El uso de drones, tanto navales como aéreos, permitió una ampliación en la detección y monitoreo de amenazas. Estas plataformas no tripuladas desempeñaron roles cruciales en el reconocimiento y la creación de

señuelos, complicando la labor de los misiles antibuques al ofrecer alternativas y distracciones en el área de operaciones (Alger, 2022).

De igual importancia, el uso de armas de energía dirigida, como los láseres de alta potencia, se consolidó como una defensa contra misiles submarino-superficie. Estos sistemas de láser de alta potencia tenían un alcance efectivo de hasta 10 millas náuticas, permitiendo interceptar y neutralizar misiles en la fase de aproximación final sin consumir municiones tradicionales. Además, los láseres ofrecían la ventaja de realizar múltiples disparos sin la necesidad de recarga, proporcionando una defensa continua contra amenazas múltiples. Al integrarse en la defensa en capas, estos sistemas aumentaron la probabilidad de interceptar misiles antes de que alcanzaran objetivos críticos, complementando otras medidas defensivas como los misiles y los CIWS (Mejia, 2012).

En adición a lo descrito anteriormente, es importante mencionar que los misiles hipersónicos antisuperficie son una clase avanzada de armamento que se caracteriza por su capacidad para volar a velocidades superiores a Mach 5, es decir, cinco veces la velocidad del sonido. Esta velocidad extrema les permite alcanzar objetivos en tiempos notablemente reducidos, lo que dificulta su detección e interceptación por parte de sistemas de defensa convencionales. Estos misiles están diseñados para atacar buques de guerra y otras plataformas navales. Una de las características distintivas de los misiles hipersónicos es su maniobrabilidad. A diferencia de los misiles balísticos y transónicos, que siguen una trayectoria predecible, los misiles hipersónicos pueden cambiar de dirección durante el vuelo, lo que complica aún más los esfuerzos de defensa. Esta maniobrabilidad, combinada con su alta velocidad, les permite evadir los sistemas de defensa, aumentando la probabilidad de éxito en el ataque.

Asimismo, el desarrollo de misiles hipersónicos antisuperficie ha sido una prioridad para varias potencias navales, incluyendo a Rusia, China y Estados Unidos. Rusia ha estado a la vanguardia en este ámbito con su misil Tsirkon, que es lanzado desde plataformas navales y puede alcanzar velocidades de hasta Mach 9. Este misil está diseñado para realizar ataques precisos a objetivos navales a grandes distancias. China también ha avanzado significativamente en el desarrollo de misiles hipersónicos, como el YJ-21, que está diseñado para neutralizar amenazas navales. Su capacidad de maniobra y velocidad le permiten eludir las defensas enemigas, lo que lo convierte en un componente crítico de la estrategia militar china en el mar del Sur de China. Estados Unidos, aunque aún no ha desplegado misiles hipersónicos en sus fuerzas navales, está desarrollando el

sistema Conventional Prompt Strike (CPS), que permitirá a buques y submarinos realizar ataques a larga distancia con capacidades hipersónicas.

5. CONCLUSIONES

a. En el análisis de las operaciones antisuperficie desde 1982 hasta 2024, destacan los avances tecnológicos, tácticos y de diseño naval. Asimismo, en la guerra de las Malvinas, los misiles Exocet revolucionaron la guerra antisuperficie, impulsando mejoras en defensa antimisiles y diseño de buques.

b. En los años 90, se desarrollaron tácticas de dispersión y sistemas de defensa en capas, las cuales se mantuvieron en las décadas posteriores.

c. Entre 2000 y 2010, se implementaron sistemas avanzados de radar, integrando misiles de largo alcance y UAV para reconocimiento y vigilancia.

d. Entre 2010 y 2024, la defensa basada en inteligencia artificial y armas de energía dirigida se consolidó como una respuesta efectiva frente a las amenazas modernas. Al mismo tiempo, el desarrollo de misiles hipersónicos antisuperficie se convirtió en una prioridad para diversas potencias navales, influyendo significativamente en la evolución de los sistemas de defensa en capas.

Referencias

Alger, P. (2022). *The Gun in Naval Warfare*. Consultado el 2 de Julio de 2024, de U.S. Naval Institute: https://n9.cl/98ae7.

Coli, A. (2007). LA FLOTA DE MAR EN LA GUERRA DEL ATLÁNTICO SUR. SU ACTUACION POSTERIOR AL 2 DE ABRIL DE 1982. *Boletín del Centro Naval*.

Department of Defense, & The Department of State, & U.S. Agency for Internacional Devolpment. (2024). *OPERATION INHERENT RESOLVE, and Other U.S Government Activities related to Iraq & Syria*.

Freedman, L. (2005). *The Official History of the Falklands Campaign* (Vol. 1 & 2). Routledge.

Lautenschl, K. (1984). *Technology and the Evolution of Naval Warfare* 1851-2001. National Academy Press.

Lombardo, j. (1989). *Malvinas: errores, anécdotas y reflexiones*.

Mayorga, H., & Errecaborde, J. (1998). *No Vencidos- Relato de las operaciones navales en el conflicto del Atlántico Sur*. Planeta.

Mejia, M. (2012). *Transformación organizacional que debe desarrollar para cumplir plenamente sus roles operacionales y estratégicos en el tema externo*.

Middlebrook, M. (2003). *The Fight for the "Malvinas": The Argentine Forces in the Falklands War*. London: Viking.

Consejo de Seguridad de las Naciones Unidas. (2021). *La situación con respecto a la piratería y el robo a mano armada en el mar frente a las costas de Somalia*.

Nordenstahl, G. (2017). *Buques sin tripulación: el futuro está aquí, ya ha llegado*. Consultado el 11 de agosto de 2024, de Fundación Nuestromar: https://acortar.link/rmxvNF.

Norman, P., & Polmar, N. (2005). *The Naval Institute Guide to the Ships and Aircraft of the U.S. Fleet*. Naval Institute Press.

Rebolar, E. (2013). Guerra submarina en el Atlántico Sur. *Revista de Marina*. Consultado el 2 de julio de 2024.

Rodríguez, J. (2015). *Sistemas de propulsión y clasificación de buques*. Consultado el 08 abril de 2024, de Universidad de la Laguna: https://acortar.link/WWuKQZ.

Sharrett, P. (1987). *The Evolution of Naval Warfare Technology and the Impact of Space Systems*. Naval Postgraduate School Monterrey CA.

Vego, M. (2020). *General naval tactics- theory and practice*. Naval Institute Press Annapolis, Maryland.

Ventura, J. (2000). *Evolución y Tendencias de los Medios Navales* (XIII). Centro Naval.

Año 2025, Vol. 22, Nº 3, pp. 57 - 71.
DOI: https://doi.org/10.35628/resup.v16i2.173

Inteligencia artificial y su consideración en el desarrollo militar como avance tecnológico

Artificial Intelligence and Its Consideration in Military Development as a Technological Advance

Recibido: 21 de septiembre de 2025 | Aceptado: 03 de diciembre del 2025

José Huertas Centurión
https://orcid.org/0009-0003-8808-2791

Infante de Marina, graduado en la Escuela Naval del Perú como Bachiller en Ciencias Navales en el año 1999. Como Oficial Subalterno, tuvo participación constante como combatiente especial en la lucha contra el terrorismo y el narcotráfico en la zona del VRAEM y UCAYALI (sierra y selva peruana, respectivamente). En el ámbito externo, durante el año 2007 se desempeñó como Soldado de la Paz en la República de Haití, y como Oficial de Intercambio de los Estados Unidos - II MEF, en Unidades Operativas de los U.S. Marines Corps de la Base de Camp Lejeune - Jacksonville NC. Ejerció comando en las Unidades de la Fuerza de Infantería de Marina, como Segundo Comandante en el Agrupamiento de Apoyo de Combate y Comandante del Batallón de Infantería de Marina de la Amazonía N.º 2. Se desempeñó como Edecán del señor Presidente Constitucional de la República del Perú. Continuó su desarrollo profesional integrando la Clase 58 del Colegio Interamericano de Defensa - Washington DC, alcanzando el grado de Magíster en Defensa y Seguridad Hemisférica. Durante los años recientes, se desempeñó como Jefe de la Sección de Planeamiento y Operaciones de la Fuerza de Infantería de Marina, así como de la Sección de Planes y Estrategias del Comando Especial VRAEM. Actualmente se desempeña como Jefe del Departamento de Inspecciones de la Inspectoría General de la Marina.
Email:jhimap1@yahoo.es

Resumen: La inteligencia artificial (IA) es una tecnología emergente que ha despertado recientemente un gran interés en la sociedad moderna, no solo en el ámbito tecnológico, sino también en diversas empresas e instituciones alrededor del mundo. Actualmente, la inteligencia artificial se ha visto desarrollada para optimizar procesos y buscar mayor eficacia en diversos ámbitos. Este artículo propone discutir el avance de la inteligencia artificial y el potencial de sus aplicaciones, con especial referencia a su empleo en el ámbito militar.

Palabras clave: inteligencia artificial, seguridad nacional, estrategias de defensa, IA, innovación.

Abstract: *Artificial intelligence is an emerging technology that has recently sparked great interest in modern society, not only in the technological field but also in various companies and institutions around the world. Currently, artificial intelligence has been developed to optimize processes and seek greater efficiency in many areas. This paper aims to discuss the advancement of artificial intelligence and the potential of its applications, with special reference to its use in the military field.*

Keywords: *artificial intelligence, national security, defense strategies, AI, innovation.*

1. INTRODUCCIÓN

La tecnología y sus avances son esenciales en nuestra vida diaria, cambiando la forma en que trabajamos, nos comunicamos y vivimos. En el escenario global, la innovación tecnológica es crucial para el crecimiento económico y la competitividad entre países. Las principales potencias del mundo están invirtiendo mucho en investigación y desarrollo en IA para mantenerse a la vanguardia. Estas inversiones no solo fomentan el progreso científico y económico, sino que también aportan nuevas herramientas y capacidades en áreas claves, como la defensa y la seguridad, en donde el ámbito naval se encuentra inmerso. Por eso, liderar en tecnología se ha vuelto vital para el poder y la influencia mundial, con los países compitiendo ferozmente por dominar las tecnologías emergentes y asegurar su lugar en un mundo en constante evolución.

Al hablar de la Inteligencia Artificial (IA), implica que conozcamos términos clave como algoritmos, que son instrucciones para tareas; aprendizaje automático, que mejora sistemas con experiencia; y redes neuronales, inspiradas en el cerebro humano. También es esencial distinguir entre IA débil (tareas específicas) e IA fuerte (capacidades generales), así como entender el procesamiento del lenguaje natural (NLP) y la visión por computadora, que permiten a la IA interpretar lenguaje humano y datos visuales. Estos conceptos son fundamentales para comprender el impacto de la IA en diversos campos.

Sin embargo, dado que el ser humano aún no ha dominado completamente esta tecnología, su implementación plantea desafíos y riesgos que necesitan un análisis detenido. Incluso en el campo de la carrera armamentista, su uso podría conllevar un riesgo impredecible, tal como advirtió Stephen Hawking, sobre el posible impacto negativo que las tecnologías de superinteligencia artificial podrían tener en la humanidad (BBC mundo, 2018).

La utilización de la IA en las fuerzas armadas ha provocado un cambio significativo en las estrategias y operaciones de defensa alrededor del mundo. Un claro ejemplo de ello es el "Joint All-Domain Command and Control", el cual es el concepto que el Departamento de Defensa Estadounidense ha propuesto para integrar sensores de todas las fuerzas armadas en una red impulsada por IA (Álvarez, 2024). En la era moderna, las fuerzas armadas utilizan la IA como una herramienta esencial, que incluye el análisis de imágenes satelitales y la detección de amenazas cibernéticas, como se verá a lo largo del artículo. En este trabajo se analiza la implementación y desarrollo de la IA en el ámbito naval, examinando sus aplicaciones actuales y potenciales, junto con las implicaciones éticas y estratégicas en el campo de la seguridad nacional.

2. CONCEPTO Y FUNDAMENTOS DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO NAVAL

La Inteligencia Artificial constituye una disciplina de la ciencia computacional orientada a desarrollar sistemas capaces de ejecutar tareas que, tradicionalmente, dependen de la inteligencia humana, como el análisis de información, la identificación de patrones, la toma de decisiones y el aprendizaje autónomo (Bostrom, 2016). Su funcionamiento descansa en algoritmos, modelos matemáticos y grandes volúmenes de datos que permiten que las máquinas perfeccionen sus respuestas de manera progresiva. Entre sus principales áreas destacan el aprendizaje automático *(machine learning)*, el aprendizaje profundo *(deep learning)*, la visión por computadora y el procesamiento del lenguaje natural, tecnologías que han adquirido una relevancia creciente en el ámbito militar a nivel global.

En el ámbito naval, la IA se ha consolidado como una herramienta estratégica que complementa y amplifica las capacidades humanas en diversos procesos institucionales. Desde la gestión del personal hasta la conducción operacional, su incorporación contribuye a incrementar la eficiencia, reducir riesgos y fortalecer el proceso de toma de decisiones. Cabe resaltar que la IA no pretende sustituir el criterio humano, sino potenciar la precisión, la oportunidad y la seguridad de las decisiones adoptadas en entornos altamente exigentes.

En el campo del personal la IA permite analizar datos de desempeño, prever necesidades de rotación, evaluar perfiles profesionales y optimizar la asignación de tripulaciones. Este tipo de capacidades resulta fundamental para fortalecer los procesos de soporte asociados a la gestión de recursos humanos, especialmente en unidades operativas y administrativas, aportando directamente al bienestar institucional.

Asimismo, en el ámbito del entrenamiento los sistemas basados en IA facilitan el desarrollo de simuladores avanzados, capaces de recrear escenarios realistas de navegación, operaciones anfibias, control de averías o guerra electrónica. Estos entornos, al emplear modelos de aprendizaje adaptativo, ajustan su nivel de dificultad en función del progreso del usuario, promoviendo procesos de instrucción más seguros, eficientes y alineados con las necesidades formativas de las escuelas de entrenamiento y centros de capacitación naval.

En el campo operacional la IA se ha convertido en un multiplicador de fuerza para las armadas modernas. Plataformas equipadas con sensores, drones, radares e imágenes satelitales procesadas por sistemas inteligentes permiten vigilar amplias áreas marítimas, detectar amenazas, identificar embarcaciones sin señal o anticipar comportamientos ilícitos (Godfrey, 2023). Países de la región como Brasil y Colombia ya incorporan sistemas basados en IA para fortalecer el control del dominio marítimo, enfrentar la pesca ilegal, desarrollar operaciones SIGINT y apoyar el control del orden interno (Pardo, 2023). Estas capacidades contribuyen directamente a los procesos misionales vinculados a la defensa de la soberanía, a la seguridad marítima y al ejercicio de la autoridad en el mar.

Por otra parte, en el planeamiento estratégico la IA permite evaluar escenarios complejos, prever riesgos, analizar grandes volúmenes de información y optimizar la asignación de recursos. Esto respalda los procesos estratégicos institucionales y favorece una toma de decisiones más informada, oportuna y con menor margen de error.

Finalmente, en el ámbito educativo la IA incorpora herramientas como tutores virtuales, sistemas de evaluación automatizada y mecanismos de aprendizaje personalizado, fortaleciendo la formación doctrinaria, técnica y táctica del personal naval, contribuyendo a la mejora continua de las competencias profesionales.

En conjunto, la IA representa un elemento fundamental para las armadas de la región sudamericana, incluida la Marina de Guerra del Perú, al facilitar la modernización de sus procesos estratégicos, misionales y de soporte. Su adopción progresiva permitirá fortalecer el poder naval, mejorar la interoperabilidad regional y favorecer el desarrollo de una institución más preparada para afrontar los desafíos del siglo XXI.

3. INTELIGENCIA ARTIFICIAL EN LAS ARMADAS MODERNAS

La IA ha logrado convertirse en una herramienta fundamental en los ejércitos modernos. Su aplicación abarca desde la optimización de procesos logísticos hasta la toma de decisiones estratégicas en el campo de batalla. Sin embargo, la definición y aplicación de la IA varía significativamente entre el ámbito cotidiano y el naval.

En la vida diaria, la IA se manifiesta en formas familiares como los asistentes virtuales, los motores de recomendación en plataformas de streaming y los sistemas de reconocimiento facial en dispositivos móviles. Estas aplicaciones se centran en mejorar la experiencia del usuario, aumentar la eficiencia y facilitar la automatización de tareas rutinarias, como la automatización de alarmas, resolución de cuestiones cotidianas e incluso planificación de rutinas, a través de programas como Chat GPT o Microsoft Copilot.

Por otro lado, en el ámbito naval, la IA se emplea para objetivos mucho más ambiciosos y críticos. Un ejemplo destacado es el uso de algoritmos de aprendizaje automático para analizar grandes conjuntos de datos y predecir patrones de comportamiento enemigos, como se puede observar en la colaboración de HPTi con el Ejército de EE.UU., para diseñar una nube privada que transmite inteligencia en tiempo casi real a las tropas en Afganistán, incluyendo bases avanzadas. Este proyecto, iniciado en 2009 y lanzado en 2011, maneja petabytes de datos y utiliza computación de alto rendimiento para cumplir con las necesidades de análisis y procesamiento de inteligencia (Conway, 2012). Esto permite a los comandantes tomar decisiones informadas y estratégicas en tiempo real, optimizando el uso de recursos y minimizando riesgos para las tropas.

También se usa la IA en sistemas autónomos como drones y robots de combate, que pueden llevar a cabo misiones de reconocimiento, vigilancia y ataque, sin necesidad de intervención humana directa. El cambio paradigmático en la forma de llevar a cabo las operaciones militares se vé representado por estos avances tecnológicos, los cuales ofrecen nuevas capacidades y aumentan la eficacia en el campo de batalla.

El dron Bayraktar Akinci de Baykar, una empresa turca, ejemplifica el uso de la IA en sistemas autónomos, como drones y robots de combate. Este dron, equipado con IA avanzada, radares aire-aire y cámaras térmicas, puede llevar a cabo misiones de reconocimiento, vigilancia y ataque sin intervención humana directa. Recientemente, su capacidad para operar en terrenos difíciles permitió localizar el helicóptero del presidente iraní Ebrahim Raisi, destacando cómo la IA en sistemas autónomos puede optimizar la efectividad y precisión en misiones críticas (Jovanovski, 2024).

Se puede ver que sectores como el de defensa y seguridad, experimenten una revolución con cambios significativos. Un ejemplo de esto es la plataforma llamada Skylight (mayor información: https://www.skylight.global/), que utiliza imágenes satelitales junto con Big Data e IA para identificar áreas de pesca ilegal y posibles zonas de influencia. Como referencia a este caso, la Armada panameña interceptó una embarcación que pescaba ilegalmente en el Área Marina Protegida de Coiba Ridge, y la Guardia Costera de Filipinas rescató a la tripulación de una embarcación de recreo, ambos con la ayuda del suministro de datos AIS en tiempo casi real de Skylight (UNODC, 2022). Esta herramienta no solo evalúa estas áreas, sino que también anticipa posibles escenarios futuros relacionados con este tipo de actividades (Godfrey, 2023; Evans, 2018).

La integración de tres componentes fundamentales es implicada por la aplicación de IA en contextos militares. Estos incluyen el procesamiento de la información, que involucra aspectos lógicos, las plataformas y armamento utilizados en operaciones, lo cual representa el componente físico, así como la constante evaluación y comprensión del entorno de amenazas y condiciones operativas. Esta última depende en gran medida del factor humano.

4. USO OPERATIVO DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO MILITAR

La IA está transformando el ámbito militar al cambiar la forma en que se enfrentan los diversos desafíos operativos y estratégicos, gracias al uso de algoritmos avanzados, análisis de datos y sistemas autónomos como los que hemos visto anteriormente. Esto ha llevado a una nueva revolución y era de cambio en operaciones de la defensa, como se puede ver en potencias como Rusia y EEUU.

La aplicación operativa de la IA en los conflictos militares ha experimentado avances significativos en los últimos años, como lo ejemplifica el 510 PackBot desarrollado por Endeavor Robotics. Este robot móvil táctico multi-misión, diseñado para ser utilizado por tropas y socorristas en escenarios de alta amenaza, es un claro ejemplo de cómo la IA puede transformar las operaciones militares. Equipado con una amplia gama de sensores avanzados y cargas útiles, el PackBot puede realizar diversas tareas críticas, desde la vigilancia y la detección de agentes químicos, hasta el despeje de edificios y la desactivación de artefactos explosivos (Army Technology, 2014).

Una de las características más destacadas del PackBot es su capacidad para operar de manera autónoma en entornos peligrosos, lo que reduce significativamente la exposición

humana al riesgo. Este ha sido empleado por soldados en misiones de búsqueda en cuevas de Al Qaeda en Afganistán y en la detección de armas químicas y nucleares en Iraq, brindando una valiosa herramienta para enfrentar amenazas sin poner en riesgo la vida de los operadores (Yamauchi, 2004).

Si la IA llega a desempeñar roles de mando en operaciones militares o combates, sería el momento de comenzar a prepararse. El ámbito de la tecnología militar ingresaría en una nueva era de posibilidades con el crecimiento de la IA, la que en las operaciones tiene la capacidad de mejorar las posibilidades de ganar un conflicto. No se trata solo de potenciar las capacidades militares.

En este sentido, muchas naciones en todo el mundo están mejorando la capacidad de sus armadas mediante el uso de IA, utilizando los siguientes métodos que menciona Mishra en el Consejo Tecnológico Global:

- Redes neuronales artificiales y grandes volúmenes de datos combinados con capacidades de aprendizaje profundo de computadoras.
- Computadoras potenciadas por IA se utilizan para mejorar las capacidades de toma de decisiones, especialmente en casos de conflictos.
- Variedad de escenarios de combate hombre contra máquina, utilizando tecnologías tripuladas y no tripuladas en conjunto.

5. EL PAPEL DE LA INTELIGENCIA ARTIFICIAL EN LA OPTIMIZACIÓN PARA EL BIENESTAR MILITAR EN EL FUTURO

La IA está destinada a desempeñar un papel transformador en la optimización de la tecnología para el bienestar militar en el futuro. El mantenimiento predictivo de equipos y maquinaria es un área en la que la IA puede tener un impacto significativo. Este enfoque proactivo no solo disminuye el tiempo inactivo y las reparaciones costosas, sino que también garantiza la seguridad y el bienestar del personal al reducir al mínimo el riesgo de fallas en el equipo durante las operaciones.

Además, el análisis impulsado por la IA puede mejorar la conciencia situacional en el campo de batalla, al procesar y sintetizar grandes volúmenes de datos heterogéneos de diversas fuentes, como imágenes de satélite, drones de reconocimiento y sensores terrestres.

Este análisis en tiempo real proporciona a los comandantes información práctica, lo que les permite tomar decisiones informadas de manera rápida y efectiva, contribuyendo en última instancia al bienestar y seguridad, al facilitar operaciones militares más estratégicas y coordinadas (Casma Zárate, 2023).

Asimismo, los sistemas autónomos impulsados por IA, incluidos los vehículos aéreos no tripulados (UAV), los vehículos terrestres y las embarcaciones marítimas, tienen el potencial de revolucionar la logística militar y el transporte. Estas plataformas autónomas pueden realizar tareas como misiones de reaprovisionamiento, patrullas de vigilancia y misiones de reconocimiento con una intervención humana mínima, reduciendo la necesidad de que las tropas estén expuestas a entornos potencialmente peligrosos y permitiéndoles centrarse en objetivos estratégicos de nivel superior.

Ejemplos como el TALON robot de Foster-Miller, utilizado por equipos militares de desactivación de explosivos (EOD), ilustran cómo la IA puede mejorar la capacidad de los soldados para enfrentar amenazas en entornos peligrosos. Con la adición de nuevas funcionalidades, como un grado de libertad adicional en el brazo manipulador del robot, se pueden lograr avances significativos en la capacidad de respuesta y la eficacia de las operaciones de desactivación de explosivos en entornos marinos. La aplicación de la IA en el diseño y la mejora de robots EOD, representa sólo una faceta de cómo esta tecnología puede contribuir al bienestar y la seguridad en el ámbito naval (Army Technology, 2020).

En el ámbito de la salud, los diagnósticos médicos y la planificación del tratamiento impulsados por IA pueden mejorar el bienestar del personal militar, al proporcionar servicios de atención médica más precisos y oportunos. Los algoritmos de IA pueden analizar datos médicos, incluidos registros de pacientes, imágenes de diagnóstico e información genética, para ayudar a los proveedores de atención médica a diagnosticar enfermedades, predecir resultados del tratamiento y desarrollar planes de tratamiento personalizados adaptados a las

necesidades individuales (Mishra, 2022).

La implementación de la IA en diagnósticos y tratamientos médicos ofrece un potencial transformador en el bienestar del personal militar. Al analizar datos genéticos y moleculares, los médicos pueden prescribir medicamentos más eficaces, reduciendo errores y efectos adversos. Además, la IA puede predecir la probabilidad de enfermedades, permitiendo intervenciones preventivas. En el ámbito de la salud militar, esto se traduce en diagnósticos más precisos y tratamientos oportunos, como en el caso del examen de Papanicolaou, donde la IA ha mejorado la eficiencia y productividad de los laboratorios clínicos (Oguilve et al., n.d.).

6. AVANCE DE LA INTELIGENCIA ARTIFICIAL EN AMÉRICA LATINA

La IA se está convirtiendo en una tecnología clave que promete transformar nuestra forma de vida en el siglo XXI. En América Latina se está comenzando a investigar de qué manera esta tecnología puede beneficiar nuestra sociedad y economía. No obstante, todavía afrontamos desafíos significativos en cuanto a inversión, talento y cuestiones éticas.

En América Latina, el sector defensa y seguridad de la región está adoptando cada vez más tecnologías de IA para mejorar su capacidad operativa y fortalecer la seguridad; esto se podrá apreciar mejor con ejemplos que iremos viendo. En este contexto, es fundamental comprender las estrategias que están siendo implementadas y sus implicaciones para el desarrollo de la región.

La aplicación de IA en la vigilancia marítima es uno de los avances notables. En Colombia, se ha empezado a implementar la Plataforma de Inteligencia de Señales (SIGINT). La IA se utiliza para analizar grandes volúmenes de datos de comunicaciones interceptadas. Esto permite identificar patrones y posibles amenazas, mejorando la capacidad de las fuerzas armadas para anticiparse a actividades ilegales o terroristas, identificando patrones de comportamiento sospechoso en alta mar, como rutas de tráfico ilícito (Pardo, 2023). Gracias a esto, se ha logrado detectar de manera más rápida y efectiva actividades delictivas en aguas territoriales y zonas económicas exclusivas.

El SISFRON (Sistema Integrado de Monitoreo de Fronteras) representa también un ejemplo destacado del uso de la inteligencia artificial (IA) para mejorar la eficiencia operativa en las fuerzas armadas latinoamericanas. Este proyecto militar brasileño está diseñado para potenciar las actividades de control y monitoreo de fronteras. Mediante la integración de una variedad de tecnologías, como radares, drones, cámaras y sensores, busca fortalecer la vigilancia y seguridad a lo largo de las fronteras de Brasil. La IA desempeña un papel crucial en este sistema al ser utilizada para detectar patrones sospechosos, prever posibles eventos de seguridad y coordinar respuestas rápidas a las amenazas que puedan surgir en las fronteras (defensa.com, 2014).

A pesar de los avances prometedores, la integración de la inteligencia artificial en el ámbito naval también enfrenta obstáculos; por ejemplo, en Argentina la limitada capacidad técnica e investigativa en IA dificulta la incorporación de tecnologías avanzadas. Asimismo, surgen preocupaciones éticas y legales sobre el empleo de sistemas autónomos en operaciones marítimas, especialmente en lo que respecta a la protección de datos y la privacidad.

Ante los desafíos presentes, el desarrollo estratégico de la IA puede fortalecer las capacidades, mejorar la seguridad y fomentar la innovación en la región. Con una colaboración efectiva entre gobiernos, industrias y academias, América Latina puede aprovechar al máximo el potencial de la IA para asegurar la prosperidad y seguridad.

7. RIESGOS E IMPLICACIONES DE LA INTELIGENCIA ARTIFICIAL

La importancia de comprender los riesgos y las ventajas estratégicas de la IA y el aprendizaje automático en la competencia estratégica contemporánea es crucial. En un mundo donde la tecnología juega un papel cada vez más dominante en todos los aspectos de la vida, incluida la seguridad nacional, entender cómo los sistemas de IA pueden ser tanto una herramienta poderosa como una vulnerabilidad potencial, es esencial para la toma de decisiones informadas (Starck, Bierbrauer, Maxwell, 2022).

Por ejemplo, durante la Segunda Guerra Mundial las operaciones de engaño, como la Operación Quicksilver, ilustraron cómo los datos manipulados podrían alterar las percepciones del enemigo, un principio que sigue siendo relevante en el contexto actual de la IA (Fortes et al., 2023). Además, el desarrollo de sistemas de IA para la identificación de objetivos militares, destaca la necesidad de considerar la integridad de los datos utilizados para su entrenamiento, ya que la manipulación de este puede inducir errores graves en la identificación de objetivos.

Los métodos adversos, como el envenenamiento y la evasión, o comúnmente llamado “data poisoning”, presentan desafíos significativos para la efectividad de los sistemas de IA en entornos militares (DIGITAL360, 2024).

El problema del envenenamiento de datos no es teórico y tiene claras muestras en el mundo real. Por ejemplo, los algoritmos de inteligencia artificial de Google han sido engañados para ver tortugas como rifles, y una empresa china logró que un Tesla condujera hacia el tráfico en sentido contrario. En el ámbito militar, este tipo de ataques son especialmente preocupantes. Las defensas automatizadas podrían ser manipuladas para ignorar amenazas peligrosas o identificar erróneamente a fuerzas amigas como enemigas, comprometiendo así la seguridad. Este enfoque se asemeja a la táctica de envenenamiento utilizada en el pasado, como la inserción deliberada de información falsa en documentos de inteligencia para confundir al enemigo. De manera similar, la inserción de datos falsos o engañosos en los conjuntos de entrenamiento de sistemas de inteligencia artificial puede socavar su fiabilidad y precisión, lo que plantea serias preocupaciones sobre la confiabilidad de estos sistemas en situaciones críticas (Galle, 2022).

Del mismo modo, los ataques de evasión, que implican manipular la entrada de datos durante la operación de un sistema de IA para inducir errores en su salida, pueden ser tan sutiles como modificar ligeramente los píxeles de una imagen para engañar al sistema de reconocimiento de objetivos. Estos métodos ilustran cómo los adversarios pueden explotar las debilidades inherentes en los sistemas de IA para obtener una ventaja estratégica (Starck, Bierbrauer, Maxwell, 2022). En el contexto de las fuerzas armadas y el ámbito naval, a lo largo del tiempo se ha podido ver que en las operaciones son mínimos detalles los que determinan el resultado. Poniendo de ejemplo el bloqueo naval impuesto a Irak durante la Crisis del Golfo, los ataques de evasión podrían generar errores en la información y confusión en la coordinación y comunicación entre las unidades navales, lo que afectaría la eficacia del bloqueo.

La ingeniería inversa y los ataques de inferencia representan otras formas en las que los sistemas de IA pueden ser comprometidos (De los Llanos Dueñas, 2024). La ingeniería inversa busca extraer el conocimiento interno de un sistema de IA para reconstruirlo o descubrir sus debilidades. Por ejemplo, un adversario podría intentar aprender cómo un sistema de IA identifica objetivos mediante la observación de sus salidas y la manipulación de sus entradas. Esto permitiría al adversario desarrollar su propio sistema de IA que contrarreste las capacidades del sistema aliado.

La ingeniería inversa se ha visto a lo largo del tiempo. Durante la Guerra Fría, se encontraron ejemplos de uso de ingeniería inversa, tal como el caso de una aeronave taiwanesa que disparó un misil AIM-9B estadounidense a un caza soviético, utilizando tecnología inversa para adaptar el misil a su sistema de armas (López Rey, 2022). Así como en este caso y con la evolución actual de la tecnología, existe un mayor riesgo de que un adversario extraiga conocimiento interno de un sistema de IA para su beneficio.

Finalmente, los ataques de inferencia buscan determinar qué datos se utilizaron para entrenar un sistema de IA, lo que puede comprometer la confidencialidad de la información clasificada (Elosua Tomé, 2024). Por ejemplo, si un adversario logra identificar los datos utilizados para entrenar un sistema de reconocimiento de objetivos, podría deducir la estrategia y los recursos de la parte aliada, lo que socavaría la efectividad de dichos sistemas en el combate. En resumen, la comprensión de estos métodos adversarios y sus implicaciones es esencial para mitigar los riesgos y proteger la integridad de los sistemas de IA en entornos militares.

8. CONSIDERACIONES TÉCNICAS Y ÉTICAS PARA EL ÁMBITO NAVAL PERUANO

La Inteligencia Artificial (IA) está progresando en el ámbito naval, con el objetivo de mejorar la eficacia y la eficiencia de las operaciones navales (Stanley-Lockman, 2021). No obstante, su integración plantea importantes consideraciones técnicas y éticas que deben ser abordadas con atención. En este sentido, es crucial que Perú no pase por alto estas realidades y las implicancias del uso de estas tecnologías, dada su naturaleza innovadora.

Desde un punto de vista técnico, la integración de la IA en el proceso de toma de decisiones militares puede ofrecer información más rápida y precisa, incrementar la conciencia situacional y reducir los errores humanos. Sin embargo, su uso también presenta desafíos significativos que deben ser enfrentados de manera adecuada. En primer lugar, se destaca la importancia de la calidad de los datos utilizados por la IA, los cuales deben ser precisos y confiables para un funcionamiento óptimo (Starck, Bierbrauer, Maxwell, 2022).

En ausencia de esta calidad, la IA podría tomar decisiones incorrectas o inapropiadas, además de presentar fallas en su entrenamiento. Por consiguiente, resulta crucial que el Perú cuente con datos precisos y actualizados para asegurar la eficacia de la IA. En segundo lugar, es esencial contar con una infraestructura adecuada para su despliegue. En otras palabras, la IA requiere una infraestructura informática robusta y una red de comunicaciones confiable para operar de manera efectiva (Stanley-Lockman, 2021). Por lo tanto, la inversión en infraestructura se convierte en un aspecto fundamental para aprovechar al máximo el potencial de la IA en la toma de decisiones militares.

Desde una perspectiva ética, el uso de la IA plantea cuestiones importantes, como el impacto en la vida de los combatientes, no combatientes y civiles afectados por conflictos armados (Farabaugh, 2019). Por lo tanto, es crucial establecer políticas claras y transparentes para regular su uso en situaciones militares. En este sentido, para garantizar la efectividad del uso de la IA en el ámbito militar (Svenmarck, 2018), es necesario definir aspectos claves: en primer lugar, el Perú debe establecer políticas claras y transparentes sobre el uso de la IA y asegurar que todos los especialistas y operadores de la IA estén debidamente capacitados en su uso, supervisión y control. En segundo lugar, el Perú debe asegurar la disponibilidad de la infraestructura informática y de comunicaciones necesaria para el uso efectivo de la IA. Esto implica adquirir equipos y tecnologías adecuadas, así como establecer una red de comunicaciones segura y confiable. En resumen, para aprovechar al máximo el potencial de la IA en la toma de decisiones

militares, resulta esencial realizar inversiones significativas en infraestructura (Bossio, 2023).

9. CONCLUSIONES

En conclusión, la evolución de la tecnología, especialmente en el ámbito de la IA está redefiniendo la forma en que interactuamos con el mundo, sobre todo en contextos navales y de seguridad nacional. A medida que la IA se convierte en una herramienta indispensable para optimizar la tecnología en beneficio del bienestar naval, surgen tanto oportunidades como desafíos significativos. La capacidad de la IA para mejorar la eficiencia operativa, aumentar la conciencia situacional y también reducir los errores humanos representa un avance prometedor en el ámbito naval, ofreciendo un potencial sin precedentes para mejorar la seguridad y el bienestar del personal de las fuerzas armadas.

No obstante, la aplicación de la IA en las fuerzas armadas también plantea peligros y preocupaciones éticas que requieren una consideración cuidadosa. Desde desafíos técnicos relacionados con la calidad de los datos y la infraestructura necesaria, hasta cuestiones éticas sobre el impacto en la vida humana y la regulación del uso de la IA en situaciones militares; es fundamental abordar estos aspectos para garantizar el uso ético y responsable de esta tecnología transformadora.

En América Latina, el avance de la IA en el ámbito naval refleja una tendencia creciente hacia la adopción de tecnologías emergentes para mejorar la seguridad y también fortalecer las capacidades defensivas en la región; sistemas como el SISFRON y plataformas como la SIGINT, demuestran este avance. Si bien existen desafíos por superar, como la limitada capacidad técnica y de investigación en IA, y también las preocupaciones éticas sobre el uso de sistemas autónomos en operaciones navales, el desarrollo estratégico de la IA ofrece oportunidades para fortalecer las capacidades navales y promover la innovación en la región.

En última instancia, para aprovechar plenamente el potencial de la IA en las fuerzas armadas y garantizar su contribución al bienestar y la seguridad del personal, es necesario abordar tanto los aspectos técnicos como éticos de su implementación. Esto requiere una inversión significativa en infraestructura, políticas claras y transparentes para regular su uso, y una capacitación adecuada para los especialistas y operadores de la IA. Con un enfoque integral y colaborativo, la IA puede convertirse en una herramienta poderosa para optimizar la tecnología en beneficio del bienestar militar y la seguridad nacional en el futuro.

Referencias

Akgül, A. (2015, Febrero 17). Artificial Intelligence Military Applications. Ankara University SBF Journal, 45(1). DergiPark Akademik.

Álvarez, R. (2024, Mayo 2). IA y Defensa: Explorando las Fronteras de la Tecnología Militar. Defensa.com. https://www.defensa.com/industria/inteligencia-artificial-defensa-explorando-fronteras-tecnologia

Arenas Pérez-Seoane, C., Rodelgo Lacruz, M., & Núñez Ortuño, J. M. (2015-2016). Desarrollo de un sistema de inteligencia artificial para la supervisión y detección de anomalías en rutas marítimas. Repositorio institucional del Centro Universitario de la Defensa. http://calderon.cud.uvigo.es/handle/123456789/254

Army Technology. (2014, Agosto 6). iRobot 510 PackBot Multi-Mission Robot. Army Technology. https://www.army-technology.com/projects/irobot-510-packbot-multi-mission-robot/?cf-view

Army Technology. (2020, Febrero 21). TALON Tracked Military Robot. Army Technology. https://www.army-technology.com/projects/talon-tracked-military-robot/

BBC Mundo. (2018, March 15). 4 advertencias de Stephen Hawking sobre los peligros que amenazan a la humanidad. BBC. Retrieved May 19, 2024, from https://www.bbc.com/mundo/noticias-43415617

Bossio Ballesteros, V. E. (2023, Octubre 26). La Inteligencia Artificial en el Ámbito Militar: Una Herramienta Relevante y Útil. Revista Seguridad y Poder Terrestre, 2(3), 53-61. https://doi.org/10.56221/spt.v2i3.33

Bostrom, N. (2016). Superinteligencia : caminos, peligros, estrategias (M. Alonso, Trans.). Teell Editorial, S.L.

Casma Zárate, C. (2023, Septiembre 02). La doble cara de la Inteligencia Artificial para la toma de decisiones. Universidad Cesar Vallejo. https://www.ucv.edu.pe/noticias-general/la-doble-cara-de-la-inteligencia-artificial-para -la-toma-de-decisiones

Conway, S. (2012, febrero 6). Big Data Cloud Delivers Military Intelligence to U.S. Army in Afghanistan. datanami. https://www.datanami.com/2012/02/06/big_data_cloud_delivers_military_intelligence_to_u-s-_army_in_afghanistan/defensa.com. (2014, noviembre 10). Brasil inaugura el SISFRON. Defensa.com. https://www.defensa.com/brasil/brasil-inaugura-el-sisfron

De los Llanos Dueñas, A. (2024, Abril). Ingeniería Inversa en Ciberseguridad: Revelando los Secretos del Software Malicioso. Minery Report. https://mineryreport. com/blog/ingenieria-inversa-ciberseguridad-desentranando-codigo/DIGITAL360,

R. (2024, February 23). El envenenamiento de datos, un peligro para toda la AI. IT Masters Mag. Retrieved May 22, 2024, from https://www.itmastersmag.com/ciberseguridad/el-envenenamiento-de-datos-un-peligro-para-toda-la-inteligencia-artificial/

ELOSUA TOMÉ, J. (2024, Abril 10). Ataques a la Inteligencia Artificial (IV): Privacy Attacks. telefonicatech. https://telefonicatech.com/blog/ataques-ia-privacy-attacks

Evans, I. (2018, Febrero 14). Deeply Talks: Fighting Illegal Fishing With Big Data, Robots and A.I. The New Humanitarian. https://deeply.thenewhumanitarian.org/oceans/articles/2018/02/14/deeply-talks-fighting-illegal-fishing-with-big-data-robots-and-a-i

Fortes, S., Aguilar, J. D., & Pérez, A. (2023, December 5). Operación Quick Silver, de Susana Fortes. Zenda. https://zendalibros.com/operacion-quick-silver-de-susana-fortes/

Galle, A. (2022, Enero). Drinking from the Fetid Well: Data Poisoning and Machine Learning. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/2022/january/drinking-fetid-well-data-poisoning-and-machine-learning

Gobierno, T. (2019, July 15). Estados Unidos lanza Plan Estratégico de Inteligencia Artificial. u-GOB. https://u-gob.com/estados-unidos-lanza-plan-estrategico-de-inteligencia-artificial/

Godfrey, M. (2023, March 20). Skylight becoming key tool in fight against IUU fishing. SeafoodSource. Retrieved May 19, 2024, from https://www.seafoodsource.com/news/premium/environment-sustainability/skylight-becoming-key-tool-in-fight-against-iuu-fishing

Jovanovski, K. (2024, Mayo 28). Sector turco de drones se impulsará por su papel en la búsqueda del accidente del Raisi. Jerusalem Post. https://www.jpost.com/spanish/omg/article-803949

Micó, J. L., & Lane, J. (2018, March 23). La guerra fría de la inteligencia artificial. La Vanguardia. https://www.lavanguardia.com/tecnologia/20180323/441857328514/guerra-fria-inteligencia-artificial.html

Mishra, s. (2022, June 27). Artificial Intelligence in Military Operations. Global Tech Council. https://www.globaltechcouncil.org/artificial-intelligence/artificial-intelligence-in-military-operations/

National Strategy for Homeland Security. (2018, Diciembre 22). Wikipedia. https://en.wikipedia.org/wiki/National_Strategy_for_Homeland_Security

Oliveira, N. (2022, October 13). Marina Brasileña despliega nuevo escuadrón de drones. Dialogo-Americas.com. https://dialogo-americas.com/es/articles/marina-brasilena-despliega-nuevo-escuadron-de-drones/

Oguilve, G., Bejarano, A., Azofeifa, C., & Bermúdez Tellería, J. (n.d.). "Los laboratorios clínicos: retos, cambios y oportunidades en la Medicina Personalizada basada en Ciencia de datos e Inteligencia artificial. El caso de Costa Rica." INNOVA salud digital. https://pps.hospitalitaliano.org.ar/landing/innova-salud-digital/articulos/los-laboratorios-clinicos-retos-cambios-y-oportunidades-en-la-medicina-personalizada-0

Pardo, J. (2023, December 10). Las Fuerzas Militares de Colombia ahora apuestan por la revolución de la inteligencia artificial. Infobae. https://www.infobae.com/colombia/2023/12/10/las-fuerzas-militares-de-colombia-ahora-apuestan-por-la-revolucion-de-la-inteligencia-artificial/

Reina, D. M. (2024). Revista ¿Cómo ves? - Divulgación de la Ciencia, UNAM. Revista ¿Cómo ves? https://www.comoves.unam.mx/numeros/articulo/162/la-singularidad-de-stephen-hawking

Romero Mier, S. G. (2019, Abril 2). Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados. Revista de la Escuela Superior de la Guerra Naval, 16(1), 51-70. https://doi.org/10.35628/resup.v16i1.67

Starck, N., Bierbrauer, D., & Maxwell, P. (2022, January 18). Artificial Intelligence, Real Risks: Understanding-and Mitigating-Vulnerabilities in the Military Use of AI - Modern War Institute. Modern War Institute -. https://mwi.usma.edu/artificial-intelligence-real-risks-understanding-and-mitigating-vulnerabilities-in-the-military-use-of-ai/

UNODC. (2022). SKYLIGHT-GMCP PARTNERSHIP. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/bmb/UNODC_AI2_partnership.pdf

Villuendas, B. (2024, January 31). Ramón López de Mántaras: "No creo en el tecnosolucionismo". Cuatroochenta. https://cuatroochenta.com/entrevistas/ramon-lopez-de-mantaras-tecnosolucionismo-inteligencia-artificial/

Yamauchi, Brian. (2004). PackBot: A Versatile Platform for Military Robotics. Proc. SPIE. 5422. 10.1117/12.538328.

Yushu, L. (2019, Abril 16). Desarrollando un sistema chino de seguridad nacional transparente, sostenible y diverso. Spanish people daily. http://spanish.peopledaily.com.cn/n3/2019/0416/c31621-9567284.html

Año 2024, Vol. 21, Nº 3, pp. 72 - 85.
DOI: https://doi.org/10.35628/resup.v16i2.174

De las alertas al análisis: la importancia de una Central de Inteligencia donde la IA acelera pero el analista proyecta

From alerts to analysis: the importance of an Intelligence Center where AI accelerates but the analyst projects

Recibido: 25 de septiembre del 2025 | Aceptado: 05 de diciembre del 2025

Bernard Cardozo Lozano
https://orcid.org/0009-0008-7728-0086

Capitán de Corbeta de la Marina de Guerra del Perú. Se graduó como Alféréz de Fragata en el 2010. Es licenciado en Ciencias Marítimo Navales por la Escuela Naval del Perú. Calificado en Electrónica e Inteligencia. Se desempeñó como Jefe de Comunicación Estratégica en el Ejercicio Multinacional BRACOLPER OURO desarrollado en el año 2024 entre la Marina de Brasil, Armada de Colombia y Marina de Guerra del Perú. Actualmente, es Jefe de la División de Frente Interno del Departamento de Inteligencia de la Dirección de Inteligencia de la Marina.

Email:bernard.estudios@gmail.com

Resumen: Entre los retos y desafios que enfrenta la inteligencia estratégica se encuentra la sobreabundancia de datos y cómo transformarla en conocimiento útil para la toma de decisiones. En este marco, la Central de Inteligencia se presenta como una plataforma viva, integrada de fuente abierta y fuente cerrada, con la capacidad de aplicar inteligencia artificial (IA) para generar productos multidinámicos de inteligencia. Las alertas constituyen un paso importante de advertencia para los usuarios del sistema de inteligencia respecto a las diferentes amenazas; sin embargo, el artículo no pretende desprestigiar esas señales, sino centrarse en el análisis. En ese sentido, traza el lineamiento de discriminar el ruido y direccionar al usuario, reducir la incertidumbre y anticipar escenarios. La

IA ofrece rapidez, potencia, optimización de procesos, entre otros, pero no deja de lado al analista, sino que se complementa para que él interprete y proyecte la situación del entorno. Bajo esta línea de ideas, el artículo finaliza entendiendo que la base de todo analista es la integridad, creando concientización en las mejoras realizadas y que con capacidades de primer nivel es necesario que sean empleadas de la mejor manera.

Palabras clave: Inteligencia estratégica, central de inteligencia, fuentes abiertas, fuentes cerradas, inteligencia artificial, análisis de datos, adaptabilidad, analista.

Abstract: *Among the challenges faced by strategic intelligence is the overabundance of data and how to transform it into useful knowledge for decision-making. In this framework, the Intelligence Center emerges as a living platform, integrating open and closed sources, with the ability to apply artificial intelligence (AI) to generate multi-dynamic intelligence products. Alerts constitute an important step in warning intelligence system users about different threats; however, the article does not seek to undermine these signals, but rather to emphasize the importance of analysis. In this sense, it outlines the guideline for filtering noise and directing the user, reducing uncertainty, and anticipating scenarios. AI provides speed, power, and process optimization, among other advantages, but it does not replace the analyst; instead, it complements their role in interpreting and projecting the operational environment. Along these lines, the article concludes that the foundation of every analyst is integrity, fostering awareness of improvements achieved, and emphasizing that top-level capabilities must be applied in the best possible way.*

Keywords: *Strategic intelligence, intelligence center, open sources, closed sources, artificial intelligence, data analysis, adaptability, analyst.*

1. INTRODUCCIÓN

Sun Tzu mencionó “Conócelo todo, pero actúa solo cuando sea el momento oportuno” (Sun Tzu, 1910/2005). Esta máxima no se limita al campo militar, sino que es transversal al trabajo en inteligencia debido a la importancia de manejar información de interés. Tal como estableció Sherman Kent, la inteligencia es el conocimiento organizado y evaluado que se presenta al tomador de decisiones para ayudarle a comprender la realidad y a actuar sobre ella (Kent, 1949). Conocer todo significa que múltiples datos y abundante información está disponible

para nosotros. Por otro lado, actuar en el momento oportuno, implica filtrar grandes volúmenes de información para generar las alertas correspondientes. En la actualidad existe una sobreexposición digital, lo cual podría ocasionar una sobrecarga de alertas en el caso que no sean filtradas, separadas y evaluadas por los analistas expertos. Las alertas son consideradas advertencias tempranas que nos dan señales tempranas de un posible riesgo o situación del entorno. De acuerdo al aporte de Richard Betts, la advertencia de inteligencia es el esfuerzo por detectar y comunicar indicios de un peligro antes de que se materialice (Betts, 2007). Estas alertas nos avisan que "algo está ocurriendo", lo cual es importante porque constituye la primera señal de aviso a nuestros usuarios principales, siendo comunicada por los canales correspondientes.

En este sentido, descifrar tendencias y aprender a separar señales de ruido en medio de un entorno saturado de información, es el análisis que en una Central de Inteligencia se debe realizar centrado en el objetivo. La Doctrina de Inteligencia de la Marina (2022), define que una Central de Inteligencia Naval centraliza, procesa y difunde oportunamente la información requerida, así como actualiza permanentemente el conocimiento sobre las capacidades del enemigo o adversario y los escenarios de riesgo.

Aunque exista una sobreabundancia de información por la cantidad de datos que circulan en los diversos medios digitales, no necesariamente va a existir mayor claridad, por eso Kenneth Waltz mencionó que la incertidumbre es inherente a sistemas donde la información nunca es completa (Waltz, 1979). En inteligencia estratégica, las alertas corren el riesgo de perder su función de advertencia temprana, sin un mecanismo de discriminación, depuración y priorización.

Este artículo se centra en la importancia del análisis en base a las alertas recibidas, donde los analistas recepcionan diversas señales para generar productos multinámicos de inteligencia; pero para ello requieren construir inteligencia básica, observando tendencias y patrones considerando todas las alertas producidas en el sistema, contrastando, filtrando, ordenando, procesando y proyectándola a través de herramientas de análisis y obtener así una mejor situación del entorno. Todo es parte de un proceso, no hay eventos aislados. Recordemos que advertir es necesario, pero comprender es aún más indispensable. Ante un entorno saturado de fake news y narrativas construidas bajo intereses de actores invisibles, es fundamental discernir presuntos hechos de manipulación.

FIGURA 1
De las alertas al salto estratégico: visualización de la transición hacia una Central de Inteligencia

Fuente: Elaboración con apoyo de ChatGPT (2025).

El principio de una Central de Inteligencia no está en acumular datos sino en transformarlos en ventaja para el decisor. La máxima es: "lo que no se integra se pierde; lo que se integra, se proyecta"; porque la integración de datos deja de ser un simple proceso técnico y pasa a ser una ventaja decisional, donde la Central de Inteligencia proyecta lo que recibe de múltiples entradas "dispersas" para convertirla en conocimiento aplicable para la toma de decisiones. Este pensamiento es el que se debe cultivar en un analista de inteligencia en todos los niveles, porque la trascendencia de una Central de Inteligencia está relacionada a un sistema vivo, colaborativo e interconectado con la capacidad de cruzar datos en tiempo casi real y generar conocimiento a través de plataformas de integración de fuentes abiertas y cerradas, aprovechando herramientas de análisis y tecnológicas, como lo es la inteligencia artificial (IA). La inteligencia artificial es el estudio de agentes que perciben su entorno y realizan acciones que afectan ese entorno (Russell y Norvig, 2010). En el presente artículo y en la línea de inteligencia estratégica, implica que la IA, más allá de un conjunto de algoritmos, es un sistema capaz de procesar grandes volúmenes de datos y que permite interactuar en un mínimo de tiempo, realizando múltiples tareas que resultarían inviables para un solo analista. De esta manera, si nos resistimos a la IA, nos resistimos al cambio, en el sentido de rechazar una herramienta que permite optimizar nuestros procesos analíticos

tradicionales. La clave está en saberla emplear de la forma correcta y sin perder el enfoque.

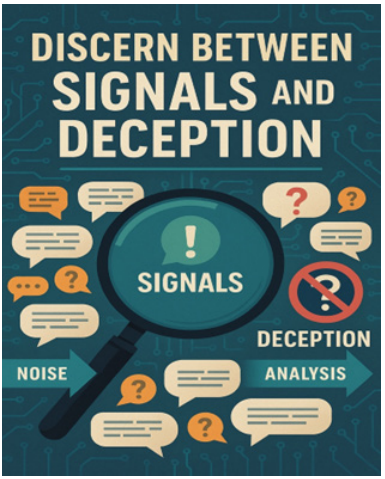
La Central de Inteligencia no es un complemento opcional, sino un concepto de doctrina, definido anteriormente y que con la tecnología mejora sus capacidades para transformar diferentes alertas en una plataforma integrada de análisis. Su aporte consiste en el que el analista pueda articular, integrar tecnología y realizar análisis crítico, apoyándose en la IA para que la inteligencia estratégica cumpla con su misión esencial: anticipar las amenazas y asegurar una ventaja decisional en un escenario global que cambia incluso mientras estamos escribiendo este artículo.

2. ANÁLISIS

2.1. Discriminar el ruido, direccionar al usuario

Es importante comprender que en la era digital existe una avalancha de información que está siendo instrumentalizada para contaminar a los analistas e incluso confundirlos. El ruido es toda información que confunde al analista, puede ser irrelevante, manipulada, distorsionada y que no aporta valor. La clave está en distinguir con precisión entre las señales y el engaño, así como lo esencial y lo superfluo, manteniendo un enfoque crítico que permita alertar a los usuarios del sistema, de acuerdo a su jurisdicción.

FIGURA 2
Discernir entre señales y engaño.



Fuente: Elaboración con apoyo de ChatGPT (2025).

Zegart (2022) advierte que la expansión de fuentes abiertas (OSINT, por sus siglas en inglés de Open Source Intelligence) democratizó el acceso a los datos, pero también multiplicó los riesgos de contaminación informativa. Tengamos presente que OSINT consiste en obtener, procesar y explotar información disponible públicamente, para producir conocimiento accionable (Steele, 2002). Esto nos muestra que mientras mayor acceso tengamos a la información, mayor riesgo tendremos de vulnerabilidad al ruido. A su vez, Rid (2016) recuerda que la guerra contemporánea ha convertido la desinformación en un

arma, diseñada para saturar con señales contradictorias y retrasar la respuesta del adversario. Esto nos muestra que el ruido siempre está presente, por lo que requiere aplicar doctrina, emplear técnicas analíticas y comprender el contexto en toda su complejidad. La normativa nacional, expresada en el Decreto Legislativo N.° 1141, es clara: la inteligencia debe regirse por los principios de pertinencia y utilidad. Dicho marco obliga a priorizar aquello que contribuye directamente a la seguridad y defensa, descartando lo superfluo.

Heuer y Pherson (2010) advierten que, si el analista lo descuida, corre el riesgo de elaborar informes llenos de datos inútiles. Clark (2019), en cambio, plantea una inteligencia "centrada en el objetivo", lo que implica formular siempre la pregunta clave: ¿qué necesita saber el decisor para actuar con ventaja? Direccionar al usuario significa, en este sentido, conocer sus requerimientos esenciales de información, cuáles son sus prioridades de Comando, qué amenazas emergentes no identificadas inicialmente son de su preocupación, cuáles son sus próximas operaciones, qué inducción necesita para sus apreciaciones, entre otras.

En la práctica, esta interacción se traduce en ajustar los productos de inteligencia a los diferentes usuarios. Bajo esta línea, la Central de Inteligencia concebida como una plataforma integradora, proyecta productos multinámicos de inteligencia acordes a sus requerimientos, entendiendo la urgencia y velocidad de información para procesar; y la manera de alcanzarlo es optimizando procesos y datos a través de la IA, a fin de asegurar que el flujo informativo se organice en función de los intereses de la Institución.

El ejercicio multinacional BRACOLPER OURO, llevado a cabo en el año 2024, demostró que la interoperabilidad fue efectiva porque la información compartida se ajustó a las necesidades inmediatas entre la Marina de Brasil, la Armada de Colombia y la Marina de Guerra del Perú. Del mismo modo, radica en la importancia de elaborar productos multidinámicos, diseñados en función del usuario y no en esquemas rígidos.

Discriminar el ruido y direccionar al usuario son tareas inseparables. La máxima es que filtrar sin comprender al decisor es tan inútil como intentar satisfacerlo con datos irrelevantes. Solo al integrar ambas dimensiones, la Central de Inteligencia cumple su propósito esencial: transformar señales dispersas en conocimiento proyectivo, útil y oportuno, que otorgue ventaja decisional al alto mando en un entorno contaminado por la información.

2.2. Integrando la fuente abierta + fuente cerrada

Por cierto, ninguna fuente por sí sola basta. El espíritu de integración entre la fuente abierta y la fuente cerrada es la convergencia entre lo amplio y lo exclusivo, lo superficial y lo profundo, transformándose en conocimiento estratégico para proporcionar al decisor un producto coherente, verificable y oportuno.

La validación cruzada es indispensable. Es cierto que puede haber señales divergentes donde lo abierto y cerrado no conversen entre sí, así como sesgos de confirmación entre los mismos analistas. El reto es contrastar evidencias, ponderarlas según confiabilidad y teniendo a la mano lo actual, porque al fin y al cabo, ¿de qué sirve tener todas las piezas del rompecabezas sino puedo armarlo para apreciarlo?

FIGURA 3
Integración de fuentes abiertas y cerradas..

Fuente: Elaboración con apoyo de ChatGPT (2025).

La Central de Inteligencia no pretende acumular datos dispersos, sino evaluarlos, validarlos, integrarlos y visualizarlos. La normativa nacional, reflejada en el Decreto Legislativo N° 1141 (2012) y en la Doctrina de Inteligencia Nacional (2021), ya subraya la necesidad de contar con canales seguros y exclusivos para intercambiar información. En ese marco, la Central de Inteligencia aparece como una plataforma capaz de articular fuentes abiertas y cerradas, en generar productos multinámicos de inteligencia para la toma de decisiones.

La IA se presenta como un aliado para integrar fuentes. La posibilidad de contar con algoritmos capaces de correlacionar grandes volúmenes de datos abiertos con señales cerradas a nivel local, permite detectar patrones ocultos en tiempo oportuno. La máxima es que la máquina no interpreta intenciones, es el analista quien debe conectar el dato con el contexto estratégico.

En múltiples conflictos recientes, desde Gaza hasta el frente ruso-ucraniano, lo que ha marcado la diferencia no ha sido tener más datos, sino integrarlos como OSINT, inteligencia de señales (SIGINT, por sus siglas en inglés de Signals Intelligence) y fuentes humanas. SIGINT comprende la recopilación y análisis de comunicaciones, emisiones electrónicas y señales utilizadas, para comprender

capacidades y actividades de un objetivo (Warner, 2009). Entonces, todos los datos analizados en forma aislada, esos datos hubieran dado una imagen parcial o incluso engañosa; pero integrados, permitieron anticipar acciones adversarias, corregir sesgos informativos y dar ventajas decisionales sustanciales.

La Central de Inteligencia institucionaliza este pensamiento. No se limita a recopilar insumos, sino que los procesa con un objetivo: servir al decisor. Clark (2019) recuerda que la inteligencia debe estar centrada en objetivos. En este marco, integrar no significa abarcarlo todo, sino seleccionar lo relevante y combinarlo en función de la necesidad estratégica. Este pensamiento no cuestiona la cantidad de alertas sino que reconoce que aspectos específicos en determinadas situaciones conllevan a que no perdamos el enfoque, en estar centrados y tener claro lo urgente versus lo importante.

Integrar fuentes abiertas y cerradas no es una opción metodológica, sino una exigencia doctrinaria aplicada a todos los niveles de inteligencia; comprendiendo que no es un asunto de querer acaparar sin objetivo, sino de separar y seleccionar lo relevante para convertirlo en producto único para el decisor.

2.3. Análisis de datos aplicando la IA

Esto es un trabajo compartido, compenetrado; es como que la IA nos ofrece potencia y velocidad; pero el analista tiene el contexto y sentido estratégico. Juntos configuran una alianza que multiplica capacidades, pero ¿es esto cierto?

El artículo tiene claro un asunto, si no aplicamos la IA en nuestra forma de trabajar estamos perdidos y nos quedaremos relegados en algún momento. Esto no está en discusión. No tiene que ver con que la IA haga todo el trabajo por nosotros, ni que piense lo que nosotros deberíamos de pensar, sino en optimizar el análisis aplicando IA ya sea para una red cerrada y local, considerando el nivel de clasificación de la información; todo esto depende de la cultura organizacional.

La máxima está en que la IA es un apoyo, no reemplaza al analista. La velocidad de los productos multinámicos demandados por el Alto Mando y su nivel de objetividad requieren sí o sí mecanismos capaces de revisar millones de registros en segundos, detectando patrones que escaparían a un equipo humano bajo la presión diaria. Gracias a ello, el analista libera esfuerzos de tareas rutinarias y concentra su atención en la interpretación estratégica. Clark (2019) subraya que el análisis debe centrarse en el objetivo; en esa línea, la IA resulta un socio importante al reducir la carga mecánica y favorecer la atención en lo realmente esencial.

La máquina procesa, pero es el analista quien interpreta, proyecta y decide. Este aspecto debe recordarse siempre. Analizar datos a través de la IA es contar con toda la data, pero ordenada, clasificada, validada y a todo eso añadir funcionalidades que nos permitan mejorar nuestra comprensión sobre ciertas amenazas.

FIGURA 4
Integración de diversas fuentes de inteligencia mediante IA para generar productos estratégicos.

Fuente: Elaboración con apoyo de ChatGPT (2025).

Zegart (2022) advierte que el exceso de datos abiertos puede amplificar la desinformación si no se somete a un marco crítico. En términos simples: la máquina ofrece una primera imagen, pero corresponde al analista decidir qué constituye señal y qué no es más que ruido, como lo he explicado antes.

Plataformas de IA pueden combinar imágenes satelitales, interceptaciones técnicas, reportes e informes de inteligencia humana, audios y videos de conferencias, entre otros, generando un valor agregado a los productos multinámicos de inteligencia. Sims (2022) menciona que la ventaja estratégica no surge de información perfecta, sino de un análisis suficiente y oportuno. El nivel de entrenamiento del algoritmo es proporcional al nivel de objetividad; sin embargo, las necesidades cambian y las actualizaciones siempre son necesarias.

Referente a las amenazas, existe evidencia que la IA permite identificar rutas de tráfico ilícito; sin embargo, no fue dejado de lado el rol de los analistas, quienes interpretaron esos hallazgos en un marco geopolítico, distinguiendo entre amenazas reales y movimientos marginales. Lo mismo ocurre en el ámbito cibernético: los sistemas automáticos generan miles de alertas diarias, pero solo el criterio humano establece prioridades y proyecta impactos estratégicos.

Steele (2002) advertía que la inteligencia debía sustentarse en múltiples herramientas, sin permitir que ninguna monopolice el proceso. Es decir, la inteligencia no depende de una sola herramienta, software, aplicativo o método; sino que es un proceso complementario porque multiplica capacidades para el analista. No debemos caer en el error de que la IA nos va a realizar todo el

proceso, ni menos caer en la tentación de delegarle todo el proceso. La IA se convierte en un acelerador dentro de un sistema híbrido, ofreciendo potencia para que el analista proyecte con el criterio y en el contexto de la situación del entorno.

2.4. Lo único constante es el cambio

Lo que no se adapta, se extingue. En un contexto como el que mencionamos en el artículo, donde la situación del entorno es cambiante, la dinámica de la tecnología transforma nuestro día a día, y la información está sobredimensionada; necesitamos contar con analistas íntegros que sustenten la confianza para trabajar, el deseo de superación y la trazabilidad de las gestiones realizadas para tener continuidad como sistema de inteligencia.

FIGURA 5
Integridad como base del analista donde se configuran alertas y análisis en una Central de Inteligencia.

Fuente: Elaboración con apoyo de ChatGPT (2025).

La clave está en entender que no somos una dirección diferente, sino una dirección referente, y esta conlleva realizar cambios de toda índole, pero una de ellas y de las más importantes, son las personas que lo conforman. El tema de valores no es un tema menor, en una organización es lo más importante. En el campo de inteligencia se aplica el mismo principio; lo que no se adapta se extingue, porque el verdadero cambio comienza con las personas, se consolida en un equipo y se visualiza en el trabajo, así como las propuestas para el Alto Mando.

Por otro lado, la Central de Inteligencia bien definida como parte de nuestra doctrina, en este artículo es concebida como una plataforma integradora, un sistema vivo, que interconecta fuentes diversas, aplica herramientas de IA optimizando procesos, métodos y aplicaciones, para que en tiempo casi real tengamos un producto multinámico de inteligencia. Sims (2022) complementa que la ventaja estratégica no depende de información perfecta, sino de productos suficientes y oportunos que permitan actuar antes que el adversario. Recordemos,

lo perfecto es enemigo de lo bueno y en un entorno como el que atravesamos, la Central de Inteligencia es clave para actualizarnos en el tiempo oportuno.

Este tipo de cambios no sólo tiene que ver con una transformación tecnológica, sino también social y política. Por ejemplo, en el mes de septiembre del presente año hemos sido testigos del modus operandi de un grupo denominado Generación Z liderado por jóvenes empleando medios y plataformas digitales para unirse a causas de reclamos ante el Estado democrático; de la misma manera, las organizaciones criminales ajustan sus operaciones cada vez más sofisticadas; y respecto a los ciberataques, estos evolucionan constantemente con el avance tecnológico. Todo ello demanda un sistema flexible en el sentido de romper con lo tradicional, de probar nuevas técnicas en automatización, de recurrir a optimización aplicando la IA creando tableros con flujos de datos, entre otros productos de interés.

Otro aspecto es la importancia de los canales exclusivos y seguros de inteligencia (Decreto Legislativo N.° 1141). El desafío es evitar que tales estructuras se vuelvan rígidas y lograr que evolucionen frente a nuevas amenazas, desde ciberataques hasta conflictos sociales con potencial de expansión digital. La Central de Inteligencia, como espacio integrador, debe garantizar la revisión constante de procesos internos y ofrecer a los analistas procedimientos formales para cuestionar supuestos y ajustar lineamientos de análisis.

Es importante considerar que las alertas proporcionadas por las agencias de inteligencia son clave en el mapeo de la situación del entorno; estas recaen en los analistas quienes con la competencia especializada en las diferentes amenazas, emplean herramientas de análisis estructuradas, rol fundamental de todo analista de inteligencia que realiza análisis de todo tipo como el descriptivo, explicativo, predictivo y prescriptivo, entre otros, sea en el nivel estratégico o en el que sea requerido por el comando. Esto se resume en pensar, relacionar, contrastar y analizar; por ello, la importancia de integrar diversas fuentes en tiempo casi real optimizando procesos. Reducir el tiempo en la elaboración de un documento de inteligencia ante la velocidad del requerimiento del usuario es determinante.

Las personas y las técnicas pueden cambiar, pero la integridad debe permanecer. La Central de Inteligencia debe institucionalizar este principio, asegurando que los productos analíticos se empleen con fines correctos y no negociables a otros intereses; antes bien, que se realicen con flexibilidad, oportunidad y disposición a la evaluación continua. Su fortaleza no está en prometer certezas absolutas, sino en entregar conocimiento dinámico y prospectivo que permita a nuestra Institución la toma de decisiones. Bajo esta perspectiva, la adaptabilidad se convierte en

el valor estratégico por excelencia y en la condición indispensable para que la inteligencia cumpla su misión fundamental.

3. CONCLUSIONES

La evolución de la inteligencia estratégica demuestra que los tiempos han cambiado: ya no es suficiente emitir alertas ni aferrarnos a modelos rígidos de análisis. En una situación de entorno marcado por la sobreabundancia de datos, la inmediatez de conocer la amenaza y la urgencia de informar al Alto Mando, la misión principal es transformar las alertas en inteligencia estratégica que le permita la mejor toma de decisiones. En este escenario, la Central de Inteligencia aparece como la respuesta institucional para enfrentar tales desafíos y consolidar un sistema vivo, dinámico y flexible.

La revolución digital y el auge del OSINT han creado un mar de información, donde muchos de los medios y plataformas digitales de información se encuentran presuntamente contaminados y mezcladas con puntos de vista y desinformación deliberada. En consecuencia, el valor de la inteligencia no reside en acumular todo lo disponible, sino en centrarse en el blanco, discriminar el ruido y direccionar al usuario información relevante. La Central de Inteligencia debe trabajar con filtros que organicen los datos de acuerdo con requerimientos prioritarios, como lo son los elementos esenciales de información. Solo de esta manera, el decisor evita perder tiempo en información irrelevante para recepcionar un producto de inteligencia claro, útil y oportuno.

Ni la fuente abierta ni la fuente cerrada, por sí solas, nos ofrecen un panorama completo. Mientras la primera aporta amplitud y rapidez, la segunda nos brinda profundidad, sensibilidad y valor agregado. Integrarlas no es una opción sino una condición estratégica; en otras palabras es la única vía para que la inteligencia pueda transformar alertas dispersas en inteligencia estratégica. El decisor no necesita conocer los insumos en cómo se alimenta una plataforma centrada en el objetivo, sino en contar con un producto multidinámico de inteligencia que le permita anticipar escenarios.

La IA procesa con rapidez, identifica patrones y clasifica insumos en segundos, pero no se le puede delegar la capacidad de interpretar y proyectar. La IA puede multiplicar las capacidades humanas, mas nunca reemplazar la competencia del analista. De ahí que la producción de inteligencia deba descansar en la complementariedad entre la máquina y la mente, donde la tecnología agiliza y el criterio del analista la interpreta. La Central de Inteligencia es un aporte importante establecido en la doctrina, por lo que debe garantizar que lo visualizado siempre

sea sometido al criterio del analista, quien aporta el contexto de la situación del entorno y con visión estratégica.

En un mundo donde lo único constante es el cambio, los sistemas rígidos están condenados al fracaso. Las amenazas mutan, las tecnologías se transforman y los escenarios se reconfiguran con gran velocidad. Por consiguiente, la Central de Inteligencia debe ser una capacidad que muestre la flexibilidad como principio organizacional, revisando periódicamente los supuestos de trabajo y permitiendo a los analistas ajustar evaluaciones a la luz de nueva evidencia.

La Central de Inteligencia representa el salto tangible que toda agencia de inteligencia necesita y que el propio sistema demanda en la elaboración de productos multinámicos de inteligencia. Su valor no está en ser un sistema pasivo, sino en funcionar como un sistema dinámico que discrimine el ruido, complemente al usuario, integre fuentes, aproveche la tecnología y se actualice en el tiempo.

Referencias

Betts, R. K. (2007). *Enemies of intelligence: Knowledge and power in American national security*. Columbia University Press. https://archive.org/details/enemiesofintelli0000bett

Cardozo Lozano, B. (2025). *De un ciclo rígido a un sistema colaborativo: Dinámica en la producción de Inteligencia Estratégica*. Revista de la Escuela Superior de Guerra Naval, 22(2), 76–89. https://doi.org/10.35628/resup.v16i2.166

Cardozo Lozano, B. (2024). BRACOLPER Ouro: Un pilar operativo en la seguridad amazónica. *Revista DEFENSA*, (diciembre), 50–53. https://www.defensa.com/revista-defensa/revista-defensa-edicion-diciembre-2024

Clark, R. M. (2019). *Intelligence analysis: A target-centric approach* (5.ª ed.). CQ Press.

Congreso de la República del Perú. (2012, 10 de diciembre). Decreto Legislativo N.° 1141, que regula el Sistema de Inteligencia Nacional (SINA) y la Dirección Nacional de Inteligencia (DINI). Diario Oficial *El Peruano*. https://busquedas.elperuano.pe.

Dirección Nacional de Inteligencia (DINI). (2021). *Doctrina de Inteligencia Nacional. Presidencia del Consejo de Ministros*.

DOCINT-21803 (2022). *Doctrina de Inteligencia de la Marina*. Marina de Guerra del Perú.

Heuer, R. J., & Pherson, R. H. (2010). *Structured analytic techniques for intelligence analysis*. CQ Press.

Kent, S. (1949). *Inteligencia estratégica para la política mundial estadounidense*. Princeton University Press.

Lowenthal, M. M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press. https://archive.org/details/intelligencefrom0000lowe_t8r9

Rid, T. (2016). *The rise of the machines: A cybernetic history*. W. W. Norton & Company.

Russell, S., & Norvig, P. (2010). *Inteligencia artificial: Un enfoque moderno* (3.ª ed.). Prentice Hall.

Sims, J. E. (2022). Transforming U.S. intelligence. Georgetown University Press.

Steele, R. D. (2002). *The new craft of intelligence: Personal, public, & political*. OSS International Press.

Sun Tzu. (2005). *El arte de la guerra* (L. Giles, Trad.). Ediciones Elaleph. (Trabajo original publicado ca. 500 a. C.)

Waltz, K. N. (1979). *Theory of International Politics*. McGraw-Hill.

Warner, M. (2009). *Intelligence as risk shifting*. En P. Gill, S. Marrin, & M. Phythian (Eds.), Intelligence theory: Key questions and debates (pp. 16-32). Routledge.

Zegart, A. (2022). *Spies, lies, and algorithms: The history and future of American intelligence*. Princeton University Press.

Año 2025, Vol. 22, Nº 3, pp. 86 - 93
DOI: https://doi.org/10.35628/resup.v16i2.175

Desafíos en el ejercicio del Comando y Control en Operaciones Navales aplicados en la Marina de Guerra del Perú

Challenges in the exercise of Command and Control in Naval Operations applied to the Peruvian Navy

Recibido: 13 de agosto del 2025| Aceptado: 05 de diciembre del 2025

Cristhian Castellares Pretell
https://orcid.org/0009-0009-7742-4809

Licenciado en Ciencias Marítimas Navales de la Escuela Naval del Perú. Licenciado en Economía Cuantitativa del United States Naval Academy. Es calificado en Submarinos y en Sistemas de Operaciones. Ha seguido los cursos Básico de Inteligencia y Básico de Estado Mayor en la Escuela Superior de Guerra Naval. Durante su servicio a bordo ha sido oficial de dotación del B.A.P. "BOLOGNESI", B.A.P. "UNIÓN", B.A.P. "ANGAMOS", B.A.P. "ARICA" y B.A.P. "CHIPANA". Actualmente se desempeña como Jefe del Departamento de Sistemas de Armas del B.A.P. "CHIPANA".

Email:castellares170930@gmail.com

Resumen: Este artículo analiza el empleo táctico de una fuerza naval, enfocándose en el Comando y Control (C2) en operaciones multidominio. Destaca la importancia de una estructura flexible para mejorar las Fuerzas de la Marina de Guerra del Perú (MGP). Describe la influencia de la interoperabilidad de plataformas en todo el espectro de las operaciones navales. Resalta la relevancia de las tácticas de guerra moderna y la capacidad de integración operativa para defender la soberanía y participar en operaciones multinacionales, apoyando a la política exterior.

Palabras clave: multidominio, comando, control, tactical data link, tácticas navales modernas, interoperabilidad, flexibilidad.

Abstract: *This article analyzes the tactical employment of a naval force, focusing on Command and Control (C2) in multidomain operations. It highlights the*

importance of a flexible structure in enhancing the Peruvian Navy forces. It describes the influence of platform interoperability across the full spectrum of naval operations. It underscores the relevance of modern warfare tactics and the operational integration capacity to defend sovereignty and participate in multinational operations, supporting foreign policy.

Keywords: *multidomain, command, control, tactical data link, modern naval tactics, interoperability, flexibility.*

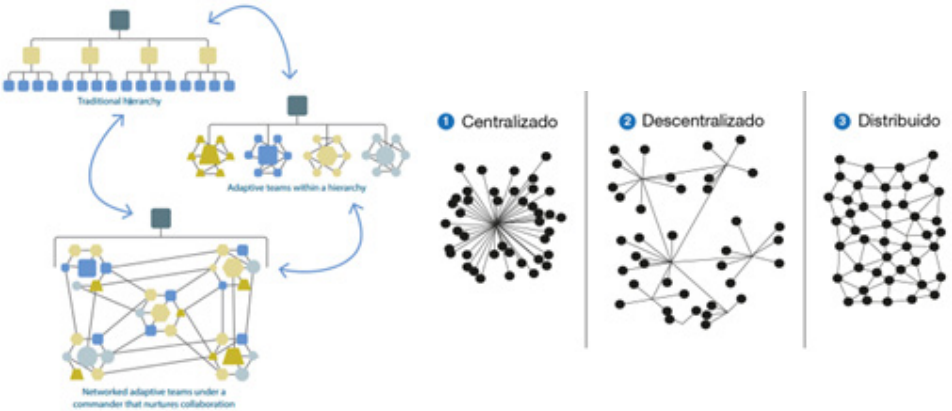
1. INTRODUCCIÓN

En las operaciones multidominio (MDO), que abarcan los ámbitos terrestre, marítimo, aéreo, ciberespacial, espacial y el espectro electromagnético, el Comando y Control (C2) es esencial para integrar fuerzas, reducir la fricción y la incertidumbre, y garantizar el cumplimiento de los objetivos en todos los niveles de la guerra (estratégico, operacional y táctico). El C2 permite dirigir y controlar medios, personal especializado e información, asegurando coherencia en el empleo del Poder Militar.

El factor principal del C2 es el Comandante. En todas las Marinas del mundo, es el comandante quien ejerce la autoridad legal de comando sobre sus subordinados, en virtud del grado o cargo (NATO Standardization Office, 2021). A su vez, el Manual de Planeamiento Naval Operativo, emplea el término de manera consistente con la idea de autoridad y responsabilidad para tomar decisiones y dirigir acciones; mientras que relacionamos el Control a la supervisión de las actividades, con el fin de asegurar el cumplimiento de los objetivos del Comando.

En tal sentido, el C2 se convierte en un proceso integrado que garantiza la unidad de esfuerzo, dirección centralizada y ejecución descentralizada dependiendo de la situación (Vego, 2020). Facilita la aplicación de una doctrina común y la interoperabilidad entre fuerzas. Se divide en dos enfoques: centralizado y descentralizado, destacándose este último por otorgar libertad de acción a los subordinados para tomar decisiones según la intención del comando, bajo el concepto de "comando por misión" (Vego, 2020). Asimismo, hoy en día, se considera también el C2 Distribuido, mediante el cual, la toma de decisiones y el control están distribuidos a través de varias entidades interconectadas que colaboran entre sí, como se aprecia en la figura 1.

FIGURA 1
Transición entre diferentes modelos de Comando y Control



Fuente:Nuevos desafíos en las Operaciones de Seguridad Marítima en relación al Ejercicio Multinacional UNITAS, Marco Mujica, p. 85

En la actualidad, se están desarrollando nuevos enfoques, desde C2 hasta C6ISR, donde los modelos jerárquicos están siendo reemplazados por estructuras flexibles que favorecen un flujo rápido de información y descentralizan la toma de decisiones, aplicando el concepto de "Mission Command[1]" en unidades tácticas con C2 distribuido, acelerando el "ciclo OODA[2]" y generando caos en el enemigo (Mujica, 2022).

2. DESARROLLO

Para lograr un comando y control eficaces, es esencial construir una estructura organizativa flexible y robusta, donde la interacción entre los diferentes niveles de comando sea fluida y adaptativa. En tal sentido, el núcleo de esta estructura radica en la relación de comando, que integra funciones como el Comando Operacional (OPCOM[3]), Control Operacional (OPCON[4]), Comando Táctico (TACOM[5]) y Control Táctico (TACON[6]), que permiten coordinar operaciones de manera

[1] Mission Command: Aplicado en la doctrina militar de EE.UU. Hace referencia a un enfoque de liderazgo donde el comandante transmite su intención de manera clara y sencilla otorgando a sus subordinados independencia de acción en la ejecución de su misión.

[2] Ciclo OODA (Observar, Orientar, Decidir, Actuar)

[3] OPCOM: Operational Command

[4] OPCON: Operational Control

[5] TACOM: Tactical Command

[6] TACON: Tactical Control

efectiva. A través del Comando Operacional (OPCOM), un Comandante tiene la autoridad para asignar misiones, desplegar unidades y tomar decisiones sobre el control operacional y táctico, adaptándose a las necesidades del entorno sin verse limitado por responsabilidades administrativas (NATO Standardization Office, 2021). Dentro de la relación de comando, existe la flexibilidad en delegar o retener el control para conducir operaciones específicas, coordinar tareas y mover unidades dentro de un teatro de operaciones, lo que asegura rapidez y precisión en las respuestas, conocido también como Control Operacional (OPCON) (Vego, 2017).

Este enfoque flexible es crucial para mantener la eficiencia en un escenario dinámico y con alto nivel de incertidumbre, como el de la Fuerza de Submarinos de la Marina de Guerra del Perú (MGP). A pesar de que las unidades submarinas participan en ejercicios multinacionales (UNITAS o SIFOREX) e integran una organización de tarea, la Autoridad Operacional de Submarinos (SUBOPAUTH[7]) ejerce el Control Operacional (OPCON) sobre estas unidades, teniendo a su cargo la planificación, dirección y coordinación de las operaciones submarinas.

Esta misma flexibilidad se aplica en el contexto de operaciones anfibias, donde se designa un Comandante de la Fuerza Anfibia (CFA), responsable del cumplimiento de la misión. El Comando Operacional Marítimo (COMA), permite la comunicación, transmisión de órdenes e interacción entre el CFA y el Jefe del Comando Conjunto de las Fuerzas Armadas (JCCFFAA), facilitando la coordinación en el nivel estratégico operacional. La Fuerza Anfibia se compone de una Fuerza de Tarea Anfibia (CFTA) y una Fuerza de Desembarco (CFD). Según la organización de tarea, el COMA ejerce el Comando Operacional (OPCOM), y el CFA el Comando Táctico (TACOM), compartiendo el Control Operacional (OPCON). A su vez, el Control Táctico (TACON) será ejercido por el CFTA y el CFD, mediante el concepto de comandos paralelos[8] (coordinación efectiva y apoyo mutuo).

Asimismo, en operaciones tácticas, como las de búsqueda y rescate, se implementa el concepto de "Cambio de Control Operacional" (CHOP[9]), lo que ilustra aún más la adaptabilidad de la estructura de comando. Este proceso permite que el COMA mantenga su autoridad sobre las unidades aeronavales; sin embargo, delega el Control Operacional a la Comandancia de Operaciones

[7] SUBOPAUTH: Submarine Operational Authority

[8] Comandos Paralelos: Organización y estructura de un sistema en el que múltiples unidades o comandos operan simultáneamente, pero de manera independiente entre sí, aunque bajo una coordinación general, para lograr una mayor eficiencia y rapidez en la toma de decisiones y la ejecución de operaciones.

[9] CHOP: Change of Operational Control (MTP-01 Volume I, 2021)

Guardacostas (COMOPERGUARD) para garantizar una respuesta más eficiente y dirigida a las circunstancias del momento. Esta flexibilidad no solo facilita la toma de decisiones en tiempo real, sino también resalta su capacidad para adaptarse a las diversas situaciones operativas, cumpliendo con uno de los roles estratégicos de la MGP: ejercer la Autoridad Marítima, que incluye la seguridad de la vida humana en el ámbito acuático.

En tal sentido, en función a los nuevos desafíos que se presentan a las diversas fuerzas armadas del mundo, se puede comprender cómo el éxito de una estructura de comando depende de la implementación de sistemas C2, que permiten planear, dirigir y controlar operaciones con información oportuna en todos los niveles. Gracias al avance tecnológico de los sistemas de C2, a través de enlaces de datos tácticos (link 11, link 16 y link 22), se puede compartir datos en tiempo real, enviar y recibir órdenes tácticas y posiciones enemigas, así como mantener una imagen operacional común (COP[10]). Por ello, se implementó la plataforma de Comando y Control WIRACOCHA a nivel de Comando Conjunto, la cual representa un avance significativo en el intercambio táctico de información en el dominio marítimo. Su implementación ha sido clave para mejorar la coordinación y la eficiencia en la gestión de información, permitiendo una mejor toma de decisiones. La continua evolución del sistema WIRACOCHA ofrece un gran potencial para optimizar la rapidez en el rastreo del desplazamiento de las unidades amigas, enemigas y neutrales, así como el proceso crítico de identificación y clasificación.

Considerando el avance tecnológico en los sistemas C2, así como los desafíos actuales y futuros, el Alto Mando Naval ha reevaluado las bondades y capacidades con las que deben contar las nuevas plataformas a incorporar, con el fin de crear un poder naval capaz de actuar con éxito donde lo requieran los intereses nacionales, tal como lo describe la visión de la MGP. En su compromiso por fortalecer la seguridad nacional y proteger su extenso dominio marítimo, la institución busca ampliar sus capacidades para adaptarse a las amenazas globales, regionales y locales. Esta adaptación resulta esencial para responder de forma efectiva a los retos de hoy, donde lo único constante es el cambio. En

[10] COP: Common Operational Picture

este escenario, cada decisión inteligente debe tener en cuenta no solo la situación presente, sino también un futuro incierto, lo que nos impulsa a replantear lo que ya estaba definido (Mujica, 2025). Como señala Geoffrey Till (2013), las marinas de primer mundo buscan proyectar su poder hacia los océanos, promoviendo la interoperabilidad de plataformas en todo el espectro de las acciones y operaciones navales, enfatizándose en la cooperación internacional y respondiendo ante desastres, lo que refuerza su capacidad disuasiva y garantiza la soberanía nacional como se observa en la figura 2.

FIGURA 2

Espectro de las acciones y operaciones navales

Fuente: Seapower: A guide for the twenty-first century, Geoffrey Till, pág. 362.

De la Rocha (2022), indica que "el dominio marítimo se origina en las bases y estaciones de la costa y no en altamar, y protegiéndola adecuadamente se mantiene la operatividad de las Fuerzas de Tareas Navales". Por ello, como se mencionó anteriormente, la visión de la MGP destaca la importancia de contar con una fuerza naval capaz de realizar despliegues oceánicos, para disuadir amenazas que puedan poner en riesgo la soberanía del país. Siguiendo las teorías navales de Alfred Mahan (Naval Institute Press, 2015), que incluyen la estrategia

naval costera, oceánica y global, la MGP se orienta a integrar una estrategia naval flexible que, sin perder su enfoque regional, se adapte a las exigencias globales, alcanzando así una capacidad de proyección más allá del mar adyacente a sus costas como bien señala el artículo 54 de la Constitución Política del Perú de 1993 (Namihas, 2014), empleando Fuerzas Híbridas[11] con elementos de marinas primer orden ("Blue Waters Navy[12]") complementándose con unidades asimétricas, generando ciclos OODA acelerados y, por ende, decisiones más rápidas y precisas, aumentando las probabilidades de éxito en operaciones militares (Scharre, 2018).

La situación del país durante los últimos 20 años y los desafíos en las operaciones navales antes mencionados, orienta a considerar unidades navales tipo multirrol por dos motivos, de acuerdo con Suarez (2022): (1) su capacidad de participar en operaciones de la guerra naval compuesta; y (2) los nuevos escenarios y amenazas relacionados a las operaciones navales diferentes a la guerra (MOOTW[13]), tales como la respuesta a desastres naturales y ayuda humanitaria (HA/DR). Enfocándonos en las tácticas navales modernas, las fuerzas navales, comprendidas como las unidades de las fuerzas operativas, deberán contar con capacidad C4I (Comando, Control, Comunicaciones, Computadoras e Inteligencia), así como contar con un avanzado sistema Tactical Data Link para el intercambio de información (data digital) de importancia táctica.

Al considerar la Estrategia Naval, resulta clave abordar la Guerra de Litoral, donde el entorno costero impone mayores exigencias al Comando y Control (C2). Según Hughes et al. (2018), la complejidad aumenta por la concentración de unidades y la necesidad de una cooperación precisa para desestabilizar al adversario. Por ello, planificar operaciones en estas zonas demanda interoperabilidad efectiva y estructuras de comando flexibles. Estas capacidades deben responder con agilidad a amenazas cambiantes, fortaleciendo así la proyección operativa de la MGP en escenarios multidominio.

3. CONCLUSIONES

La Marina de Guerra del Perú se adapta y se moderniza para enfrentar amenazas futuras y fortalecer su proyección hacia los océanos. Un sistema eficaz

[11] Estructuras armadas adaptativas y ambiguas, diseñadas para operar en entornos multidominio usando una mezcla de medios convencionales, irregulares y tecnológicos (como IA, drones y ciberataques). (Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. WW Norton & Company).

[12] Blue Waters Navy: Marina con la capacidad de operar en aguas oceánicas profundas, permitiéndole proyectar poder a nivel global.

[13] MOOTW: Military Operations Other Than War

de Comando y Control (C2) es esencial para coordinar operaciones e integrar fuerzas multidominio. La estructura flexible y la tecnología avanzada, como los Tactical Data Links (TDL), mejoran la comunicación, la toma de decisiones y la eficiencia operativa.

Debe existir una simbiosis entre el factor humano en función a la toma de decisiones y el empleo idóneo de la tecnología dentro del sistema C2, teniendo una relevancia significativa mayor en su empleo en las operaciones navales.

Las fuerzas navales, con capacidades C4I y tecnologías innovadoras, mejorarán la capacidad operativa en aguas litorales y abiertas, enfrentando amenazas de guerra naval moderna y respondiendo a emergencias y desastres naturales.

Finalmente, el fortalecimiento de la interoperabilidad y la inversión en nuevas tecnologías son clave para enfrentar los retos estratégicos, garantizando la defensa de la soberanía e integridad territorial y participando activamente en operaciones multinacionales y de seguridad marítima, en apoyo a la política exterior.

Referencias

De la Rocha, H. (2022). Estrategia Naval 2050. *Revista de Marina*, 22(1), 102-107

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

Hughes Jr. et al (2018). *Fleet Tactics and Naval Operations Third Edition*

Namihas, S. (2014). La posición oficial del Perú en torno a las zonas marítimas de la CONVEMAR a partir del diferendo marítimo con Chile. *Revista de la Facultad de Derecho PUCP*, N° 73, 95-108).

Naval Institute Press (2015). *Mahan on naval strategy: selections from the writings of rear admiral Alfred Thayer Mahan. Annapolis*, Maryland.

MAPLO – 22516 (2014): *Manual de Planeamiento Naval Operativo*

MTP-01 Volume I (2021): *Multinational Maritime Tactical Instructions and Procedures*. Edition (H) Version (1). North Atlantic Treaty Organization

Mujica, M. (2022). Nuevos desafíos en las Operaciones de Seguridad Marítima en relación al Ejercicio Multinacional UNITAS. *Revista de Marina*, 22(1), 72-87

Mujica, M. (2025). Paradigmas de la guerra de minas navales, una guerra silenciosa y letal. *Revista de Marina*, 25(1), 76-85

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. WW Norton & Company.

Suarez, S. (2022). Buque Multirrol – Necesario reemplazo de nuestras Unidades de altamar. *Revista de Marina*, 22(3), 8-31

Vego, M. (2017). *Operational warfare at sea: theory and practice*. Routledge

Vego, M. (2020). *General naval tactics: theory and practice*. Naval Institute Press

Año 2025, Vol. 22, Nº 3, pp. 94- 114.
DOI: https://doi.org/10.35628/resup.v16i2.176

La guerra como fenómeno social: aportes desde la sociología y la inteligencia estratégica

War as a Social and Strategic Phenomenon: Contributions from Sociology and Strategic Intelligence

Recibido: 25 de septiembre de 2025 | Aceptado: 05 de diciembre de 2025

Jorge Montoya Ruibal
https://orcid.org/0009-0000-5995-4771
Egresado de la Escuela Naval del Perú; calificado en Guerra de Superficie. Se desempeñó en el área de operaciones en unidades de combate tipo Fragata Misilera. Fue Comandante del BAP Castilla, Oficial del Estado Mayor de la Comandancia de Operaciones de la Amazonía y dotación del Componente Naval del Comando Especial VRAE. Se desempeñó también como Comandante de la Flotilla de Unidades Fluviales de la Amazonía.
Email:jorgeluismontoya77@gmail.com

Resumen: En el presente artículo se analiza la guerra como fenómeno social desde una perspectiva funcionalista, integrando la tesis de Gastón Bouthoul para lograr una comprensión más profunda. También se cita a Carl von Clausewitz, haciendo énfasis en la vinculación que siempre existirá entre la política y la voluntad de lucha de la población para iniciar y sostener una guerra. Con Kenneth N. Waltz se hace referencia solo al primer nivel de análisis de su tesis sobre las causas de la guerra, con el fin de vincular el comportamiento humano de los líderes políticos con el sistema social del Estado; es decir, cómo la sociedad influye en el sistema político y viceversa. Luego, se cita a Frederick H. Hartman a fin de resaltar que la guerra es una característica del sistema internacional. La reflexión más importante en Hartman es que la guerra puede aparecer de manera sorpresiva; uno solo se da cuenta cuando un Estado ya atacó a otro. Es así que se recurre a la inteligencia estratégica con la finalidad de valorar su competencia, importancia y

rol en el conocimiento de las ciencias sociales, para estar en capacidad de prever amenazas y considerar que esta solo será útil si el Estado cuenta con la capacidad permanente de vigilar el comportamiento del sistema social y el liderazgo político de Estados competidores, para anticipar la guerra y tomar decisiones estratégicas de manera oportuna. Finalmente, desde la teoría sociológica, se argumenta y analiza lo anteriormente señalado, citando a Emile Durkheim y Talcott Parsons y proponiendo que la teoría del sistema social de Parsons, utilizada para analizar fenómenos sociales, también es aplicable al estudio del fenómeno de la guerra.

Palabras Clave: guerra como fenómeno social, causas de la guerra, inteligencia estratégica.

Abstract: *This article analyzes war as a social phenomenon from a functionalist perspective, integrating Gaston Bouthoul's thesis for a deeper understanding. It also cites Carl von Clausewitz to emphasize the enduring link between politics and the population's will to fight, both essential for initiating and sustaining a war. Kenneth N. Waltz is referenced only regarding the first level of analysis of his thesis on the causes of war, in order to connect the human behavior of political leaders with the State's social system, that is, how society influences the political system and vice versa. Frederick H. Hartman is then cited to highlight that war is a characteristic of the international system. Hartman's most important insight is that war can erupt unexpectedly; one becomes aware of it only when a State has already attacked another. Thus, the article turns to strategic intelligence to assess its competence, importance, and role within the social sciences, to enable anticipation of threats. Such intelligence will only be useful if the State has the permanent capacity to monitor the behavior of the social system and the political leadership of competing States, in order to anticipate war and make timely strategic decisions. Finally, the article argues and analyzes the points outlined above from a sociological perspective, citing Émile Durkheim and Talcott Parsons, and proposes that Parsons' social system theory, intended for the analysis of social phenomena, is also applicable to the study of war as a phenomenon.*

Keywords: *war as a social phenomenon, causes of war, strategic intelligence.*

1. INTRODUCCIÓN

La guerra es un fenómeno que integra a todos los esfuerzos del Estado para desarrollarla. Es sumamente violenta y no deseada por ningún ser humano en plena capacidad de sus facultades. Pero lamentable e históricamente, ha sido medio de resolución de controversias entre países, estando condicionada al comportamiento humano de los líderes y la voluntad de lucha de su población. Nunca estaremos a salvo de ella por completo; nos toca a los profesionales de la guerra, los miembros de las Fuerzas Armadas, conocer desde todas las perspectivas posibles sus causas y efectos. Desde la inteligencia estratégica debemos poder anticipar su advenimiento y de llegar el momento de desarrollarla, haber contado con la información suficiente para que en el nivel político se hayan tomado las mejores decisiones en tiempo de paz; y si la guerra es inevitable, ser conscientes que debemos ser tan violentos como lo permitan nuestras unidades de combate y sus comandantes, esto porque es nuestra tarea defender a nuestra patria y a nuestros conciudadanos. Nuestro sentido de protección a los nuestros es sumamente elevado y, por esto mismo, lo es también nuestra preocupación por el estudio de este fenómeno. Tradicionalmente la guerra ha sido estudiada desde la perspectiva militar, sobre la conducción y el empleo de los medios en combate en los niveles táctico, operacional y estratégico militar. Por ello, en el presente artículo se presentarán algunas ideas y propuestas sobre cómo conocer más a profundidad el fenómeno de la guerra, esta vez desde una perspectiva sociológica.

Gaston Bouthoul propuso estudiar la guerra científicamente, como un fenómeno social específico. En esta línea, autores de las relaciones internacionales como Frederick H. Hartmann y Kenneth N. Waltz, coincidieron en que la guerra es una característica persistente del sistema internacional, que debe comprenderse en sus causas profundas para poder aspirar a reducir su surgimiento.

Este artículo integra estas perspectivas clásicas de la guerra, con el enfoque de la inteligencia estratégica, siguiendo a Sherman Kent y Washington Platt. La inteligencia estratégica cumple una función de alarma temprana, analizando el comportamiento de los liderazgos políticos y de las sociedades como sistemas. Finalmente, se incorporan teorías sociológicas, el concepto de hecho social de Émile Durkheim y el modelo funcional AGIL de Talcott Parsons, para entender la guerra como una función social más del sistema. Estas teorías ofrecen un marco para analizar la guerra que, aplicada desde la inteligencia estratégica, permite mejorar la capacidad de anticipar y advertirlas al identificar factores sociales subyacentes.

El artículo combina, principalmente, teorías sobre la sociología de la guerra y de la inteligencia estratégica, para ofrecer una comprensión de la guerra como fenómeno social y estratégico, y explorar cómo dicha comprensión puede ayudar a anticipar conflictos armados.

2. DEFINICIONES CLÁSICAS DE LA GUERRA

LA GUERRA SEGÚN CLAUSEWITZ

Carl von Clausewitz (2005/1832) estudió detalladamente el fenómeno de la guerra en su obra "De la guerra". Ella está descrita en el contexto de la acción propiamente dicha, de la ejecución de la guerra, no en el contexto de sus causas como fenómeno, sino únicamente con un enfoque militar. Su definición yace en ilustrar el poder de la violencia para someter al enemigo a voluntad:

> La guerra no es más que un combate singular ampliado. Si queremos pensar en el sinnúmero de combates singulares en los que consiste como en una unidad, haremos mejor en imaginar a dos combatientes. Cada uno trata de forzar al otro, empleando la violencia física, a obedecer su voluntad; su fin más inmediato es derrotar al contrario y hacerle de ese modo incapaz de cualquier resistencia ulterior. (p. 17)

Si bien es cierto la guerra se lleva a cabo por decisiones políticas, estas no surgirían si no se cuenta con la voluntad de lucha de la población; esta voluntad es motivada por ciertas causas que responderán a la conciencia colectiva creada en un devenir de acontecimientos previos:

Si las guerras entre los pueblos civilizados son mucho menos crueles y destructivas que las que se producen entre no civilizados, ello se debe a las circunstancias sociales, tanto a las de los Estados en sí como entre sí. De esas circunstancias y sus relaciones surge la guerra, por ellas se ve condicionada, y, en consecuencia, su violencia se determina por ellas. No forman parte de ella, sólo la limitan, moderándola; pero eso no significa que pueda establecerse un principio de moderación en la filosofía de la guerra misma sin cometer un absurdo. (p. 19)

Clausewitz deja en claro que la guerra está vinculada a la política porque es una herramienta subordinada a ella. El sistema político es el que define los objetivos nacionales, mientras que la guerra es un medio para alcanzarlos. La conducción de la guerra no es un fin en sí mismo, sino un instrumento cuya razón de ser depende de los fines políticos que lo originan:

- Vemos pues que la guerra no es sólo un acto político, sino un verdadero instrumento político, una continuación del tráfico político, una ejecución

> del mismo por otros medios. Lo que sigue siendo peculiar de la guerra se refiere tan sólo a la naturaleza singular de sus medios. El arte militar en su conjunto, y el general al mando en cada caso concreto, pueden exigir que las direcciones e intenciones de la política no entren en contradicción con esos medios, y probablemente esa pretensión no sea pequeña; pero, por mucho que influya en algún caso sobre las intenciones políticas, siempre habrá de pensarse tan solo como una modificación de estas, porque la intención política es el fin, la guerra el medio, y nunca puede pensarse en el medio sin el fin. (p. 31)

La conducción de la guerra implica un diálogo constante entre las necesidades operativas y las intenciones políticas. La conducción de la guerra puede exigir ajustes para que las órdenes políticas sean viables dentro de las condiciones reales del combate. Por ello la importancia de comprender la guerra analizando la interacción dinámica entre el poder político y el arte militar, pues es en esa relación donde se determina el rumbo y la intensidad del conflicto.

LA GUERRA SEGÚN BOUTHOUL: CONCEPTUALIZACIÓN DE LA POLEMOLOGÍA

Gaston Bouthoul (1971) afirma que "de entre todos los fenómenos sociales, la guerra es, sin discusión, el más violentamente espectacular" (p.14). En su libro "El fenómeno Guerra" hace varias explicaciones desde una perspectiva sociológica, y la describe como un fenómeno social, prácticamente natural en las sociedades.

También comenta que las guerras han dado vida a la historia, ya que ellas tienden a ser los puntos de referencia para su estudio. Él no se refiere a la guerra desde la perspectiva militar, sino a cómo en las escuelas de las fuerzas armadas se enseña como una técnica o arte, para organizar los ejércitos, sus tácticas y estrategias para el mejor empleo de los medios de combate. En cambio, el objetivo de Bouthoul era crear un capítulo más en la sociología, que estudie la guerra, preocupado por su estudio como fenómeno. Aquel señaló: "si quieres la paz conoce la guerra" (p. 27).

Bouthoul propone el estudio científico de las guerras como cualquier otro fenómeno social, por lo que afirma que el estudio de las guerras debe estar en el campo de la sociología. Él sustenta esto en varios puntos.

El primero es que la guerra está interiorizada en nosotros al ser parte de la historia, es punto de referencia de nuestros cursos de historia en el currículo escolar y está presente en el paisaje en que nos desarrollamos, como lo son los monumentos a los héroes, nombres de avenidas, calles, parques, etc.

En segundo lugar, Bouthoul señala que la guerra depende de la voluntad del hombre; es decir, forma parte de las posibilidades en su agencia. Al ser esto así, es importante determinar cuándo la motivación de un grupo humano hace que este sea agresivo en algún momento dado. También es importante analizar cómo influye la sociedad sobre el grupo en ese mismo sentido.

Bouthoul señala que las guerras presentan varios aspectos a la vez, por ser un fenómeno muy amplio. Afirma que todas las guerras son políticas (porque en ellas desempeñan un papel los gobiernos), económicas, demográficas (porque elevan las estadísticas de mortalidad) y religiosas (porque es un factor que está contenido en la guerra al entrar en juego creencias, dogmas y principios). En su conceptualización de la guerra hace una analogía anatómica comparándola a una enfermedad y señala que no se puede curar una enfermedad sin conocer sus causas. Por ello, él incentiva a usar la polemología como método o ciencia para conocer la guerra. También diferencia entre guerra y otras formas de lucha, considerando que existen formas de lucha que pueden ser desarrolladas contra adversarios inconscientes o cosas inertes. En cambio, la guerra sí considera un enemigo con voluntad y conciencia, y tiene como fin la destrucción contra su adversario.

Bouthoul describe los rasgos principales que permiten limitar el fenómeno guerra, señalando que: "su trazo más notorio es su carácter de fenómeno colectivo. En este sentido la guerra debe ser claramente diferenciada y separada de los actos violentos individuales" (p. 44). Esta afirmación hace énfasis sobre la característica colectiva que tiene la guerra.

Bouthoul detalla su argumento de la siguiente manera:

> Hemos de tomar en consideración dos elementos: De un lado la naturaleza del grupo, es decir precisamente la colectividad que combate, y de otro, el elemento subjetivo, o sea, esencialmente la faceta intencional o, dicho de otro modo, las finalidades, que persiguen los autores de una guerra. (p. 44).

En este párrafo, el autor empareja el factor de la finalidad de la guerra con la naturaleza de los grupos que entran en combate, lo que muestra la importancia de reconocer las características esenciales que los define como grupos diferentes. Se constituyen mediante su identidad colectiva, involucrando su dinámica, cómo se forman, evolucionan, cohesionan o fragmentan.

Bouthoul describe los rasgos que, según él, son principales para un estudio metódico de las guerras y los enumera en ocho directrices:

1. Descripción de los hechos materiales: Se refiere a describir los acontecimientos y comportamientos vistos desde el exterior, respondiendo las siguientes preguntas. ¿En qué difiere el estado de guerra del de paz? ¿En qué consiste el material guerrero y la manera de servirse del mismo? ¿Cuáles son las características, la formación, el reclutamiento y la organización de los grupos armados en campaña y sus maneras de actuar antes del combate, durante este y después del mismo?
2. Descripción de los comportamientos psíquicos: se analizan las motivaciones y explicaciones de los actores, desde los jefes de Estado hasta los soldados; se debe estudiar la intencionalidad, es decir, las razones que los combatientes declaran para justificar su participación.
3. Primer grado de explicación: Se basa en interpretar un conflicto en particular; los historiadores y analistas deben buscar las causas ocasionales e inmediatas de una guerra, explicando cómo se relacionan los hechos entre sí.
4. Segundo grado de explicación: En este nivel se examinan las doctrinas y teorías generales sobre la guerra, se intenta dar un sentido universal al fenómeno.
5. Elección y reagrupación de hechos: El investigador selecciona, compara y clasifica hechos, agrupando aquellos que muestran analogías y divergencias en diferentes sociedades. También se consideran las formas de justificación de la guerra.
6. Hipótesis sobre las funciones: La guerra debe ser analizada como un fenómeno social que cumple funciones específicas; su concepto principal es analizar el papel que desempeña en la historia de la sociedad. Destruye estructuras sociales, refuerza otras y genera un nuevo tipo de organización social. Por ejemplo, redistribuye poblaciones, cambia jerarquías políticas, transforma economías o acelera procesos de cambio social.
7. Hipótesis sobre periodicidad de las guerras: Las guerras pueden ser comparadas con las crisis económicas, ya que ambas aparecen con un carácter cíclico marcado por intervalos de recurrencia variables y reconocibles.

8. Tipología de las sociedades y de las guerras: El último paso consiste en establecer una clasificación que relacione los tipos de guerras con los tipos de sociedades. Bouthoul advierte, sin embargo, que esta tarea es compleja, pues los criterios técnicos, políticos, demográficos o culturales se interponen y modifican entre sí, lo que hace difícil formular una tipología rigurosa. Aún así, considera indispensable avanzar en ese esfuerzo comparativo (p. 34).

Bouthoul señala sobre la guerra y sus efectos demográficos:

> La esencia misma del fenómeno es el homicidio organizado, y convertido en lícito. Pues la guerra, désele el nombre que se le dé, es una lucha sangrienta entre grupos organizados. Sin homicidio no hay guerra. Así pues, todas las guerras presentan efectos demográficos, porque acrecientan la mortalidad. Por consiguiente, podemos postular que, entre todos los factores, el demográfico, por ser el que alimenta la guerra en combatientes y en víctimas, tiene una importancia muy particular. (p. 109)

En ese sentido, la función demográfica de la guerra es la única de las funciones sociales que es constante y por consiguiente la más relevante; la estructura demográfica es clave para determinar los gatilladores de algún conflicto. Precisa también que, sin duda y lamentablemente, la guerra es una función social. Hace la analogía con la fisiología, que conoce otras funciones penosas como la muerte, la vejez, las enfermedades, y que pese a ello, no se va a dejar de investigar. Por el contrario, solo si se es consciente del gran daño que esto causa es posible estudiar los fenómenos y se puede llegar a combatirlos, atenuarlos, por no suprimirlos.

LA GUERRA SEGÚN WALTZ: INTERDEPENDENCIA ENTRE SUJETO-SISTEMA

Kenneth Waltz (2013/2007) señala en la introducción de su libro "El hombre, el Estado y la guerra" que cuestionar quién ganó una guerra equivale a preguntar quién salió victorioso en un terremoto, lo cual enfatiza la inutilidad de hablar de vencedores en medio de una catástrofe. A lo largo del siglo XX se fue consolidando la convicción de que en los conflictos armados no existen victorias auténticas, sino únicamente distintos niveles de derrota. De ahí Waltz presenta una interrogante central: ¿Es posible reducir la recurrencia de las guerras y ampliar las posibilidades de la paz? ¿Podremos aspirar a un futuro más pacífico que nuestro pasado? Posteriormente precisa que, para explicar cómo la paz puede alcanzarse con mayor facilidad, es indispensable analizar primero las causas profundas que originan la guerra. Waltz, partiendo desde la perspectiva de las

relaciones internacionales, muestra su preocupación por conocer las causas de la guerra.

Inspirado por Rousseau, señala:

> La naturaleza misma del comportamiento humano, que muchos han tomado como una causa, es en gran parte, de acuerdo con Rousseau, un producto de la sociedad en la que vive. Y la sociedad, asegura, es inseparable de la organización política. (p. 6)

En esta cita, Waltz vincula el sistema social con el sistema político; él resalta su interdependencia y de acuerdo con ello es importante vigilar la influencia que tiene un sistema en el otro. El comportamiento humano es de igual importancia como factor paralelo a tomar en cuenta. En este contexto, se constituye como un actor dentro del sistema social, que también genera influencia en el comportamiento del sistema, recíproca e interdependientemente. Es decir, el comportamiento de un individuo puede influir en el comportamiento de un sistema social, como el sistema social influye en el individuo. Ello también sería aplicable al análisis de los líderes políticos, que influyen en la población, pero a su vez son influidos por el sistema social.

Waltz continúa desglosando su conceptualización de la siguiente manera:

> De acuerdo con la primera imagen de las relaciones internacionales, las causas importantes de la guerra se encuentran en la naturaleza y el comportamiento del hombre. Las guerras son el resultado del egoísmo, de impulsos agresivos mal canalizados, de la estupidez. Otras causas son secundarias y deben interpretarse a la luz de estos factores. Si estas son las causas primarias de la guerra, entonces la eliminación de la guerra debe darse a través del mejoramiento y la ilustración de los hombres, o de asegurar su reajuste psicosocial. (p. 19)

Sintéticamente, Waltz propone que las causas más importantes de la guerra se encuentran en la naturaleza y el comportamiento humano, explayándose dicha importancia dentro del contexto del primer nivel de análisis de su libro. En ese sentido, los conflictos internacionales no se pueden entender solo en virtud de las causas externas de su surgimiento. Aunque la tesis de Waltz sea más extensa, en este texto nos centramos solo al primer nivel de análisis de su libro.

LA GUERRA SEGÚN HARTMANN: CARACTERÍSTICA PERSISTENTE EN EL SISTEMA INTERNACIONAL

Frederick Hartmann (1986) desarrolla la guerra desde la perspectiva de las relaciones internacionales:

> Por más desagradable que sea, la guerra continúa siendo una característica del sistema de Estados; por eso debemos tratar de comprender el papel que desempeña. Debemos examinar sus causas, su desarrollo y sus rasgos contemporáneos, y preguntarnos, en particular, de qué modo las armas nucleares han cambiado, o no, la naturaleza de uno de los problemas más antiguos de la humanidad. (p.165)

En esta cita, se afirma que la característica más importante del sistema internacional es la guerra; también plantea la reflexión sobre la importancia de investigar sus causas:

> Así como las víctimas de un asalto no eligen libremente que las roben, del mismo modo no todas las naciones que libran una guerra no lo hacen por puro deseo de guerrear. Si una nación es atacada, debe rendirse o luchar; al menos, es evidente desde el punto de vista de la lógica. Pero, si bien las naciones atacadas casi nunca lo son nominal y que la nación agredida no esté totalmente libre de culpa, en el nivel más elemental podemos llegar a la conclusión de que las guerras estallan porque una nación soberana decide atacar a otra. Y pero ¿por qué la ataca? (p.165)

La guerra entre Estados se desarrolla de manera sorpresiva, se inicia cuando ya un Estado atacó al otro; para prevenir ello se requiere de un sistema de Inteligencia, que anticipe estas acciones, monitoreando las dinámicas internas de los Estados competidores. Este debe estudiar, por ejemplo, el sistema social, el sistema político, el comportamiento humano de los líderes políticos y otros factores. Entre otras cosas, también en lo descrito anteriormente queda siempre la tarea de intentar responder la pregunta citada: ¿por qué un Estado atacaría a otro?

3. EL ROL DE LA INTELIGENCIA ESTRATÉGICA EN LA COMPRENSIÓN DE LA GUERRA EMPLEANDO LAS CIENCIAS SOCIALES

Washington Platt (1983) se enfoca en el conocimiento que se debe tener sobre Estados competidores. La orientación de la inteligencia estratégica es producir inteligencia, para que todos los sectores del Estado que correspondan dicten las directivas y tomen las acciones correspondientes relacionadas a la seguridad nacional. Por consiguiente, la producción de inteligencia estratégica debe ser insumo para el diseño de las políticas nacionales:

> La Inteligencia Estratégica es el conocimiento referido a las capacidades, vulnerabilidades y probables cursos de acción de las naciones extranjeras. Se dirige principalmente para guiar la formulación y ejecución de las medidas de seguridad nacional en la paz y en la guerra; la conducción de operaciones militares en tiempo de guerra, así como para el desarrollo de la planificación estratégica para el período de postguerra. (p.20)

La Inteligencia Estratégica no debe tener límites en cuanto a producir la información necesaria para salvaguardar la seguridad nacional. Quien la dirige debe contar con amplia experiencia en el campo, para que sea eficiente y tenga los enfoques necesarios. Esta actividad está muy estrechamente ligada al conocimiento del poder nacional, la política exterior, las relaciones entre Estados, la diplomacia, el derecho internacional, la economía internacional y la guerra, entre otras:

> La "Guerra Total" ha hecho necesaria la "Inteligencia Total" o, en otras palabras, la "Inteligencia Estratégica". Para resumir la amplia naturaleza de la Inteligencia Estratégica podemos empezar con el bien conocido lema de Terencio: "Homo sum, humani nihil a me alienum puto", que puede traducirse como "Yo soy un hombre: nada que pertenezca a los seres humanos está fuera de mis intereses". Esto puede ser parafraseado así: "Yo soy un hombre de la Inteligencia Estratégica: nada de lo que pertenezca a las actividades humanas extranjeras está fuera de mis intereses". (p.21)

Platt presenta esta pregunta y se responde:

> ¿Por qué un especialista en inteligencia debe leer ampliamente sobre ciencias sociales? Primero, porque las ciencias sociales tratan con las actividades humanas en grupos; precisamente, actividades que son sumamente importantes para inteligencia. Segundo, porque muchos de los problemas, conceptos y métodos de las ciencias sociales pueden tomarse prestados y adaptarse a los problemas de inteligencia. La lectura sobre ciencias sociales da amplitud y perspectiva a nuestra comprensión sobre los problemas de inteligencia, ofreciendo ejemplos, analogías y contrastes. (p.176)

Con esta pregunta y respuesta Platt clarifica, desde la perspectiva de la Inteligencia, la importancia del conocimiento de las ciencias sociales para comprender los problemas de Inteligencia. Las teorías de las ciencias sociales permiten ver la realidad de los sistemas sociales y políticos de manera más clara, nos permite comprender las dinámicas sociales, y poder determinar el porqué de los comportamientos, tanto de los individuos como los de la sociedad.

Sherman Kent (1994) señala en el capítulo cinco de su libro, la Inteligencia en cuanto a su organización y enfatiza en el concepto del espíritu de sus tareas en ese aspecto, precisando lo siguiente:

> La inteligencia constituye una institución; es una organización física de seres vivos que persigue, como fin, una clase especial de conocimiento. Una organización semejante debe hallarse preparada para poner a los países extranjeros bajo vigilancia u observación y debe estar preparada para explicar sus pasados, su presente y probables futuros. Debe tener la seguridad de que lo que produzca en el sentido de información sobre esos países, sea útil a la gente que toma las decisiones, es decir, que sea apropiado para sus problemas, que sea completo, seguro y oportuno. Se desprende que tal organización debe poseer un equipo de diestros expertos que al mismo tiempo conozca cuáles son los problemas estratégicos y la política exterior, y que dediquen su pericia profesional a la producción de una información útil sobre estos problemas. (p.85)

Sherman Kent (1994) señala que la información va variando constantemente, nada en el mundo permanece constantemente inmóvil, el analista de inteligencia debe ser consciente de eso, debe tener el conocimiento profundo de los temas para poder así detectar el cambio. Es así como precisa los siguiente:

Tal vez, el más importante de los fenómenos sociales que el elemento informativo debe vigilar es el de la población. Debe vigilarlo en todos sus aspectos: su aumento o disminución, sus promedios de crecimiento y disminución, los cambios en los grupos de edad, sus grupos de ocupación y sus grupos consumidores. Debe vigilar los cambios de distribución entre ciudad y campo, entre región y región. Debe tomar nota de las migraciones dentro del país y de las emigraciones y, hasta que el tiempo y la residencia permanente las afiance, debe mantener un ojo de águila sobre las personas desplazadas. Habrá también cambios en la estructura social que están íntimamente ligados a ciertas fases del cambio económico y que deben estar bajo constante observación. El elemento informativo de la inteligencia debe mantenerse al tanto de sus cambios en tamaño y estructura y, sobre todo, debe vigilar cómo se está organizando y bajo qué directivas para su lucha. (p.51)

Kent, da relevancia al conocimiento que se debe tener sobre la población de un Estado competidor, como lo es la dinámica del sistema social, tema importante para predecir comportamientos; con ello se puede analizar la capacidad del Estado en cuanto a la voluntad de lucha, por qué valores están dispuestos a integrarse y luchar. Se deben conocer cuáles son los valores compartidos en su sistema social, y la evolución de estos con el transcurrir del tiempo de acuerdo con las diferentes situaciones analizadas antes.

4. PERSPECTIVAS SOCIOLÓGICAS COMPLEMENTARIAS PARA LA POLEMOLOGÍA

El hecho social de Emile Durkheim

Emile Durkheim (1986/2001) definió el hecho social como aquellos modos de actuar, pensar y sentir que existen fuera de los individuos y que ejercen sobre ellos una influencia o coerción externa. En otras palabras, son fenómenos colectivos, como normas, costumbres o instituciones que trascienden al individuo y orientan o presionan su conducta. Los individuos las encuentran ya establecidas al nacer y, por lo general, las acatan o interiorizan sin cuestionarlas explícitamente. Durkheim sostenía que la sociología debe estudiar estos hechos sociales como "cosas", es decir, como realidades objetivas y externas al individuo, para entender cómo mantienen la cohesión y el orden social.

Durkheim señala que la definición de hecho social puede ser confirmada:

> Podemos confirmar mediante una experiencia característica esta definición del hecho social: basta observar la forma en que se educa a los niños. Cuando se observan los hechos tal como son y como han sido siempre, salta a la vista que toda educación consiste en un esfuerzo continuo por imponer al niño formas de ver, de sentir y de actuar a los cuales no llegaría espontáneamente. Desde los primeros momentos de su vida lo obligamos a comer, a beber, a dormir a horas regulares, lo coaccionamos a la limpieza, la tranquilidad, la obediencia; más tarde, lo obligamos a que aprenda a tener en cuenta al prójimo, a respetar los usos, las conveniencias, le imponemos el trabajo, etc. (p. 43)

Para Durkheim los hechos sociales existen porque cumplen una función en la sociedad. En el caso de la guerra, los argumentos de Bouthoul nos permite inferir que la guerra es un hecho social, puesto que, según él, la guerra cumple funciones sociales, precisando que la principal y esencial es la función demográfica.

La definición que Durkheim da al hecho social explicado líneas arriba nos permite identificar más fácilmente que la guerra sería una función social, tomando como ejemplo la educación del niño que Durkheim presenta. La educación infantil y la guerra ejemplifican cómo un mismo marco teórico de Durkheim, puede aplicarse a fenómenos tan dispares. La primera es constructiva, inculca la cohesión y los valores que mantienen la sociedad unida; la segunda es destructiva, operando casi como un mecanismo de reajuste extremo cuando fallan otras formas

de regulación social. Ambas, sin embargo, son producto de la vida colectiva y no pueden explicarse únicamente por las características de individuos aislados. Esta comparación subraya la riqueza del concepto de Durkheim: nos permite analizar un hecho tan trágico como una guerra entendiendo su origen sociológico y su función en el sistema social. De esa manera, podemos comprender la guerra como hecho social siguiendo a Bouthoul y nos ayuda a buscar soluciones colectivas que aborden sus causas y eviten que esa "función" violenta tenga que manifestarse en nuestras sociedades.

La conciencia colectiva de Emile Durkheim

Para Durkheim (1893/2007) la sociedad va a tener un rol fundamental en el individuo, el individuo es un resultado de la sociedad. Cuando los individuos empiezan a vivir en sociedad, generan un producto muy superior a la simple conciencia individual, a la que la llama conciencia colectiva, definiéndola de la siguiente manera:

El conjunto de las creencias y de los sentimientos comunes al término medio de los miembros de una misma sociedad, constituye un sistema determinado que tiene su vida propia, se le puede llamar la conciencia colectiva o común (p.89).

La psicología se encarga de estudiar la conciencia individual, la sociología se encarga de estudiar cuando el individuo vive en sociedad y un grupo de individuos generan un conjunto de ideas comunes producto de su interrelación; entonces, se construye una conciencia en sociedad, no es la sumatoria de las conciencias individuales. La sociedad va a producir un sistema de ideas, creencias, normas, valores y sentimientos que van a constituir la conciencia colectiva.

La conciencia colectiva son maneras de obrar, pensar y sentir, son representaciones sociales, que solamente tienen sentido en el razonamiento colectivo de la sociedad, muchas veces entran en conflicto con la conciencia individual. La única manera que tiene la conciencia colectiva para imponerse a la conciencia individual es la coerción (Durkheim, 1893/2007).

La conciencia colectiva le va a dar un marco de integración social a la persona, que supone el reconocimiento de que el individuo es parte de un grupo social, y crea identidad, un sentido de pertenencia, le da un sentido a la existencia de las personas individuales. La conciencia colectiva influye en la creación, entonces, de las organizaciones y grupos sociales, y a la sociedad.

La identidad nacional, por ejemplo, es en gran medida la expresión de una conciencia colectiva; los ciudadanos de un país se sienten vinculados por valores

que trascienden la individualidad, es así como Durkheim (1912/1982) lo explica de la siguiente manera:

> El soldado que muere por su bandera muere por su patria; pero, de hecho, en su conciencia, la idea de la bandera es la que ocupa un primer plano. Incluso ocurre que determina directamente la acción. Porque un estandarte aislado quede o no en mano de los enemigos, la patria no se perderá y, sin embargo, el soldado se hace matar por recuperarlo. Se pierde de vista que la bandera no es más que un signo, que no tiene valor por sí mismo, sino que tan sólo hace recordar la realidad que representa; se la trata como si fuera en sí misma esa realidad. (p. 207)

Teoría del sistema social de Talcott Parsons

Para George Ritzer (1993), Talcott Parsons constituye un representante del funcionalismo estructural, quien decía que la sociedad está formada por varios subsistemas que cumplen diferentes funciones. La economía se ocupa de la adaptación, porque a través del trabajo, la producción y la distribución ayuda a que la sociedad se ajuste al entorno y a que el entorno responda a sus necesidades. La política cumple la función de lograr metas, organizando personas y recursos para alcanzar objetivos colectivos; precisó también lo siguiente:

> Un sistema social reducido a los términos más simples consiste pues, en una pluralidad de actores individuales que interactúan entre sí en una situación que tiene, al menos. un aspecto físico o de medio ambiente, actores motivados por una tendencia a obtener un óptimo de gratificación y cuyas relaciones con sus situaciones incluyendo a los demás actores están mediadas y definidas por un sistema de símbolos culturalmente estructurados y compartidos. (p.119)

El sistema socializador, que incluye instituciones como la familia y la escuela, cumple la función de transmitir valores y normas culturales para que las personas los aprendan e interioricen. La integración corresponde a la comunidad social, como el derecho, que coordina y mantiene unidas a las distintas partes de la sociedad. Aunque todas estas estructuras son importantes, Parsons consideraba que el sistema cultural era el más relevante, al punto de definirse a sí mismo como un determinista cultural.

> Fernández Cardoso (2011) señala que, para Talcott Parsons, "la propiedad más importante de un sistema es la interdependencia de sus partes, la unidad más significativa es el actor en su relación con otros y el significado funcional que esto adquiere para el sistema. Al estar los valores extraídos del sistema cultural, son estos los que definen la organización sistémica". (p.12)

Parsons también propuso que todo sistema social debe satisfacer cuatro necesidades o imperativos funcionales para mantener su equilibrio y persistir en el tiempo (Camou, 2023). Estas cuatro funciones se resumen en el acrónimo AGIL (por sus siglas en inglés) las cuales se mencionan a continuación:

I. Adaptación (A): la capacidad del sistema para adaptarse a su entorno y asegurar los recursos necesarios. Implica las funciones económicas y de ajuste al medio ambiente, ya que el sistema debe extraer, distribuir y gestionar recursos materiales y energéticos para sobrevivir.

II. Logro de metas (G): la capacidad de definir objetivos colectivos y movilizar recursos para alcanzarlos. Corresponde a la función política o de dirección; el sistema social debe establecer metas, por ejemplo, seguridad, bienestar, expansión y tomar decisiones para lograrlas, articulando esfuerzos hacia esos fines.

III. Integración (I): la necesidad de coordinar y mantener la cohesión interna entre las partes del sistema. Esto abarca las instituciones normativas (leyes, valores compartidos, control social) que aseguran la solidaridad social y la cooperación entre individuos, evitando la disgregación.

IV. Latencia o mantenimiento de patrones (L): la función de preservar los patrones culturales y motivacionales fundamentales del sistema a lo largo del tiempo, la gestión de la tensión latente y la motivación para que los individuos cumplan sus roles. Esta función cultural garantiza la continuidad de las pautas normativas y la identidad colectiva del sistema social. (p.370)

5. ANÁLISIS DEL FENÓMENO GUERRA EMPLEANDO EL MARCO TEÓRICO DEL SISTEMA SOCIAL DE TALCOTT PARSONS

El marco conceptual de Parsons resulta aplicable para analizar el fenómeno de la guerra teóricamente, en términos de sus implicancias en las cuatro funciones AGIL de un sistema social. A continuación, se desarrolló qué funciones desempeña la guerra con respecto a la Adaptación, al Logro de Metas, a la Integración y a la Latencia del Sistema Social en que ocurre:

I. Función de adaptación al entorno (A): La guerra suele vincularse con problemas de adaptación al entorno, especialmente en términos de recursos y población. Cuando una sociedad enfrenta escasez de recursos o una sobredemografía que excede sus capacidades económicas, la guerra puede surgir como un trágico mecanismo de ajuste. Por otro lado, en línea con la tesis de Bouthoul, la guerra reduce la presión demográfica

consumiendo excedentes poblacionales y destruye parte de los recursos acumulados; paradójicamente readapta la proporción entre población y medios disponibles, cambiando la estructura demográfica y con eso el carácter y comportamiento de un sistema social. Bouthoul señalaba que poblaciones con mayor porcentaje de jóvenes eran más susceptibles al conflicto, es así como esto podría servir de indicador de posibles causas de conflictos.

Así, funcionalmente la guerra puede considerarse un mecanismo de adaptación del sistema social, también impulsa avances tecnológicos para sobrevivir, la evolución de la tecnología militar luego es aplicadas en el ámbito empresarial. Esta visión no implica que la guerra sea deseable, sino que desempeña de hecho una función adaptativa extrema cuando fallan soluciones pacíficas para equilibrar población, recursos y necesidades.

II. Función política de logro de metas colectivas: En términos de la función política del sistema social, la guerra se interpreta como un instrumento al servicio de objetivos colectivos, generalmente definidos por los Estados y sus líderes. Desde el modelo AGIL, una sociedad a través de su liderazgo político puede recurrir a la guerra con la expectativa de alcanzar metas que considera vitales, como asegurar la supervivencia del Estado. Se podría decir también que ciertas guerras han contribuido a preservar valores fundamentales de una sociedad, como la libertad y la soberanía, o alcanzar metas que la sociedad se había propuesto. La guerra puede entenderse como una respuesta extrema del sistema político para resolver conflictos y conseguir objetivos que no se pudieron lograr por otras vías. Aplicando el marco teórico de Parsons, podemos decir que la guerra refuerza temporalmente la capacidad del sistema político, al fortalecer la relevancia de la toma de decisiones en ese nivel, subordinando la economía y otros sistemas al esfuerzo de la guerra y orientando todo hacia la meta de vencer al enemigo.

III. Función de integración de las partes del sistema (I): Desde la perspectiva funcionalista, la guerra puede desempeñar un papel paradójico respecto a la cohesión interna de una sociedad. Por un lado, ante una amenaza externa, las sociedades tienden a experimentar un aumento de la solidaridad social, las diferencias internas se atenúan mientras los miembros se unen para enfrentar al enemigo común. La guerra, en este sentido, actúa como un factor integrador que refuerza la identidad colectiva y la lealtad al grupo, solidificando las fronteras del "nosotros" frente a un "ellos" externo.

Durkheim y otros autores han señalado cómo el conflicto externo puede generar efervescencia colectiva y fortalecer la moral grupal. Incluso símbolos colectivos como banderas, himnos, marchas, arengas, etc., cobran mayor importancia durante la guerra, unificando emocionalmente a la población y creando conciencia colectiva empleando valores compartidos; esto puede ser utilizado por líderes políticos, cuyo sistema social y su política interna se encuentra en crisis y requieren una integración del sistema social de su país para atenuar sus fracasos en política interna.

IV. Latencia / Mantenimiento de patrones (L): Finalmente, la guerra tiene profundas implicaciones en el plano cultural y de valores, que corresponden a la función de latencia o mantenimiento de patrones. Un sistema social en guerra adapta su cultura para sostener el esfuerzo bélico; se exaltan valores como el patriotismo, el sacrificio, el heroísmo y la disciplina, que sirven para motivar a los individuos a cumplir los roles exigidos a los miembros de las fuerzas armadas y a la población que participa en el conflicto. La guerra puede verse como un proceso de intensificación de la socialización en torno a ciertos valores clave para mantener la moral colectiva. Incluso tras el conflicto, las sociedades construyen narrativas históricas, días de recuerdo, monumentos, que incorporan la experiencia del combate, lo cual mantiene vivos patrones culturales de identidad y aprendizajes para generaciones futuras.

En conjunto, este análisis con el modelo AGIL nos muestra que la guerra es un fenómeno social que se puede analizar con las señaladas cuatro funciones sociales básicas. Con este enfoque queremos ayudarnos a entender qué rol funcional está jugando la guerra en la dinámica del sistema social. La guerra no tendría una única función, sino más de un efecto funcional: adaptativo, político, integrativo y cultural.

6. CONCLUSIONES

a. La guerra entre Estados se desarrolla de manera sorpresiva, se inicia cuando ya un Estado atacó al otro. Para prevenir esto se requiere de un Sistema de Inteligencia que anticipe estas acciones, monitoreando las dinámicas internas de los Estados competidores. Dichas dinámicas son producto de la interdependencia entre los líderes políticos y la población; cuando se inicia la guerra, la conducción de esta exige que el nivel político esté comprometido con el conocimiento de la capacidad militar, para que las órdenes

políticas sean viables dentro de las condiciones reales del combate. Por ello la importancia de comprender la guerra analizando la interacción dinámica entre el poder político y el arte militar, pues es en esa relación donde se determina el rumbo de su intensidad.

b. La guerra como fenómeno social, colectivo y voluntario involucra a grupos sociales que se organizan para ejercer la violencia de manera voluntaria. Surge de decisiones humanas conscientes que responden a motivaciones políticas, sociales, ideológicas o religiosas. La gran diferencia con otras formas de violencia es el carácter colectivo, lo que la distingue de la violencia individual. De ahí que sea indispensable estudiar las motivaciones colectivas y la psicología social de los grupos que deciden combatir o que son llevados a ello. La guerra debe estudiarse científicamente como cualquier otro fenómeno social; la polemología es la disciplina destinada a identificar causas, funciones y recurrencias de la guerra.

c. La guerra involucra, principalmente en su surgimiento, durante y después del conflicto, al sistema social, sistema político y sistema económico, los mismos que son interdependientes e influyen unos a los otros; por ello el seguimiento y el análisis de su dinámica y comportamiento, son factores sobre los que hay que analizar en los Estados competidores. Las guerras destruyen estructuras sociales, pero también refuerzan otras o generan nuevas formas de organización, reconfiguran la sociedad que la experimenta, redistribuye recursos y población. La clave está en no limitarse a describir las guerras desde una sola perspectiva, sino analizarla con profundidad para que sirva para comprenderla en su verdadera magnitud. La guerra nace de una necesidad del sistema social, por ello Bouthoul propone al fenómeno guerra como una función social, señalando que su principal función social es la demográfica; esto porque la estructura demográfica de un país, por edades, géneros, distribución geográfica, la dinámica migratoria y otros factores similares, influyen en la capacidad de un Estado en lo relativo a su Poder Nacional, directa e indirectamente antes, durante y después de una guerra.

d. El presente artículo, al aplicar el modelo AGIL de Talcott Parsons siguiendo siempre a Bouthoul, partiendo de que la guerra es una

función social, nos ha permitido apreciar cómo la guerra puede ser analizada como una función social, desde distintos ángulos teóricos. Por ejemplo, Parsons, mediante su propuesta AGIL, nos brinda un marco teórico para describir las varias funciones de guerra dentro del sistema social, adaptativas, políticas, integradoras y culturales. Eso mismo nos orienta hacia qué áreas funcionales de la guerra, desde la perspectiva sociológica, debemos enfocarnos en el análisis de Inteligencia Estratégica, con la finalidad de determinar cuáles se alteran o buscan restablecerse con esta y así poder prevenir la guerra, analizando la dinámica del comportamiento del sistema social, político, así como el sicológico del liderazgo político.

e. La Inteligencia Estratégica es crucial para anticipar la guerra, ya que proporciona un nexo entre la comprensión teórica de las causas sociales del conflicto y la anticipación de su surgimiento. Como señalan Kent y Platt, un analista de inteligencia estratégica debe integrar conocimientos de las ciencias sociales, para monitorear las dinámicas internas de las sociedades y prever posibles conflictos. Aplicar teorías sociológicas como herramienta de análisis en la inteligencia estratégica, aumenta la capacidad de alarma temprana, al permitir entender la guerra como una función social, lo que dota a los analistas de un marco para identificar factores estructurales que predisponen a un país al conflicto, y así anticipar y prevenir la guerra.

f. Es importante también identificar la conciencia colectiva que vincula a los ciudadanos de un país competidor, y por cuáles están dispuesto a luchar colectivamente; saber cuáles son sus creencias, normas, valores y sentimientos que la van a constituir. También, por lo tanto, saber cuáles son sus maneras de obrar, pensar y sentir, debemos analizar que los une. Un factor que es evidente es que si su supervivencia está en peligro van a luchar por ella, he ahí donde la escasez de recursos vinculado a la composición de la estructura demográfica de un Estado podría generar incertidumbre de su bienestar general en el futuro. El sistema social, político y el liderazgo, y su interdependencia, generarán comportamientos en los líderes políticos que se tendrán que vigilar con detenimiento.

Referencias

Bouthoul, G. (1971). El fenómeno guerra. Plaza & Janés. (Originalmente publicado en 1962)

Camou, A. (2023). Talcott Parsons: del estructural-funcionalismo al modelo AGIL. *En Cuestiones de teoría social contemporánea*. EDULP.

Fernández Cardoso, S. (2011). Teoría, sociedad y poder en Talcott Parsons, C. Wright Mills, Jurgen Habermas y Anthony Giddens [en línea]. Tesis de Doctorado, Universidad Católica Argentina, Facultad de Ciencias Sociales, Políticas y de la Comunicación

Clausewitz, C. (2005). *De la guerra*. Esfera Libros. (Originalmente publicado en 1832)

Durkheim, E. (1982). *Las formas elementales de la vida religiosa* (R. Ramos, traducción). Akal. (Originalmente publicado en 1912)

Durkheim, E. (2001). *Las reglas del método sociológico*. Cuadernos de la Gaceta, Fondo de Cultura Económica México. Fondo de Cultura Económica de México. (Originalmente publicado en 1986)

Durkheim, E. (2007). *La División del Trabajo Social* (C. Posada). Colofón. (Originalmente publicado en 1893)

Dirección Nacional de Inteligencia. (2021). *Doctrina de Inteligencia*. República del Perú.

Hartmann, F. H. (1986). *Las relaciones internacionales* (2.ª ed.). Fondo de Cultura Económica. (Originalmente publicado en 1983)

Kent, S. (1994). *Inteligencia estratégica: para la política mundial norteamericana* (5ª ed.). Pleamar.

Platt, W. (1983). *Producción de inteligencia estratégica: Principios básicos*. Editorial Struhart.

Ritzer, G. (1993). *Teoría sociológica contemporánea*. MCGRAW HILL.

Secretaría de Seguridad y Defensa Nacional (SEDENA). (2015). *Doctrina de seguridad y defensa nacional*.

Waltz, K. (2013). *El hombre, el Estado y la guerra: un análisis teórico*. Librería CIDE. (Originalmente publicado en 2007)

Año 2025, Vol. 22, Nº 3, pp. 115- 138.
DOI: https://doi.org/10.35628/resup.v16i2.177

Dominio marítimo del Perú, seguridad y gobernanza oceánica: evolución normativa, institucional y desafíos

Peruvian maritime domain, security and oceanic governance: normative, institutional evolution and challenges

Recibido: 25 de septiembre de 2025 | Aceptado: 05 de diciembre de 2025

Carlos E. Gamarra Elías
https://orcid.org/0009-0005-7685-9991
Vicealmirante de la Armada Peruana. Licenciando y Bachiller en Ciencias Navales, con especialización en el Instituto Hidrográfico de la Armada de España. Diplomado en Relaciones Internacionales por la Pontificia Universidad católica del Perú PUCP y Magister en Estrategia Marítima por la Escuela Superior de Guerra Naval. Ejerció el cargo de Comandante General de la Marina en el año 2008. Miembro de la Comisión Consultiva Ad-hoc del Ministerio de Relaciones Exteriores sobre Delimitación Marítima con Chile e Integrante del Equipo Peruano ante la Corte Internacional de Justicia de La Haya. Miembro del Consejo Consultivo de la Comandancia General de la Marina de Guerra. Miembro de Número y Presidente de la Comisión de Estudios Estratégicos del Instituto de Estudios Histórico-Marítimos del Perú IEHMP. Asesor de la Dirección General de Comunicaciones e Intereses Marítimos, y Representante Alterno de Defensa en la Comisión Multisectorial de la Acción del Estado en el Ámbito Marítimo (COMAEM).
Email:quicogamarraelias@gmail.com

Resumen: El mar ha sido motor histórico de desarrollo y seguridad para los Estados. En el caso peruano, se afirmó tempranamente derechos soberanos sobre sus recursos marinos hasta las 3 millas, alcance ampliado hasta las 200 millas marinas con el Decreto Supremo Nro. 781 de 1947; principios de soberanía y jurisdicción reforzados en la Declaración de Santiago (1952) y en su práctica normativa, anticipando principios que más tarde consolidaría la Convención de las Naciones Unidas sobre el Derecho del Mar (1982). Institucionalmente, la Marina de Guerra del Perú, por mandato constitucional, ejerce competencias y funciones vinculadas con la defensa, control y vigilancia del uso de los espacios de su dominio marítimo, así como la supervisión de las actividades que en este ámbito se realizan, para el fortalecimiento de los intereses marítimos nacionales, tareas que se cumple apoyados por instrumentos internacionales. Sin embargo, si bien el Perú no es Parte de la Convención de las Naciones Unidas sobre el

Derecho del Mar, ha reconocido formalmente ante la Corte Internacional de Justicia de La Haya, que "el término «dominio marítimo» empleado en nuestra constitución es aplicado de manera consistente con las zonas marítimas señaladas en la Convención de 1982 ... el Perú acepta y aplica las normas del derecho internacional del mar consuetudinario como están reflejadas en la Convención…" Este artículo complementa y actualiza el publicado por la Fundación Academia Diplomática del Perú: El Perú y la Convención del Mar, Balance y Perspectivas, primera edición mayo del 2023, con el título "Seguridad y Defensa en el marco de la Convemar".

Palabras Clave: Dominio Marítimo peruano, 200 millas, CONVEMAR, ZEE; Seguridad Marítima, OMI, DICAPI.

Abstract: *The sea has historically been a driving force for development and security for states. In the case of Peru, sovereign rights over its marine resources were asserted early on up to 3 miles, this was extended to 200 nautical miles with Supreme Decree No. 781 of 1947; principles of sovereignty and jurisdiction were reinforced in the Declaration of Santiago (1952) and in its regulatory practice, anticipating principles that would later be consolidated in the United Nations Convention on the Law of the Sea (1982). Institutionally, the Peruvian Navy, by constitutional mandate, exercises powers and functions related to the defense, control, and surveillance of the use of its maritime domain, as well as the supervision of activities carried out in this area to strengthen national maritime interests; tasks that are carried out with the support of international instruments. However, although Peru is not a party to the United Nations Convention on the Law of the Sea, it has formally recognized before the International Court of Justice in The Hague that "the term «maritime domain» used in our constitution is applied in a manner consistent with the maritime zones identified in the 1982 Convention... Peru accepts and applies the rules of customary international maritime law as reflected in the Convention..." This article complements and updates the article published by the Diplomatic Academy of Peru Foundation: Peru and the Convention on the Sea, Review and Perspectives, first edition May 2023, entitled "Security and Defense within the Framework of UNCLOS."*

Keywords: *Peruvian maritime domain, 200 miles, UNCLOS; EEZ, maritime safety, IMO, DICAPI.*

1. INTRODUCCIÓN

A través de la historia, los océanos y mares han gravitado profundamente en la vida de los pueblos, particularmente desde que el hombre aprendió a usarlos y disponer de los recursos que estos brindan. Con el correr del tiempo y con los avances científicos, dichas facilidades y recursos se han incrementado, hasta alcanzar en la actualidad un elevado nivel como impulsor para el desarrollo de las naciones, así como un elemento trascendental para garantizar su seguridad. (Política Nacional Marítima 2019-2030, 1. Antecedentes, 1.1 Presentación).

El poblador peruano tiene una especial vinculación con su mar, que representa más del 65% de su superficie continental, con una franja de costa de 3,080 km. de longitud. Este mar es la vía de acceso principal al intercambio del comercio marítimo internacional y contiene una enorme riqueza biológica, producto de características oceanográficas especiales que lo hace uno de los más ricos del planeta, y en su suelo y subsuelo se cuenta con potenciales recursos "no vivos", que no son aprovechados aún eficientemente.

Desde su surgimiento como Estados-Nación, los Gobiernos han realizado distintos intentos para garantizar el uso de estos espacios y el control de los recursos existentes en el mar adyacente a las costas en beneficio de su población. El Perú (Decreto Supremo Nro. 781, 1947), fue de los primeros países en proclamar la necesidad de ampliar el ámbito de su jurisdicción sobre su mar hasta las 200 millas marinas, con la finalidad de protegerlo, controlar sus recursos y preservarlos para las futuras generaciones, frente a las acciones que realizaban las flotas balleneras extrajeras que se aventuraban frente a las costas del Pacífico Oriental para la pesca y la caza de cetáceo, recursos que por entonces se creían inagotables.

Esta posición de defensa de los recursos del mar fue sustentada y reiterada ante la comunidad internacional, al suscribir junto con Chile y Ecuador, la "Declaración de Santiago en 1952", - instrumento que se constituyó en un valioso insumo para el lineamiento de la gobernanza de los mares, considerando que a esa fecha las Naciones Unidas aún no contaban con una postura clara sobre la determinación de exigencias y códigos en las distintas zonas marítimas; posición reiterada en los Acuerdos y Convenios adoptados en las Conferencias de Lima de 1954 y en las sucesivas conferencias internacionales en las que el Perú participó a lo largo del siglo XX, individual y regionalmente, en defensa de los derechos de los Estados sobre el mar.

En todos esos ámbitos, el Perú invocó principios jurídicos, geopolíticos, biológicos y económicos de las riquezas marinas, sosteniendo la necesidad de su

defensa, protección y preservación para sus nacionales, por ser de importancia vital para su seguridad alimentaria; precisado siempre que estos derechos soberanos no afectaban la libertad de navegación, conforme lo establece el derecho internacional.

Estos principios de derechos soberanos del Estado sobre el mar adyacente a nuestras costas, se vieron finalmente reflejados en la legislación internacional con la aprobación de la Convención de las Naciones Unidas sobre el Derecho del Mar (CONVEMAR), firmada en Montego Bay, Jamaica, en 1982 y en vigor desde 1994.

Esos principios, a los que debemos adicionar los de seguridad, se ven reafirmados con la aprobación de la Política Nacional Marítima 2019-2030 PNM (Decreto Supremo N° 012-2017-DE), que es el marco estratégico para promover el uso racional y sostenible del mar; integrando las actividades económicas, sociales y ambientales e impulsando la conciencia y prosperidad marítima del país. La PNM destaca las características del mar peruano como fuente de alimentación y medio de desarrollo socio económico del país, resaltando su ubicación geográfica en el nuevo escenario geopolítico del Océano Pacífico, como pivote y centro estratégico para el tráfico marítimo internacional.

2. EVOLUCIÓN DE LA ACCIÓN DEL ESTADO EN EL MAR

Desde los albores de la humanidad, el mar ha sido utilizado como fuente de provisión para la alimentación de sus pueblos y como vía principal de transporte y comunicación. La gran cantidad de recursos de los océanos y el dominio sobre su uso y aprovechamiento, generó tensiones entre las naciones, que ejercieron muchas veces por la fuerza sus reivindicaciones sobre los espacios marítimos adyacente a sus territorios, por lo que, en el tiempo, se fue construyendo en el contexto internacional un ordenamiento jurídico para su regulación. Desde el concepto de "Mare Nostrum" del imperio romano hasta nuestros tiempos, se procuró la búsqueda de consensos internacionales que regulasen los derechos de soberanía y jurisdicción de los países ribereños, consolidado el Derecho del Mar en el marco del derecho internacional.

El Derecho del Mar ha sido utilizado, tanto durante épocas de guerras mediante aplicación de bloqueos y presencia de flotas de guerra, como en tiempo de paz, buscando solucionar controversias referidas a los intereses de las flotas mercantes, y principalmente la presencia de flotas pesqueras extranjeras frente a sus costas.

En el caso del Perú, debemos precisar que, a pocos años de la declaración de la independencia ya se emitía una norma (Decreto Supremo N° 14, 1833)

que consideraba que la pesca en las costas e islas de la República debía hacerse exclusivamente por ciudadanos del Perú; ello, motivado por la presencia de "buques extranjeros invadiendo la propiedad y privando por la fuerza a lo naturales del país que se emplean en ella"; decretándose:

- Art. 1. Queda prohibida absolutamente a los extranjeros la pesca de cetáceos y anfibios en las playas e islas del Perú.
- Art. 2. Los capitanes de buques extranjeros que contraviniesen a esta disposición serán tenidos por contrabandistas.
- Art. 3 Los capitanes de puerto darán permiso a los ciudadanos del Perú para este ejercicio, con conocimiento de la autoridad superior del departamento, comandante general de marina, y jefes de aduanas de la costa
- Art. 4 Cualquier buque nacional que se encuentre en las inmediaciones de las costas e islas sin los documentos legales que acrediten el permiso, podrán ser detenidos como sospechoso en cualquier puerto de la república sin que tengan derecho a reclamar por ello daños y perjuicios.

Esta acción del Estado peruano, para protección de los recursos del mar, fue mantenida en las décadas sucesivas, pese a que entonces no existían consensos respecto de la extensión del mar territorial sobre el cual ejercían jurisdicción los Estados. Con la aprobación del "Reglamento de visita y permanencia de los buques y aeronaves de guerra extranjeros en los puertos y aguas territoriales del Perú en tiempo de paz" (Decreto Supremo Nro. 13, 1934), se fija "la extensión de las aguas territoriales del Perú en tres millas de las costas, contadas a partir de la línea de más baja marea". El concepto de mar territorial se incorpora en nuestro Código Civil recién en 1936, que en su art. 822 señaló: "Bienes del Estado. Son del Estado 1. Los bienes de uso público. 2. El mar territorial y sus playas y la zona anexa que señala la ley de la materia". Cabe precisar que, en dicho Código Civil, no se indica cuál era la extensión del mar territorial.

Con la aprobación del Reglamento de Capitanías y de la Marina Mercante Nacional (1940), se establecían las competencias de las Capitanías de Puerto con relación a las funciones de la Policía Marítima y en especial, sobre el control de la pesca; pero no se consideraron entonces regulaciones sobre la represión de actividades ilícitas. Sin embargo, se reitera que: "Las aguas territoriales se extienden hasta tres millas de las Costas e Islas, a partir del límite de las más bajas mareas".

En 1947, con Decreto Supremo N° 781 del 1 de agosto, el Perú proclamó ante la comunidad internacional, su soberanía y jurisdicción sobre un mar de 200 millas marinas, así como sobre el suelo, el subsuelo y todos los recursos vivos y no vivos

que se encuentren en su "dominio marítimo", con el fin de protegerlos y conservarlos para el sustento y desarrollo de su población. Consecuentemente, poco después se emite el Reglamento de Capitanías y Marina Mercante del año 1951 que, con base a estos derechos de soberanía y jurisdicción, regula aspectos referidos a la policía marítima y la pesca: se prohibía "a las embarcaciones extranjeras el ejercicio de la pesca en aguas peruanas" ... "la infracción por este artículo traerá consigo la aprehensión de la embarcación, de sus pertrechos de pesca y cargamento, como contrabando, y será penado con arreglo a las disposiciones que rigen la materia".

En 1952 se celebró en la ciudad de Santiago de Chile, la Primera Conferencia de Explotación y Conservación de las Riquezas Marítimas del Pacífico Sur, cuyo objetivo fue analizar la problemática relacionada con la explotación y conservación de las riquezas marítimas del Océano Pacífico Sur; cita en la que participaron delegaciones de Chile, Ecuador y el Perú, con el objeto de coordinar acciones para impedir la explotación de flotas extranjeras de los recursos marinos de esta parte del Pacifico, que pusieran en peligro la existencia, integridad, conservación y desarrollo principalmente de la fauna y la flora marina, recursos económicos que se consideraron vitales para cada país. La conferencia culminó con la emisión de la "Declaración de Santiago de 1952", a la vez que se generó un organismo regional al que pocos años después se sumó Colombia: la Comisión Permanente del Pacífico Sur.

En 1954, a dos años de esta declaración, en circunstancias que no existían aún normas del Derecho Internacional que regulasen la extensión de los espacios a las que esas Zonas Marítimas aludían, el Gobierno peruano tuvo que enfrentarse a poderosos intereses económicos internacionales y con participación de unidades de la Armada Peruana, se capturó un grupo de embarcaciones balleneras que faenaban dentro de nuestro dominio marítimo.

La flota del griego Aristóteles Onassis, compuesta de 16 barcos, había partido del puerto de Kiel (Alemania) enarbolando banderas panameñas. Pese a las advertencias emitidas por el Gobierno del Perú por vía diplomática, los armadores anunciaron su disposición a cazar ballenas frente a las costas occidentales de Sud América, señalando que sólo respetarían el límite tradicional de 3 millas que correspondería a cada país.

Un grupo de estas embarcaciones fueron localizadas por buques de la Armada Peruana a 110 millas de la costa "cazando ballenas en número de 2,500 a 3,000", por lo que cumpliendo instrucciones del Gobierno, el 17 de noviembre de 1954, aproximadamente a 115 millas al oeste de Punta Aguja, se capturaron al "Olympic Factory" y al "Olympic Lightning"; al "Olympic Fighting" y al

"Olympic Conqueror" se les detuvo cerca de las 200 millas frente a las costas de Paita. Al día siguiente, se apresó al buque madrina "Olympic Challenger", en cuyas bodegas se hallaron 6,800 toneladas de aceite de ballena. En el "Olimpic Splendor", otro buque madrina que huyó y no pudo ser capturado, en su descarga en Panamá, manifestó la cantidad de 5,000 toneladas de aceite de ballena.

Al armador Onassis se le impuso una multa de USD 3 millones, que fue aceptada y pagada, según consta en la Sumaria realizada por el Capitán de Puerto de Paita. Se les aplicó el Decreto Supremo Nº 781 del 1° agosto 1947, que se armoniza con la Declaración de Zona Marítima del 18 agosto de 1952, y el Reglamento de Capitanías y Marina Mercante Nacional aprobado por Decreto Supremo Nro. 21 del 31 octubre de 1951:

"Que, en las aguas territoriales solamente pueden cazar y pescar los peruanos y extranjeros domiciliados en la república, conforme lo dispone el art. 731;

"la caza de las ballenas, así como el aprovechamiento industrial de sus productos está reservado a los ciudadanos nacionales y a los extranjeros domiciliados en el Perú." art. 740.

"Toda persona o empresa que pretenda ejercer la industria de la pesca o de la caza marina, ya sea costera o de altura, solicitará permiso al Supremo Gobierno", art. 764°

En diciembre de ese mismo año, los representantes del Perú, Ecuador y Chile se reunieron en Lima, para la suscripción de varios convenios vinculados con el ejercicio soberano de sus derechos sobre los recursos del mar, entre estos, el "Convenio sobre medidas de vigilancia y control de las Zonas Marítimas de los Países Signatarios" de fecha 4 de diciembre de 1954, que estableció en entre otros compromisos:

PRIMERO

Corresponde a cada país signatario efectuar la vigilancia y control de la explotación de las riquezas de su zona marítima, por conducto de los organismos y medios que considere necesarios.

SEGUNDO

La vigilancia y control a que se refiere el artículo primero, sólo podrán ser ejercitados por cada país dentro de las aguas de su jurisdicción. Sin embargo, sus naves o aeronaves podrán ingresar a la zona marítima de otro país signatario, sin necesidad de autorización especial, cuando dicho país solicite expresamente su cooperación.

TERCERO

Las naves o aeronaves de los países signatarios estarán obligadas a enviar a la autoridad que cada país señale, toda la información posible acerca de la situación, identificación y faena de los barcos de pesca y caza que avisten en el curso de su derrota. Las telecomunicaciones que se efectúen con este fin estarán libres de portes, tasas e impuestos. Cada país reglamentará la forma de operar para el cumplimiento de estas disposiciones.

……

Todo lo establecido en el presente Convenio se entenderá ser parte integrante, complementaria y que no deroga las resoluciones y acuerdos adoptados en la Conferencia sobre Explotación y Conservación de las Riquezas Marítimas del Pacífico Sur, celebrada en Santiago de Chile, en agosto de 1952.

En 1958, buscando codificar el Derecho Internacional del Mar, que tenía un carácter esencialmente consuetudinario, se celebró la I Conferencia de las Naciones Unidas sobre el Derecho del Mar, en Ginebra, Suiza; aprobándose 4 Convenciones: Mar Territorial y Zona Contigua, Alta Mar, Plataforma Continental, y Pesca y Conservación de Recursos Vivos en Alta Mar; sin embargo, no hubo consenso en cuanto a la extensión de estos espacios.

La II Conferencia de las Naciones Unidas sobre el Derecho del Mar se celebró también en Ginebra en 1960, donde tampoco se alcanzaron acuerdos sobre la anchura del mar territorial y sobre la jurisdicción para derechos de pesca.

El año 1969, considerando su misión constitucional y mandato de la Ley Orgánica de la Marina, se crea el Cuerpo de Capitanías y Guardacostas (Decreto Ley No. 17824) , como Cuerpo Auxiliar de la Marina de Guerra del Perú, bajo la autoridad del Director General de Capitanías, con la finalidad de ejercer las funciones de Policía Marítima, Fluvial, Lacustre y Pesquera; de control y vigilancia del litoral, del tráfico acuático en las aguas jurisdiccionales; de seguridad y vigilancia de los puertos, así como el control y protección de los recursos y riquezas naturales, de acuerdo a lo establecido en el Decreto Supremo Nro. 781 del 01 de Agosto de 1947, en la declaración sobre Zona Marítima y en los Convenios Internacionales suscritos para esos fines, y en general de toda actividad que se desarrolle en el ámbito acuático.

A partir de 1973 y hasta abril de 1982, en el seno de la Organización de las Naciones Unidas, se desarrolló la III Conferencia del Mar, foro en el que se armonizaron las diversas posiciones sobre los derechos de los Estados respecto del uso y aprovechamiento sostenible del mar adyacente a sus costas y la extensión de estos espacios. Las sesiones culminaron con la aprobación de la Convención

del Derecho del Mar, que recoge los principios por los que Chile, Ecuador y Perú lucharon por décadas para ampliar su soberanía y jurisdicción hasta las 200 millas marinas, con la finalidad de cautelar y preservar sus recursos, ejercer sus derechos soberanos para la exploración, explotación y administración, tanto de los recursos vivos como no los no vivos, así como facultades jurisdiccionales para su protección y conservación.

La Convención de las Naciones Unidas sobre el Derecho del Mar (CONVEMAR), en vigor desde 1994, establece un régimen integral de ley y orden en los océanos y mares del mundo, con reglas que rigen todos los usos de los océanos y de sus recursos. Incorpora en un sólo instrumento las reglas tradicionales y, al mismo tiempo, introduce nuevos conceptos, regímenes jurídicos y aborda otras preocupaciones.

La CONVEMAR trata sobre los espacios oceánicos, los derechos de navegación, la paz y la seguridad en los océanos, la conservación y gestión de los recursos marinos, la protección y preservación del medio marino, la investigación científica, las actividades en los fondos marinos más allá de los límites de las jurisdiccionales nacionales y la solución de controversias entre Estados.

Si bien nuestro país no es parte de la CONVEMAR, muchas de las normas recopiladas en esta Convención son normas imperativas de derecho internacional y otras, por su aceptación universal y constituirse en costumbre internacional por la práctica resultante del comportamiento de los Estados (derecho internacional consuetudinario), son ya parte del Derecho del Mar Consuetudinario y obliga a todos los Estados, independientemente que sean o no parte de la CONVEMAR.

La CONVEMAR reconoce prácticamente los mismos derechos de soberanía y jurisdicción sobre el dominio marítimo, sobre el suelo y el subsuelo establecido por Perú con el Decreto Supremo de 1947 y la Declaración de Santiago de 1952, con la sola limitación del derecho de sobrevuelo de terceros Estados, y de tendido de cables y de tuberías submarinas. No existe otro convenio internacional que ampare estos derechos, salvo esta Convención, de la cual el Perú no es parte.

Respecto de las libertades de sobrevuelo y de tendido de cables y tuberías submarinas, que marcan la diferencia entre el mar territorial y la zona económica exclusiva, estas son libertades consagradas por la costumbre internacional, por normas convencionales anteriores a la Convención del Derecho del Mar y que están perfectamente definidas en el derecho internacional y obligan a todos los Estados.

La CONVEMAR estableció nuevos espacios marítimos, acabando con las controversias que sólo existía "altamar" y "mar territorial", cuya extensión la fijaba unilateralmente cada Estado, y en esencia fija y aborda:

1. El respeto a la soberanía de todos los Estados.
2. El orden jurídico para mares y océanos:
   - □ establecimiento límites territoriales del mar a 12 millas de la costa.
   - □ establecimiento de zonas económicas exclusivas a 200 millas de la costa.
   - □ creación de normas para la extensión de los derechos en la plataforma continental a 350 millas de la costa.
3. La facilitación de la comunicación internacional.
4. Promueve los usos pacíficos de mares y océanos, creando mecanismos alternativos para la resolución de conflictos.
5. La utilización equitativa y eficiente de sus recursos, creando la Autoridad Internacional de los Fondos Marinos.
6. Promueve el estudio y protección y preservación del medio marino.
7. Tiene una especial preocupación por la conservación de los recursos vivos.

En julio de 1994, la Asamblea General de las Naciones Unidas aprobó el Acuerdo Relativo a la aplicación de la Parte XI de la CONVEMAR - que entró en vigor en noviembre de 1994 – y que está referido a los recursos del lecho marino y su subsuelo, más allá de los límites de la jurisdicción nacional, denominada "La Zona", que se declaran "Patrimonio Común de la Humanidad". Esta Parte XI establece la creación de la Autoridad Internacional de los Fondos Marinos, el organismo encargado de organizar y controlar la exploración y explotación de los recursos de La Zona.

En 1995, la Asamblea General de las Naciones Unidas adoptó el Acuerdo sobre aplicación de disposiciones de CONVEMAR relativas a la Conservación de las Poblaciones de Peces Transzonales y las Poblaciones de Peces Altamente Migratorios (conocido como Acuerdo de Nueva York), que entró en vigor el 11 diciembre 2001.

La CONVEMAR a la fecha ha sido ratificada por 168 Países y por 2 Estados libres asociados; la Aplicación de la Parte XI ha sido ratificada por 153 países. El Acuerdo de Nueva York de 1995, sobre poblaciones de peces transzonales y las poblaciones de peces altamente migratorios, ha sido ratificada por 94 países.

Como se ha comentado anteriormente, la importancia de la CONVEMAR radica en ser un instrumento codificador de principios consuetudinarios y normas convencionales; entendiéndose como principios consuetudinarios aquellas que,

por su origen, provienen de la costumbre internacional general y que cualquier Estado puede invocarlas, independientemente que sean parte o no de un tratado, pues obliga a todos los Estados del mundo a cumplirlas.

En el contencioso por la delimitación marítima con Chile, el Perú acudió el año 2008 ante la Corte Internacional de Justicia de La Haya (CIJ), organismo de las Naciones Unidas, solicitando que aplique la costumbre internacional general en materia de delimitación marítima. Chile por su parte, afirmó ante la CIJ que el dominio marítimo del Perú era contrario al Derecho Internacional.

El Agente del Perú, en representación del Gobierno, afirmó ante la Corte Internacional de Justicia, en la fase de alegatos orales, que el "dominio marítimo" del Perú es plenamente conforme a la costumbre internacional:

"Sr. Presidente, en nombre del Gobierno del Perú, deseo formalmente dejar constancia del compromiso del Perú con el moderno derecho del mar, como se encuentra reflejado en la Convención de las Naciones Unidas sobre el Derecho del Mar de 1982.

La Constitución del Perú de 1993, su derecho interno y la práctica del Perú se encuentran en plena conformidad con el derecho del mar contemporáneo.

El término «dominio marítimo» empleado en nuestra constitución es aplicado de manera consistente con las zonas marítimas señaladas en la Convención de 1982; la Constitución se refiere expresamente a la libertad de comunicación internacional.

En resumen, el Perú acepta y aplica las normas del derecho internacional del mar consuetudinario como están reflejadas en la Convención…"

La Corte Internacional de Justicia resolvió la controversia de los límites marítimos entre el Perú y Chile, aplicando la costumbre internacional. En su Fallo del 24 enero del 2014, en el punto 178 precisa los siguiente:

"Mientras que Chile ha suscrito y ratificado la CONVEMAR, el Perú no es parte de ese instrumento. Ambas Partes reivindican títulos marítimos de 200 millas marinas. Ninguna de las Partes reivindica una plataforma continental extendida en el área concernida en este caso. La reivindicación chilena consiste en un mar territorial de 12 millas marinas y una zona económica exclusiva y plataforma continental de 200 millas marinas de extensión desde la costa. El Perú reivindica un "dominio marítimo" de 200 millas marinas. El Agente del Perú declaró formalmente en representación de su Gobierno que "[e]l término 'dominio marítimo' que utiliza [la] Constitución [del Perú] es aplicado de manera consistente con las zonas marítimas establecidas en la Convención de 1982".

La Corte toma nota de esta declaración, que expresa un compromiso formal del Perú."

3. EL CONCEPTO DE SEGURIDAD

Un asunto para considerar es conocer cuál ha sido la posición del Perú en la búsqueda de consensos en foros internacionales, respecto del entendimiento del concepto seguridad dentro de los procesos de integración que se propiciaron a inicios de siglo, para generar la confianza y reducir las tensiones en las relaciones internacionales, de manera de contribuir a consolidar la paz y la seguridad regional y hemisférica.

La seguridad es un concepto universal y natural que ha demostrado su existencia y vigencia en todos los pueblos, en todas las épocas, así como en todas las filosofías sociales y políticas, cualquiera que sea su grado de evolución y cultura. La seguridad implica una percepción de la situación, que debe ser de tal naturaleza que permita a las personas satisfacer sus necesidades, tanto de orden material como espiritual y esto es posible solamente dentro de un sistema en el que el Estado impone el orden.

A inicios del presente siglo, se comenzó a discutir en foros internacionales la existencia de otros aspectos a incorporar dentro del concepto de seguridad; las denominadas "nuevas amenazas" que afectaban el orden, entre otras, debido a los cambios de la política internacional; el incremento de fenómenos étnicos, tribales, culturales y religiosos; el narcotráfico y el terrorismo; la irrupción de riesgos medio ambientales, entre otras más, que habían ido generado cambios sustanciales en el enfoque teórico mundial en campo de la seguridad.

La Novena Política de Estado del Acuerdo Nacional, aprobada en el año 2002, refiere que la "Política de Seguridad Nacional" es un compromiso del Estado para que garantice la independencia, soberanía, integridad territorial y salvaguarda de los intereses nacionales. Este Foro propuso como política, un conjunto de previsiones y acciones que el Estado genera y ejecuta permanentemente para "Garantizar la soberanía, la independencia, la integridad territorial y la protección de los intereses nacionales".

En este contexto, el Perú propuso en el marco de la Organización de los Estados Americanos, el concepto de "seguridad para el bienestar", que sea aplicable en todo momento, como ingrediente del proceso de desarrollo sincrónico en la región. Una seguridad basada en la consolidación de la democracia; la participación y creación de oportunidades; elevación de la calidad de la educación en todos los niveles para fortalecimiento del capital social; la búsqueda de acuerdos en el tratamiento

y respeto por los derechos humanos; la extensión de los servicios sanitarios y alimentarios; y otros desafíos que asegurasen el bienestar de la población. Un concepto global de seguridad económica que contribuya a minimizar la extrema pobreza, causa profunda y generadora de situaciones subversivas e ingobernabilidad, con el deterioro del medio ambiente y degradación de los valores de la sociedad por el tráfico de drogas y otras fuentes de corrupción.

Muchos de los conceptos esgrimidos por el Perú, fueron recogidos en la "Declaración sobre Seguridad en las Américas", realizada en la Conferencia Especial de la Seguridad de la Organización de los Estados Americanos (OEA 2003 Ser.K/XXXVIII CES/dec.1/03 rev.), que reconoce:

> "Nuestra nueva concepción de la seguridad en el hemisferio es de alcance multidimensional, incluye las amenazas tradicionales y las nuevas amenazas, preocupaciones y otros desafíos a la seguridad de los Estados del Hemisferio; incorpora las prioridades de cada Estado, contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, y se basa en valores democráticos, el respeto, la promoción y defensa de los derechos humanos, la solidaridad, la cooperación y el respeto a la soberanía nacional.Las nuevas amenazas, preocupaciones y otros desafíos a la seguridad hemisférica son problemas intersectoriales que requieren respuestas de aspectos múltiples por parte de distintas organizaciones nacionales y, en algunos casos, asociaciones entre los gobiernos, el sector privado y la sociedad civil, todas actuando de forma apropiada conforme a las normas y principios democráticos y las normas constitucionales de cada Estado. Muchas de las nuevas amenazas, preocupaciones y otros desafíos a la seguridad hemisférica son de naturaleza transnacional y pueden requerir una cooperación hemisférica adecuada"

Es así como, en la Doctrina de Defensa peruana, se entiende como concepto de Seguridad Nacional (Libro Blanco de la Defensa Nacional 2005) "la situación en la cual el Estado tiene garantizada su independencia, su soberanía e integridad y, la población los derechos fundamentales establecidos en la Constitución. Esta situación contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, basada en los valores democráticos y en el respeto a los derechos humanos. Las nuevas amenazas y otros desafíos a la seguridad constituyen problemas complejos que requieren respuestas multisectoriales, complementadas por la sociedad civil, todos ellos actuando en su ámbito de responsabilidad de conformidad con el ordenamiento jurídico".

El Estado garantiza la Seguridad de la Nación mediante el Sistema de Seguridad y Defensa Nacional, que tiene por función preparar, ejercer y dirigir la Defensa Nacional en todos los campos de la actividad nacional.

4. LA SEGURIDAD EN EL ÁMBITO MARÍTIMO PERUANO

Hay usos indebidos del medio marítimo que puedan afectar la seguridad de los Estados, como por ejemplo, en el transporte y comercio marítimo; en el aprovechamiento indebido de sus recursos, por incumplimiento de normas que conllevan a la contaminación del ambiente y los ecosistemas; etc. De ahí que el concepto de seguridad marítima implica un abanico de acciones muy amplias para salvaguardar los recursos y el uso del ámbito marítimo peruano- conformado este por el dominio marítimo y sus aguas interiores- en los que se debe aplicar, en estricto cumplimiento y respeto, los mecanismos legales establecidos en las normas nacionales, así como con los que se asumen por compromisos internacionales y los aplicables al Estado peruano.

Si identificamos cuáles son los intereses nacionales en el mar, comprobaremos que estos están vinculados a los asuntos relacionados con el aprovechamiento de sus recursos y con el desarrollo de actividades en los campos político, social, económico, jurídico, científico, cultural y otros, que contribuyen con el logro del bienestar general y la seguridad e implican:

1. La conservación y el aprovechamiento de los recursos marinos renovables, y los no renovables. La investigación, desarrollo tecnológico e innovación en el campo de las ciencias del mar. El comercio marítimo, la marina mercante, puertos, cabotaje, aduanas, agencias marítimas, corredores logísticos, etc. La industria de construcciones y reparaciones navales.
2. Las actividades turísticas y recreativas vinculadas al mar, así como la conservación del medio marino y su biodiversidad, en lo referente a la protección, ecología, áreas protegidas, ordenamiento territorial y espacial, entre otros.
3. La identidad del poblador peruano y su vinculación con el medio marino para su uso y protección, así como la toma de conciencia para su desarrollo en actividades vinculadas con el mar.
4. Las relaciones con países de interés, y las que derivan del marco legal nacional e internacional, que determinan las reglas con las que el Estado debe accionar, con visión geopolítica, para orientar sus propias decisiones.
5. La presencia del Estado, promocionando las actividades que se desarrollan en el dominio marítimo, administrando y controlando estas actividades

> ejerciendo su soberanía y jurisdicción, de conformidad con la Constitución Política, la ley, los tratados internacionales de los que el Perú es parte, y otras normas y principios de derecho internacional aplicables a este, mediante el Poder Naval y el ejercicio de la Autoridad Marítima.

Le corresponde al Poder Naval, con empleo de las Fuerzas Navales Operativas, la vigilancia y defensa del dominio marítimo, de conformidad con la Ley y con los tratados ratificados por el Estado. Le corresponde a la Autoridad Marítima Nacional (Decreto Legislativo N° 1147), ejercer la administración marítima del Estado con la autonomía necesaria en el ámbito de su jurisdicción; aplicando y haciendo cumplir la normativa nacional, los instrumentos internacionales dé los que el Perú es parte, y otras normas de derecho internacional sobre la materia que puedan ser de aplicación al Estado peruano. Esto le permite actuar con el uso de la fuerza para la represión de actividades ilícitas, dentro de los lineamientos de los convenios internacionales sobre la materia.

El Perú es parte de la Organización Marítima Internacional (OMI), agencia especializada de las Naciones Unidas, creada por convenio de 1948 y que tiene como función principal establecer un marco eficaz para el transporte marítimo, con normas para la seguridad, contribuyendo al uso pacífico de los océanos, a la protección y la preservación del medio marino.

La OMI se ha convertido en el foro de temas tan diversos como búsqueda y salvamento, bienestar de la gente de mar, polizones, disposición de migrantes, refugiados y otras personas rescatadas en el mar; investigaciones de siniestros marítimos, lugares de refugio para naves y embarcaciones en peligro, tráfico ilícito de drogas por mar, sustancias psicotrópicas y precursores químicos; desguace de barcos, reciclaje y eliminación; responsabilidad por lesiones a pasajeros; remoción de naufragios, navegación polar e incluso proyectos de fertilización oceánica a gran escala diseñados para combatir el calentamiento global.

Es a través de la aplicación de varios instrumentos de la OMI, relacionados con el control de las actividades en el ámbito marítimo y la represión de actividades ilícitas, que se regula el grado en que los Estados pueden aplicar reglas y normas sobre la seguridad, protección, prevención de la contaminación, formación y titulación de la gente de mar, etc. , así como las actividades de supervisión mediante el control por el Estado Rector del Puerto, para garantizar que los buques extranjeros cumplan con las normas internacionales para:

- Protección de los Recursos Marinos
- Seguridad de la Vida Humana en el Mar

- Prevención y de la Contaminación Marina
- Represión de las Actividades Ilícitas

Todos los instrumentos de la OMI funcionan dentro del marco legal de la CONVEMAR. La OMI funciona como la "convención constitucional", que establece un marco legal para los Estados y las organizaciones internacionales competentes, de manera que permite que este marco evolucione y responda de una manera eficaz y flexible a los nuevos desafíos y desarrollos en el ámbito marítimo; como por ejemplo en temas vinculados con:

- Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Navegación Marítima, 1988.
- Protocolo para la Represión de Actos Ilícitos contra la Seguridad de las Plataformas Fijas emplazadas en la Plataforma Continental, 1988.
- Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas, 1988.
- Acuerdo para Promover el Cumplimiento de las Medidas Internacionales de Conservación y Ordenación por los Buques Pesqueros que Pescan en Alta Mar. (Conferencia de FAO, en 27º período de sesiones noviembre 1993).
- Acuerdo sobre Medidas del Estado Rector del Puerto destinadas a Prevenir, Desalentar y Eliminar la Pesca Ilegal, no Declarada y no Reglamentada, 2009,

En concordancia con todo lo anterior, el Artículo 56° de la CONVEMAR reconoce al Estado ribereño, jurisdicción para la protección y preservación del medio marino dentro de su zona económica exclusiva. En tal virtud, dicho Estado tiene el derecho de dictar sus propias leyes y reglamentos para:

- prevenir, reducir y controlar la contaminación procedente de fuentes terrestres (Art. 207, párrafo 1) y la producida por actividades en los fondos marinos sujetos a su jurisdicción (Art. 208 párrafo 1);
- • permitir, regular y controlar el vertimiento desde buques, aeronaves, plataformas y otras construcciones, o el hundimiento deliberado de los mismos (Art. 210, párrafo 5, según de la definición de vertimiento contenida en el Art.1 apartados a) y b);
- establecer leyes y reglamentos para prevenir, reducir y controlar la contaminación causada por buques, de conformidad con reglas internacionales generalmente aceptadas (Art. 211, párrafo 5) y para adoptar

otras medidas en áreas especiales, previa conformidad de la organización competente (Art. 211, párrafo 6);

- hacer cumplir sus leyes y reglamentos en los casos precitados; y el derecho de tomar medidas para proteger sus costas e intereses conexos en los casos de peligro de contaminación por accidentes marítimos (Art. 221, párrafo 1)

Este contexto jurídico internacional presenta situaciones que exigen nuevos roles y áreas de misión para las Armadas de los países. Mantener una estricta vigilancia de sus aguas jurisdiccionales, para enfrentar las amenazas reales y potenciales de actores foráneos que pretendan actuar en esos espacios sin el debido consentimiento del país ribereño. Al respecto, cabe mencionar que en noviembre del año 2004, el Gobierno peruano dispuso la ejecución de un gran operativo con participación de unidades navales de superficie, submarinas y aéreas que, apoyando al personal de la Autoridad Marítima Nacional (DICAPI), capturaron nueve embarcaciones de bandera china que realizaban actividades de pesca ilegal de calamar gigante y otras especies marinas, entre las 190 y 200 millas marinas de las costas de Huarmey, Ancash. En sus bodegas se encontraron más de 690 toneladas de pota.

6. LA LIBERTAD DE NAVEGACIÓN EN EL DOMINIO MARÍTIMO DE 200 MLLAS MARINAS Y LA SEGURIDAD

En cuanto a la libertad de navegación dentro de las 200 millas marinas, la CONVEMAR establece el paso inocente en el mar territorial y la libre navegación en la Zona Económica Exclusiva. Ambos conceptos concordantes con lo que se proclamó con el Decreto Supremo Nº 781 del 1 agosto 1947 (art. 4°), que estableció una zona marítima especial de 200 millas marinas sin afectar el derecho de libre navegación de las naves de todas las naciones, conforme al Derecho Internacional.

El Reglamento del D.L. Nº 1147 (Artículo 32.- Navegación en las aguas jurisdiccionales) precisa: "El Estado peruano respeta las libertades de comunicación internacional en materia de navegación de naves de bandera extranjera en las aguas jurisdiccionales peruanas, siempre que no se afecte la paz, el orden, la seguridad o los derechos e intereses nacionales, conforme a la Constitución Política del Perú, otras disposiciones de la legislación nacional, los instrumentos internacionales de los que el Perú es parte y demás normas de derecho internacional sobre la materia que puedan ser de aplicación al Estado peruano".

"La navegación en las aguas jurisdiccionales tiene que cumplir con las siguientes condiciones:

a) Las naves que naveguen en aguas jurisdiccionales peruanas en demanda de puerto nacional y aquellas que efectúen navegación de cabotaje, deben observar el rumbo y la velocidad contemplados en su plan de navegación, pudiendo variarlos, detenerse o fondear en caso de algún incidente normal de navegación o cuando se preste auxilio a personas, buques o aeronaves en peligro. Igual obligación tienen las naves que zarpen de puerto peruano en navegación de travesía.
b) Las aguas jurisdiccionales peruanas constituyen una zona de paz, en cuya virtud no pueden realizarse en estas ejercicios o maniobras militares de cualquier tipo sin el expreso consentimiento del Estado, ni tampoco pueden efectuarse actividades de navegación que atenten o puedan atentar contra la paz y su seguridad.
c) Los buques de guerra de bandera extranjera que naveguen en aguas jurisdiccionales peruanas deben cumplir con la normativa nacional y los instrumentos internacionales de los que el Perú es parte acerca de la Defensa Nacional, seguridad de la vida humana, protección del medio ambiente, sanidad y prevención de abordajes en el mar.
d) El tránsito por aguas jurisdiccionales peruanas de buques de bandera extranjera impulsados por energía nuclear o que transporten sustancias radioactivas requiere de notificación previa al Estado y de la autorización expresa de este con anterioridad a dicho tránsito".

En cuanto a represión de las actividades ilícitas contempladas en la CONVEMAR como el contrabando, la piratería, el narcotráfico, la pesca ilegal, la investigación científica marina sin el conocimiento del Estado; la captura de especies transzonales y altamente migratorias en la Alta Mar y la contaminación entre otras, la CONVEMAR fija muy claro las competencias que tienen los Estados para actuar en los espacios marítimos: mar territorial, zona contigua y zona económica exclusiva.

En el "mar territorial" hay soberanía plena de los Estados ribereños, que pueden dictar las leyes y reglamentos relativos al "paso inocente" por su "mar territorial"; sin embargo, los buques de todos los Estados gozan del derecho de "paso inocente" a través del mar territorial. El "paso es inocente" debe efectuarse con arreglo a la CONVEMAR y otras normas de derecho internacional, mientras no sea perjudicial para la paz, el buen orden o la seguridad del Estado ribereño, señalándose en el Art. 19° las diversas actividades que no están permitidas. El art. 20° indica que: "los submarinos y cualesquiera otros vehículos sumergibles deberán navegar en la superficie y enarbolar su pabellón".

En la "zona contigua", regulada convencionalmente tanto por el artículo 24° de la Convención de 1958 sobre mar territorial y zona contigua, como por el artículo 33° de la CONVEMAR, los Estados tienen competencias para "prevenir y sancionar las infracciones a sus leyes y reglamentos en materia aduanera, fiscal, de inmigración o sanitaria cometidas o que se puedan cometer en su territorio o en su mar territorial".

No obstante, en las últimas décadas, la práctica general de los Estados ha generado una nueva norma consuetudinaria, tal como lo demuestra el artículo 8° de la Convención sobre la Protección del Patrimonio Cultural Subacuático de 2001, que otorga competencias normativas y de ejecución a los Estados ribereños en materia de protección del patrimonio cultural subacuático situado en la Zona Contigua.

Una cuestión debatida respecto de las competencias del Estado ribereño en su "zona contigua"- considerando la práctica de ciertos Estados- es si estas incluyen el ejercicio de controles en materia de seguridad. Al este respecto, la Corte Internacional de Justiciade La Haya, ha declarado que aunque la práctica demuestra que algunos Estados incluyen en sus legislaciones disposiciones en ese sentido, tal "práctica" ha sido protestada por otros Estados. Al analizar la controversia entre Nicaragua y Colombia, la CIJ confirmó que "el decreto colombiano sobre zona contigua incluye competencias en materia de seguridad, lo que no está permitido por el Derecho internacional consuetudinario".

Respecto de las competencias en "la zona económica exclusiva", situada más allá del mar territorial y adyacente a éste, el Estado ribereño tiene:

a) "Derechos de soberanía para los fines de exploración y explotación, conservación y administración de los recursos naturales, tanto vivos como no vivos, de las aguas suprayacentes al lecho y del lecho y el subsuelo del mar, y con respecto a otras actividades con miras a la exploración y explotación económicas de la zona, tal como la producción de energía derivada del agua, de las corrientes y de los vientos;
b) Jurisdicción, con respecto a:
   i. El establecimiento y la utilización de islas artificiales, instalaciones y estructuras;
   ii. La investigación científica marina;
   iii. La protección y preservación del medio marino;
c) Otros derechos y deberes previstos en esta Convención."

En las zonas económicas exclusivas, "todos los Estados gozan de las libertades de navegación y sobrevuelo, y de tendido de cables y tuberías submarinas a que

se refiere el artículo 87, y de otros usos del mar internacionalmente legítimos relacionados con dichas libertades, tales como los vinculados a la operación de buques, aeronaves y cables y tuberías submarinos, y que sean compatibles con las demás disposiciones de esta."

Teniendo en consideración estas atribuciones, derechos y deberes de los Estados, es muy importante entender que, la Autoridad Marítima Nacional (DICAPI) tiene la facultad para controlar en su área de jurisdicción, las actividades acuáticas y fiscalizar el cumplimiento de la normativa nacional, los instrumentos internacionales de los que el Perú es parte y otras normas de derecho internacional sobre la materia que puedan ser de aplicación al Estado peruano, para la represión de actividades ilícitas en el medio acuático y terrenos ribereños.; y si bien no hay una normativa específica al respecto, existe el compromiso y reconocimiento ante una alta instancia de las Naciones Unidas -Corte Internacional de Justicia de la Haya- que la interpretación jurídica del dominio marítimo empleado en nuestra Constitución es aplicado de manera consistente con las zonas marítimas señaladas en la Convención de 1982.

En este sentido, el Reglamento del DL 1147, (Artículo 23°) "Persecución de naves en el medio acuático", establece lo siguiente:

"Las unidades guardacostas o unidades navales asignadas a la Autoridad Marítima Nacional pueden emprender la persecución de una nave cuando tengan motivo fundado para considerar que esta, sus embarcaciones auxiliares o alguno de sus tripulantes haya infringido la normativa nacional, instrumentos internacionales de los que el Perú es parte y otras normas de derecho internacional sobre la materia que puedan ser de aplicación al Estado peruano.

a) En el caso de naves extranjeras, la persecución se inicia mientras estas se encuentren en aguas jurisdiccionales respecto de hechos que puedan constituir ilícitos prescritos en la normativa nacional, en concordancia con los instrumentos internacionales de los que el Perú es parte y otras normas de derecho internacional sobre la materia que puedan ser de aplicación al Estado peruano.
b) En el caso de naves extranjeras, la persecución solo puede continuar fuera de aguas jurisdiccionales peruanas a condición de no haberse interrumpido, en concordancia con la normativa nacional, instrumentos internacionales de los que el Perú es parte y otras normas de derecho internacional sobre la materia que puedan ser de aplicación al Estado Peruano. No se considera interrumpida la persecución cuando la unidad que la inicie sea relevada por otra"

7. CONCLUSIONES

Si bien el Perú no es parte de la Convención de las Naciones Unidas sobre el Derecho del Mar, esta es una realidad indiscutible y a la fecha forma parte del derecho internacional consuetudinario, por lo cual, en lo que se refiere a la seguridad y defensa, aún cuando el Perú exigiera mayores controles al paso de buques de guerra y submarinos extranjeros, estos podrían no ser aceptados por los demás Estados para quienes el sistema internacional reconoce la libertad de navegación fuera de las 12 millas marinas del mar territorial

A pesar de que el artículo 309° de la CONVEMAR indica que "No se pueden hacer reservas o excepciones a la Convención a no ser que se permitan expresamente por otros artículos de la Convención", el artículo 310° faculta a los Estados a formular "declaraciones o manifestaciones, cualquiera que sea su enunciado o denominación, a fin de, entre otras cosas, armonizar su derecho interno con las disposiciones de la Convención"

Algunos países han formulado declaraciones que señalan explícitamente que el goce de la comunicación internacional, de conformidad con la CONVEMAR, excluye todo uso no pacífico sin el consentimiento del Estado ribereño, como por ejemplo, ejercicios que requieran el uso de armas o ejercicios militares respectivamente, u otras actividades que puedan afectar los derechos o intereses del Estado ribereño. Excluye, además, recurrir a la amenaza o al uso de la fuerza contra la integridad territorial del Estado ribereño.

En este sentido, en la oportunidad en la que se decida adherir a la CONVEMAR e invocando a los Artículos 88° y 301°, así como también al Preámbulo, el Perú puede objetar el despliegue de una fuerza naval en aguas de su jurisdicción, así como la navegación de submarinos en inmersión, por percibir tal actividad como una amenaza contra su seguridad y la paz internacional, lo cual es ilegal de conformidad con la Carta de las Naciones Unidas.

Hay que recordar que Brasil, Argentina, y Ecuador formularon sendas manifestaciones al momento de declarar su adhesión a la Convención, en el sentido de que las disposiciones de la Convención no otorgan derechos a los demás Estados para llevar a cabo ejercicios o maniobras militares en la Zona Económica Exclusiva, en particular, aquellas que implican el uso de armas o explosivos, o transporte de sustancias radiactivas, sin el consentimiento del Estado ribereño:

- "El Gobierno del Brasil entiende que las disposiciones de la Convención no autorizan a otros Estados la realización de ejercicios militares o maniobras, en particular aquellas que implican el uso de armas o explosivos, sin el consentimiento del Estado ribereño"

- "La República Argentina respeta totalmente los derechos a la libre navegación comprendidos en la Convención; sin embargo, considera que el tránsito de buques que transportan substancias altamente radioactivas debe ser debidamente regulado".
- "El Estado ecuatoriano declara, de conformidad con los artículos 5 y 416 de la Constitución de la República, que sus espacios marítimos constituyen una zona de paz, en tal virtud, en dicha zona no podrá realizarse ningún tipo de ejercicios o maniobras militares, ni actividades de navegación que atenten o puedan atentar contra la paz y seguridad, sin su expreso consentimiento. Asimismo, manifiesta que se requerirá de notificación y autorización previas, para el tránsito por sus espacios marítimos, de buques impulsados por energía nuclear o que transporten sustancias radioactivas, tóxicas, peligrosas o nocivas"

Asimismo, podría invocarse el espíritu de la CONVEMAR, de conformidad con el Preámbulo adoptado, para promover los usos de los océanos con fines pacíficos, por lo que, suponiendo que una actividad de una potencia extranjera no fuese cuestionada como amenaza, el Perú podría invocar la cláusula general del Artículo 87° sobre la libertad de la alta mar, reclamando que esa actividad interfiere con un uso pacífico del mar. Por ejemplo, que les niega el acceso a las zonas de pesca tradicionales o que le crea peligros a su transporte marítimo comercial.

Finalmente, cubriendo otros asuntos vinculados con la seguridad, en las declaraciones al adherir a la CONVEMAR los Estados ribereños también se reservan el derecho exclusivo de construir y operar toda clase de instalaciones y estructuras sobre la plataforma continental incluyendo también instalaciones y estructuras militares.

Referencias

Acuerdo para Promover el Cumplimiento de las Medidas Internacionales de Conservación y Ordenación por los Buques Pesqueros que Pescan en Alta Mar, (1993) Organización de las Naciones Unidas para la Alimentación y la Agricultura

Acuerdo Relativo a la aplicación de la Parte XI de la CONVEMAR, (1994)

Acuerdo sobre aplicación de disposiciones de CONVEMAR relativas a la Conservación de las Poblaciones de Peces Transzonales y las Poblaciones de Peces Altamente Migratorios, (2001)

Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas, (1988). Organización Marítima Internacional.

Código Civil (1936), Ley 8305 de 30 de agosto de 1936, artículo 822 que establece que, dentro de los bienes de uso público del estado están incursos el mar territorial y sus playas y la zona anexa que señala la ley de la materia

Conferencia Especial de la Seguridad de la Organización de los Estados Americanos, (2001) Declaración sobre Seguridad en las Américas,

Convención de las Naciones Unidas sobre el Derecho del Mar, (1982),

Convención sobre la Protección del Patrimonio Cultural Subacuático, (2001)

Convenio para la Represión de Actos Ilícitos contra la Seguridad de la

Navegación Marítima, (1988). Organización Marítima Internacional.

Convenio sobre medidas de vigilancia y control de las Zonas Marítimas de los Países Signatarios, (1954) II Congreso sobre Explotación y Conservación de Riquezas Marítimas Pacífico Sur

Declaración sobre Zona marítima o Declaración de Santiago, (1952), por la cual los delegados de Chile, Ecuador y Perú proclaman la soberanía y jurisdicción de sus exclusivas sobre el mar que baña las costas de sus respectivos países hasta una distancia mínima de 200 millas marinas desde las referidas costas

Decreto Legislativo 1138, (2012) Ley de la Marina de Guerra del Perú

Decreto Legislativo N° 1147, (2012) que regula el fortalecimiento de las Fuerzas Armadas en las competencias de la Autoridad Marítima Nacional – Dirección General de Capitanías y Guardacostas

Decreto Supremo Nº 015-2014-DE, (2014) que aprueba el Reglamento del Decreto Legislativo Nº 1147, que regula el fortalecimiento de las Fuerzas Armadas en las competencias de la Autoridad Marítima Nacional – Dirección General de Capitanías y Guardacostas

Decreto Supremo Nro. 012-2017-DE ,(2012) que aprueba la Política Nacional de Seguridad y Defensa Nacional del Perú, estableciendo los lineamientos y principios para la protección de los intereses nacionales, la soberanía y la integridad territorial

Decreto Supremo Nro. 012-2019-DE, (2019) que aprueba la Política Nacional Marítima

Decreto Supremo nro. 14, (1833), que regulaba la pesca sólo para ciudadanos peruanos.

Decreto Supremo nro. 13, (1934), que aprueba el Reglamento de visita y permanencia de buques y aeronaves de guerra extranjeros en aguas territoriales peruanas

Decreto Supremo 781, (1947). Por el cual se fija el dominio marítimo de la Nación

Fallo de la Corte Internacional de Justicia de la Haya, (24 enero 2014). Controversia marítima Perú-Chile

Gamarra, C. (2023), Seguridad y defensa en el marco de la Convemar, El Perú y la Convención del mar, Nicolas Roncagliolo, Oscar Vidarte, Fundación Academia Diplomática

Libro Blanco de la Defensa Nacional, (2005) Política de Seguridad y Defensa Nacional, capitulo III

Novena Política Nacional, (2002) Política de Seguridad Nacional, que se constituye un Acuerdo Nacional

Protocolo para la Represión de Actos Ilícitos contra la Seguridad de las Plataformas Fijas emplazadas en la Plataforma Continental, (1988). Organización Marítima Internacional.

Reglamento de capitanías y de la marina mercante nacional, (1940) Ministerio de Marina y Aviación. Talleres Tipográficos de la Escuela Naval del Perú

Reglamento de capitanías y de la marina mercante nacional, RSC-139, (1951) Editorial Torres Aguirre

Schiaffino, C., (1995) Marina de guerra del Perú y el caso Onassis, *Revista de Marina*, nro. 3, Jul-set 1995, Dirección de Información de la Marina

Año 2025, Vol. 22, Nº 3, pp. 139- 155.
DOI: https://doi.org/10.35628/resup.v16i2.178

Ciberdefensa: Una opción para reforzar las capacidades de Ciberseguridad en el Perú

Cyberdefense: An Option to Strengthen Cybersecurity Capabilities in Peru

Recibido: 18 de agosto del 2025 | Aceptado: 05 de diciembre de 2025

José Aguirre R
https://orcid.org/0009-0006-8430-6243
Capitán de Fragata de la Marina de Guerra del Perú, Licenciado en Ciencias Marítimo Navales, Maestro en Dirección Estratégica en Telecomunicaciones, Ingeniería de Sistemas y Seguridad Informática. Doctorando en Proyecto de Ciberseguridad y Ciberdefensa, Certificaciones en Seguridad de la Información, Continuidad de Procesos, I.A. entre otros. Con amplio recorrido en soluciones seguridad, tecnologías de la información y telecomunicaciones, gestión de recursos y optimización de procesos. Docente de Ciberseguridad y TIC´s.
Email:josejo2@proton.me

Resumen: El presente artículo examina cómo las capacidades de ciberdefensa pueden apoyar y fortalecer las actividades de ciberseguridad en el contexto peruano. A través del análisis del caso de los Juegos Panamericanos y Parapanamericanos Lima 2019, se evalúa cómo la incorporación de estrategias y procedimientos operativos propios de la ciberdefensa, mejoró la resiliencia cibernética frente a posibles ciberamenazas, destacando su aplicabilidad en la protección de activos críticos nacionales. La relación entre la ciberseguridad y la ciberdefensa se discute desde un enfoque teórico y práctico, aportando una visión estratégica de cómo estas capacidades pueden integrarse para fortalecer la seguridad digital en el Perú.

Palabras Clave: Ciberdefensa, Ciberseguridad, Resiliencia Cibernética, Activos Críticos, Juegos Panamericanos Lima 2019, Perú, Estrategia Digital.

Abstract: *This article examines how cyberdefense capabilities can support and strengthen cybersecurity activities within the Peruvian context. Through the analysis of the Lima 2019 Panamerican and Parapanamerican Games case, it evaluates how the incorporation of strategies and operational procedures specific to cyberdefense enhanced cyber resilience against potential cyber threats, highlighting their applicability in protecting national critical assets. The relationship between cybersecurity and cyberdefense is discussed from both theoretical and practical perspectives, offering a strategic view of how these capabilities can be integrated to reinforce digital security in Peru.*

Keywords: *Cyberdefense, Cybersecurity, Cyber Resilience, Critical Assets, Lima 2019 Pan American Games, Peru, Digital Strategy.*

1. INTRODUCCIÓN

La creciente y vertiginosa dependencia de la tecnología en las infraestructuras críticas de un Estado, su desarrollo y las amenazas cibernéticas, han llevado a los países a adoptar medidas rigurosas de protección. En este contexto, la ciberseguridad y la ciberdefensa juegan roles centrales. La ciberseguridad se centra en proteger sistemas y redes frente a ataques cibernéticos, mientras que la ciberdefensa involucra medidas defensivas y ofensivas para salvaguardar la soberanía y seguridad nacional en el ciberespacio. Ante la creciente amenaza que los ciberataques representan, ambos conceptos han adquirido relevancia estratégica y operativa en el Perú, donde se han implementado leyes específicas para regular estas actividades (Ministerio de Defensa, 2019; Ley N° 30999, El Peruano, 2019), como se muestra en el transcurso de este texto.

El objetivo general de este artículo enfocado en la investigación, es demostrar que las capacidades de ciberdefensa pueden complementar y fortalecer las actividades de ciberseguridad en el Perú, particularmente en la protección de activos críticos nacionales (ACN). En el contexto de los XVIII Juegos Panamericanos y VI Juegos Parapanamericanos de Lima 2019, el uso de estas capacidades en la protección de infraestructuras digitales temporales se presenta como un caso de estudio relevante, para analizar cómo la ciberdefensa y la ciberseguridad pueden actuar de manera sinérgica. La hipótesis del estudio sugiere que la integración de la ciberdefensa en los procesos de ciberseguridad mejora el tiempo de respuesta frente a incidentes de seguridad y, en consecuencia, aumenta la efectividad de la protección de los activos digitales.

2. MARCO TEÓRICO

De acuerdo con la Stanford University (2020) la ciberseguridad es conjunto de técnicas utilizadas para proteger la integridad de las redes, programas y datos contra ataques, daños o accesos no autorizados. En el contexto nacional, se define la ciberseguridad como la "capacidad de preservar el adecuado funcionamiento de los activos informáticos, protegiéndolos de amenazas y vulnerabilidades…" (DU N° 007-2020, El Peruano, 2020). La ciberseguridad en el Perú se fundamenta en la preservación de tres principios, que funcionan también como pilares de este concepto: disponibilidad, integridad y confidencialidad de la información en el ciberespacio, aplicables tanto a sectores públicos como privados, especialmente aquellos vinculados a los activos críticos nacionales.

Por otro lado, la ciberdefensa, con una trayectoria relativamente reciente en el Perú, surgió como una estrategia dentro del Ministerio de Defensa con la creación de los Comandos de Ciberdefensa del Ejército y la Marina entre los años 2018 y 20191. De acuerdo con Ley N° 30999 (2019), esta describe a la ciberdefensa como "la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional…"

También y de acuerdo con Sáinz (2016) la ciberdefensa no solo implica proteger los sistemas propios, sino también realizar operaciones ofensivas y de inteligencia para neutralizar amenazas. Del marco legal descrito en el párrafo precedente, se subraya la importancia de que las capacidades defensivas y ofensivas del Estado peruano en el ciberespacio sean organizadas y ejecutadas de forma que permitan responder adecuadamente a las amenazas externas, tomando en cuenta la definición que la Cooperative Cyber Defence Center Of Excellence de la NATO (2013) hace al ciberespacio, como "…el entorno en el que se desarrollan las operaciones de ciberdefensa para proteger y defender los sistemas de información y las redes contra amenazas y ataques cibernéticos".

Es importante mencionar que los incidentes de seguridad informática son recurrentes en las redes de datos de todas las organizaciones y forman el quehacer diario en los diferentes Centros de Operaciones de Seguridad (SOC) de las entidades que operan en el Estado peruano, tanto públicas como privadas. Es así que dentro de las entidades privadas en el país, cualquiera fuese su rubro, algunas de ellas se han encargado también de su propia seguridad informática; por ello han optado por gestionar la seguridad de su información, con personal y procesos propios, bajo el soporte de la tecnología necesaria y así lograr alcanzar este objetivo.

Vinculado a ello, existen otras entidades privadas que buscan tercerizar su seguridad de información e informática, con empresas dedicadas al rubro. En

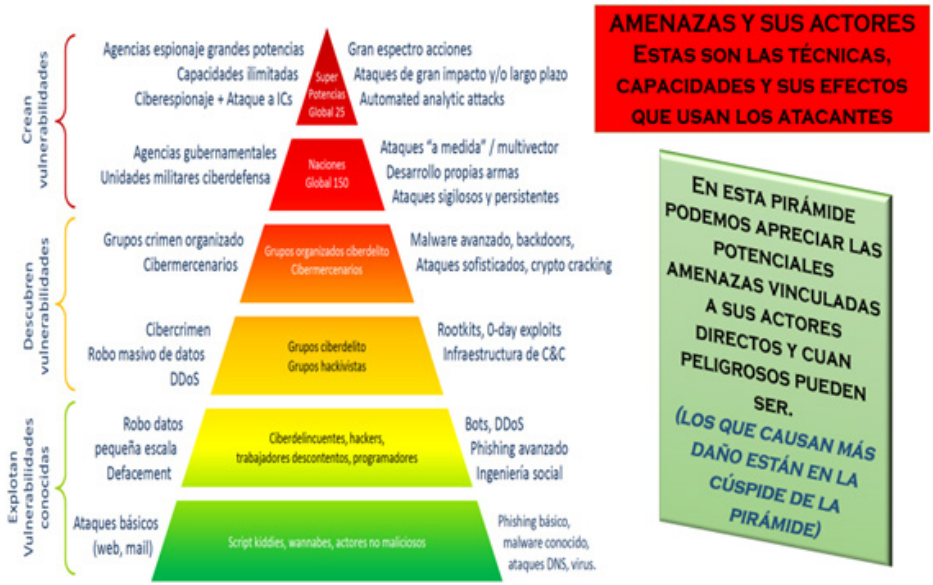
este punto, cabe resaltar que existen entidades privadas que brindan servicios de protección y seguridad informática, donde se puede inferir que estas últimas al brindar estos servicios, tienen la suficiente autonomía para la protección de su propia información y redes informáticas, al contar una madurez mayor en procesos de seguridad de la información y ciberseguridad. Asimismo, tenemos a las entidades públicas, donde algunas de ellas manejan información de seguridad a nivel bajo, medio e información no sensible, generada producto de sus actividades diarias.

Por otro lado, tenemos a las entidades públicas que gestionan el manejo de información para operaciones que sostienen servicios ligados con activos críticos nacionales (ACN); estos activos críticos nacionales son de gran interés para la Nación, dado que la continuidad de sus operaciones tiene impacto directo en la ciudadanía y en las actividades que generan recursos para el Estado.

En ese sentido, las entidades que administran los ACN se convierten en un interesante blanco para los ciberataques, los cuales podrían ser realizados por los siguientes actores y sus respectivas capacidades:

FIGURA 1

Escala de actores vs. sus capacidades en el ciberespacio (Ecosistema de las ciberamenazas)



Fuente: Unidades de Ciberinteligencia y ciberguerra al servicio de Estados (Cubeiro E. 2021)

El vínculo entre ciberseguridad y ciberdefensa en el Perú se podría establecer a través de la coordinación de sus capacidades, sin perjuicio de las normas mencionadas en los párrafos precedentes y que describen sus funcionalidades. La ciberseguridad, desde un enfoque preventivo y reactivo, implica la capacidad de detectar y reaccionar frente a ataques para proteger la integridad de los sistemas. La ciberdefensa, por su parte y en adición, aporta capacidades de explotación y respuesta, siendo esta última la proyección del poder en el ciberespacio para contrarrestar a adversarios, de forma preventiva y correctiva. De este modo, ambas capacidades se complementan: mientras la ciberseguridad protege a los sistemas de ataques, la ciberdefensa amplía este rol al crear una estrategia ofensiva para enfrentar a actores hostiles (Faliero, 2020, p. 65).

3. BREVE RESEÑA DE LA METODOLOGÍA

La investigación para este artículo utiliza una metodología de revisión documental y análisis de caso. En primer lugar, se realizó una revisión sistemática de la legislación y teorías asociadas a la ciberseguridad y la ciberdefensa, tanto en el ámbito nacional como internacional, con especial enfoque en los conceptos de ciberespacio, ciberseguridad y ciberdefensa, y la interrelación y vínculos en las actividades de estos conceptos. En segundo lugar, se analizó el caso de éxito de los Juegos Panamericanos y Parapanamericanos de Lima 2019, evento en el cual se implementaron capacidades de ciberdefensa y ciberseguridad para proteger la infraestructura digital del evento. La hipótesis se valida a través de indicadores, como el tiempo de reacción frente a incidentes de seguridad, y la efectividad de los procedimientos operativos de ciberdefensa implementados.

Análisis del Caso de Éxito: Juegos Panamericanos y Parapanamericanos Lima 2019

Los Juegos Panamericanos y Parapanamericanos de Lima 2019 representaron un evento de gran magnitud en el Perú, considerado un activo crítico nacional temporal. En este contexto, la infraestructura digital del evento fue objeto de una estrategia de ciberseguridad y ciberdefensa que incluyó la implementación de un Centro de Operaciones de Seguridad (SOC). Este centro tuvo la finalidad de monitorear y proteger los sistemas y redes del evento. La Marina de Guerra del Perú fue la entidad responsable de liderar las actividades de ciberdefensa, en coordinación con el Proyecto Especial de los Juegos Panamericanos y Parapanamericanos (PEJP), y el sector privado, que incluyeron a las empresas

nacionales e internacionales líderes en el aseguramiento en transmisión de datos y su respectiva seguridad informática.

El SOC, implementado en las instalaciones del Centro de Convenciones de Lima (CCL), contó con personal de la Marina y de otras fuerzas, quienes implementaron una serie de procedimientos operativos para monitorear y responder ante incidentes de seguridad en tiempo real. Los procedimientos de ciberdefensa incluyeron actividades de detección de malware, ataques DDoS, amenazas en redes sociales y amenazas de ransomware. En términos de métricas, el SOC logró reducir el tiempo de reacción frente a incidentes de seguridad, mediante la implementación de protocolos de ciberdefensa que optimizaron la respuesta y mitigación de los ataques detectados. Este caso permitió demostrar que la combinación de ciberseguridad y ciberdefensa mejoró significativamente la resiliencia cibernética en un evento de alto perfil.

Resultados de la investigación

El análisis del caso de los Juegos Panamericanos y Parapanamericanos de Lima 2019 evidenció una clara mejora en las capacidades de respuesta ante incidentes de seguridad, gracias a la integración de procedimientos de ciberdefensa en las actividades de ciberseguridad. Las métricas de tiempo de reacción, comparadas con los tiempos promedio de incidentes gestionados en otros contextos, demostraron que el uso de protocolos de ciberdefensa permitió responder de manera más rápida y efectiva.

Además, el caso evidenció que los procedimientos de ciberdefensa influyeron positivamente en la protección de los activos críticos del evento, al establecer una barrera adicional frente a ciberamenazas avanzadas (Rodríguez, 2020, p. 86).

Ahora bien, en el análisis de los resultados se analizarán las diferencias entre los tiempos de reacción, sometiendo las métricas obtenidas a los cálculos de las fórmulas establecidas (ensayos propios) para su evaluación. Se emplearán los siguientes cálculos:

- IPC = ∑ PROCEDIMIENTOS VINCULADOS DE CIBERDEFENSA (PVCD)
- PR = ∑ PROCEDIMIENTOS REGULARES DE CIBERSEGURIDAD (PRCS)
- TRA = ∑ TIEMPO DE ACTIVIDADES DONDE SE CONSIDERAN PROCEDIMIENTOS DE CIBERDEFENSA (TAPCD)
- TR = ∑ TIEMPO DE ACTIVIDADES DONDE NO SE CONSIDERAN PROCEDIMIENTOS DE CIBERDEFENSA (TANPCD)

En ese sentido de la siguiente formula general:

$$Si,\ IPC \geq PR \Rightarrow TRA < TR$$

Obtendremos la siguiente formulada detallada con las métricas a calcular:

$$SI,\ \sum(PVCD) > \sum(PRCS) \Rightarrow \sum(TAPCD) < \sum(TANPCD)$$

En análisis comparativo, se trataron los eventos e incidentes de seguridad informática con la intervención de las actividades de ciberseguridad, respecto a la posterior implementación de los procedimientos de ciberdefensa asociados a cada uno de los eventos e incidente de seguridad.

A continuación, presento el cuadro resumen, para visualizar de forma clara los tiempos mínimos tomados en las actividades de ciberseguridad y los procedimientos de ciberdefensa, con respecto a los eventos e incidentes de seguridad informática:

TABLA 1

Cuadro resumen con las métricas tomadas de las actividades de ciberseguridad y los procedimientos de ciberdefensa.

	EVENTOS E INCIDENTE DE SEGURIDAD INFORMÁTICA	ACTIVIDADES DE CIBERSEGURIDAD	TIEMPO EMPLEADO PARA REACCIÓN	PROCEDIMIENTO DE CIBERDEFENSA ASOCIADO	TIEMPO MÍNIMO ALCANZADO PARA LA REACCIÓN
1	Ataque por inserción de virus	Actividad de detección y reacción	51 minutos	Procedimiento para la detección de virus/malware	28 minutos
2	Ataque por inserción de malware de tipo gusano y troyano	Actividad de reacción antimal-ware	38 minutos	Procedimiento para la detección de malwares de tipo gusano/ troyanos	32 minutos
3	Ataque por inserción de malware de tipo spyware/ rootkit/otros	Actividad de reacción antimalware	38 minutos	Procedimiento para el ataque de malware tipo spyware/rootkit/ otros	26.5 minutos
4	Ataque de denegación de servicio simple y distribuida	Acción automáti-ca de reacción ante ataque DoS y DDoS	Inmediato, a re-acción de la her-ramienta (hasta una capacidad "Y" en GB)	Procedimiento para el ataque de DDoS	Inmediato, a reacción de la herramienta (hasta una capacidad "Y + 15" en GB)
5	Ataque a las páginas Web de los JPP	Actividad de reacción ante defacement	75 minutos	Procedimiento para el ataque web defacement y otros	13 Minutos
6	Amenazas mediante redes sociales	Actividad de detección y reacción ante amenazas por redes sociales	125 minutos	Procedimiento para las amenazas por redes sociales de los JPP	36 Minutos
7	Ataques que ocasionan la pérdida de conectividad de las redes inter-nas y externas de los JPP	Actividad de reacción ante pérdidas de conectividad	55 minutos	Procedimiento para la pérdida de conectividad por ataques	38 minutos

8	Ataque de tipo ransomware	Actividad de reacción ante eventos de tipo ransomware	Indeterminado	Procedimiento para el ataque de tipo ransomware	6 Minutos, para el aislamiento del equipo y pasa a forense
9	Identificación de amenazas latentes en la red en contra de los JPP	Indeterminado	Indeterminado	Procedimientos para la activación de la capacidad de explotación	37 Minutos
10	Ataque al funcionamiento del SIEM	Indeterminado	Indeterminado	Procedimiento ante caída del SIEM por ataques externos e interno	8.3 Minutos
11	Malos manejos de seguridad en los accesos y claves por parte de los usuarios	Actividad de reacción ante fallas de seguridad por usuarios	Entre 40 a 50 minutos, varios casos	Procedimientos ante fallos de operación o manipulación de usuarios	Entre 15 y 20 minutos, varios casos
12	Generación de eventos disruptivos	Protocolos ante eventos sísmicos o siniestros	10.5 minutos	Procedimientos ante eventos disruptivos (Desastres naturales)	2.7 minutos
13	Generación de siniestros y otros	Protocolos ante eventos sísmicos o siniestros	10.5 minutos	Procedimiento ante eventos de siniestros, inundaciones, otros	1.4 minutos

Fuente: Elaboración propia.

Ahora bien, como se puede apreciar en el cuadro N° 1, en la gran mayoría de los casos los procedimientos de ciberdefensa implementados tienen menores tiempos de reacción que las actividades de ciberseguridad por sí solas. Menciono en la mayoría de los casos, dado que para algunos eventos de seguridad no se implementaron actividades de reacción en ciberseguridad, como son los casos de los ataques de tipo ransomware, las amenazas identificadas y latentes en contra de los JPP, ataque a la operatividad del Gestor de Eventos de Seguridad de la Información o conocido por su traducción al inglés, como Security Information and Event Management (SIEM), entre otros. En ese sentido, en ese momento

los procedimientos de ciberdefensa abordaron todos esos eventos, y donde estos procedimientos tuvieron coincidencia con las actividades de ciberseguridad, los tiempos de reacción favorecieron a estos procedimientos de ciberdefensa versus las actividades de ciberseguridad. Resumiendo, este punto distingue a los procedimientos de ciberdefensa, al estar altamente entrenados con protocolos bien definidos, una distinción que marcaría una gradual mejora en este caso en particular, sobre las actividades de ciberseguridad en los Juegos. A continuación, se muestra un detalle de las diferencias:

TABLA 2
Cuadro con métricas comparadas y sus respectivos porcentajes por eventos e incidentes de seguridad.

	EVENTOS E INCIDENTE DE SEGURIDAD INFORMÁTICA	ACTIVIDADES DE CIBERSEGURIDAD	PROCEDIMIENTO CIBERDEFENSA	RESULTANTE A FAVOR DE PROCEDIMIENTOS	PORCENTAJE DISMINUCIÓN
1	Ataque por inserción de virus	51 minutos	28 minutos	**23 Minutos Menos**	**45.10%**
2	Ataque por inserción de malware de tipo gusano y troyano	38 minutos	32 minutos	**6 Minutos Menos**	**15.79%**
3	Ataque por inserción de malware de tipo spyware/ rootkit/otros	38 minutos	26,5 minutos	**11,5 Minutos Menos**	**30.27%**
4	Ataque de denegación de servicio simple y distribuida	Inmediato, a reacción de la herramienta (hasta una capacidad "Y" en GB)	Inmediato, a reacción de la herramienta (hasta una capacidad "Y + 15 en GB)	**Mejora en la capacidad de la herramienta de 22 a 37 GB.**	**68% (Aumento en capacidad)**
5	Ataque a las páginas Web de los JPP	75 minutos	13 minutos	**62 Minutos Menos**	**82.67%**
6	Amenazas mediante redes sociales	125 minutos	36 Minutos	**89 Minutos Menos**	**71.20%**

7	Ataques que ocasionan la pérdida de conectividad de las redes internas y externas de los JPP	55 minutos	38 minutos	**17 Minutos Menos**	**30.91%**
8	Ataque de tipo ransomware	Indeterminado	6 Minutos, para el aislamiento del equipo y pasa a forense	Sin Cálculo	**100.00%**
9	Amenazas latentes en la red en contra de los JPP	Indeterminado	37 Minutos	Sin Cálculo	**100.00%**
10	Ataque al funcionamiento del SIEM	Indeterminado	8.3 Minutos	Sin Cálculo	**100.00%**
11	Malos manejos de seguridad en los accesos y claves por parte de los usuarios	Entre 40 a 50 minutos, varios casos	Entre 15 y 20 minutos, varios casos	30 Minutos Menos	**60.00%**
12	Generación de eventos disruptivos	10.5 minutos	2.7 minutos	7.8 Minutos Menos	**74.29%**
13	Generación de siniestros y otros	10.5 minutos	1.4 minutos	9.1 Minutos Menos	**86.54%**
				PROMEDIO (%)	**66.40%**

Fuente: Elaboración propia, con datos del SOC de los JPP.

Los procedimientos de ciberdefensa tienen, en promedio, un porcentaje del 66.40% en disminución del tiempo de reacción con respecto a las actividades de ciberseguridad; esto podría indicar que los cálculos en la fórmula general propuesta en la hipótesis serían positivos.

"Ataque a las páginas Web de los JPP", que se redujo de 75 a 13 minutos; esto evidencia de forma positiva, que efectivamente los procesos de ciberdefensa aplicados a las equivalentes actividades de ciberseguridad, pueden sumar a sus capacidades de reacción.

En adición, eventos donde el tiempo de reacción es vital, porque no solo involucra la integridad física de los equipos, sino también a las personas encargadas de las operaciones, como el Centro de Operaciones de Seguridad (SOC) y el Centro de Operaciones de Tecnología (TOC), son los eventos referidos a los eventos disruptivos, los mismos que pueden presentarse en diferentes situaciones, pero que en esencia son los movimientos telúricos y los incendios, para los cuales se elaboraron procedimientos a medida de acuerdo a la distribución del recinto, cantidad de personas, tomas eléctricas, zonas de resguardo, salidas de emergencia, entre otros. Como podemos apreciar en el cuadro N° 2, en los procedimientos 12 (generación de eventos disruptivos) y 13 (generación de siniestros y otros) que, si bien es rescatable que estos ejercicios se practicaron con cierta regularidad y obtuvieron resultados aceptables, el entrenamiento realizado sobre la base de los procedimientos de ciberseguridad, le dieron a esta actividad una mejora del 74% y 86% respectivamente, en tiempo de reacción.

El porcentaje promedio de mejora se podría considerar como un aporte significativo de los procedimientos de ciberdefensa sobre las actividades de reacción de ciberseguridad. Este análisis previo se consolidaría con la ejecución de la fórmula descrita en la hipótesis propuesta.

Visualización de Resultados

Luego de evaluar y analizar respecto a los procedimientos de la ciberdefensa con las actividades de ciberseguridad, aplicamos la fórmula a los resultados obtenidos, con el siguiente detalle:

TABLA 3

Cuadro con Procedimientos de ciberdefensa y sus tiempos de reacción durante los JPP.

#	EVENTO O INCIDENTE DE SEGURIDAD INFORMÁTICA	PROCEDIMIENTOS CIBERDEFENSA
1	Ataque por inserción de virus	28 minutos
2	Ataque por inserción de malware de tipo gusano y troyano	32 minutos
3	Ataque por inserción de malware de tipo spyware/rootkit/otros	26.5 minutos
4	Ataque de denegación de servicio simple y distribuida	Inmediato, a reacción de la herramienta (hasta una capacidad "Y + 15 en GB)
5	Ataque a las páginas Web de los JPP	13 Minutos
6	Amenazas mediante redes sociales	36 Minutos
7	Ataques que ocasionan la perdida de conectividad de las redes internas y externas de los JPP	38 minutos
8	Ataque de tipo ransomware	6 Minutos, para el aislamiento del equipo y forense
9	Identificación de amenazas latentes en la red en contra de los JPP	37 Minutos
10	Ataque al funcionamiento del SIEM	8.3 Minutos
11	Malos manejos de seguridad en los accesos y claves por parte de los usuarios	Entre 15 y 20 minutos, varios casos
12	Generación de eventos disruptivos	2.7 minutos
13	Generación de siniestros y otros	1.4 minutos

Fuente: Elaboración propia, con datos del SOC de los JPP.

Al sumar los tiempos de estos procedimientos (en minutos), sobre la base de 12 procedimientos (no se toma en consideración el procedimiento de mitigación ante ataques de denegación de servicio simple y distribuido – DDoS, dado que no devela un tiempo perse, sino que demuestra una mejora en la capacidad de ancho de banda mientras recibe un ataque de denegación de servicio), se obtiene el siguiente resultado:

$$TRA = 28 + 32 + 26.5 + 13 + 36 + 38 + 6 + 37 + 8.3 + 20 + 2.7 + 1.4 = 248.9 \text{ Minutos.}$$

Cuyo promedio es entre 12 (cantidad de procedimientos sumados)

$$\text{Promedio IPC} = 248.9 \div 12 = 20.74 \text{ Minutos.}$$

- TR = ∑ TIEMPO DE ACTIVIDADES DONDE NO SE CONSIDERAN PROCEDIMIENTOS DE CIBERDEFENSA (TANPCD)

TABLA 4

Cuadro con las actividades de reacción de ciberseguridad y sus tiempos de reacción durante los JPP.

#	EVENTO O INCIDENTE DE SEGURIDAD INFORMÁTICA	ACTIVIDADES CIBERSEGURIDAD
1	Ataque por inserción de virus	51 minutos
2	Ataque por inserción de malware de tipo gusano y troyano	38 minutos
3	Ataque por inserción de malware de tipo spyware/rootkit/otros	38 minutos
4	Ataque de denegación de servicio simple y distribuida	Inmediato, a reacción de la herramienta (hasta una capacidad "Y" en GB)
5	Ataque a las páginas Web de los JPP	75 minutos
6	Amenazas mediante redes sociales	125 minutos
7	Ataques que ocasionan la perdida de conectividad de las redes internas y externas de los JPP	55 minutos
8	Ataque de tipo ransomware	Indeterminado
9	Identificación de amenazas latentes en la red en contra de los JPP	Indeterminado
10	Ataque al funcionamiento del SIEM	Indeterminado
11	Malos manejos de seguridad en los accesos y claves por parte de los usuarios	Entre 40 a 50 minutos, varios casos
12	Generación de eventos disruptivos	10.5 minutos
13	Generación de siniestros y otros	10.5 minutos

Fuente: Elaboración propia, con datos del SOC de los JPP.

Los procedimientos de ciberseguridad respecto al caso de éxito alcanzaron tiempos aceptables de reacción en su ejecución; estas actividades y sus tiempos de reacción son los siguientes:

Procedemos ahora con la suma de los tiempos de estas actividades de ciberseguridad (en minutos), pero en este caso, a diferencia de los 12 procedimientos usados en ciberdefensa, únicamente usaremos el tiempo de 9 actividades. De igual manera, la actividad que mitiga los ataques de denegación de servicio simple y distribuido DDoS, no devela un tiempo perse, sino un ancho de banda mientras recibe un ataque de denegación de servicio. Asimismo, no se registró una actividad de reacción en ciberseguridad para los ataques de tipo ransomware, ni para la identificación de amenazas latentes en la red contra los JPP.

Adicionalmente, en los eventos de seguridad que no cuenten con actividades de ciberseguridad que ayuden a mitigarlo, se asignará el tiempo de reacción máximo alcanzado por una actividad de ciberseguridad. Entonces, se efectúa el siguiente cálculo:

TR = 51 + 38 + 38 + 75 + 125 + 55 + 75(*) + 75(*)
+ 75(*) + 50 + 10.5 + 10.5 = 678.0 Minutos.
(*) Tiempo alto de una actividad de ciberseguridad,
usado como reemplazo para actividades que no contaban con
reacción para un determinado evento de seguridad.
Cuyo promedio es entre 12 (cantidad de procedimientos sumados)
Promedio PR = 678.0 ÷ 12 = 56.50 Minutos.

Luego de la toma de métrica y cálculos, reemplazo en la fórmula propuesta en la hipótesis:

Si, IPC ≥ PR => TRA < TR

Entonces:
IPC = 13 Procedimientos de ciberdefensa
PR = 10 Actividades de reacción de ciberseguridad
TRA = 248.9 Minutos
TR = 678 Minutos

Si, 13 ≥ 10 => 248.9 < 678

Luego, como podemos visualizar, se cumple el postulado de la hipótesis, donde a mayor o igual cantidad de inclusión de procedimientos de ciberdefensa versus las actividades de ciberseguridad, se tiene que los tiempos de reacción ante eventos de seguridad, mejoran con respecto a los iniciales.

Esto evidencia que la hipótesis planteada para el trabajo de investigación es correcta.

Fórmula inicial de la hipótesis:
Si, IPC ≥ PR => TRA < TR

Fórmula de la hipótesis con datos de la investigación:
Si, 13 ≥ 10 => 248.9 < 678

4. UNA BREVE DISCUSIÓN

La experiencia de los Juegos Panamericanos y Parapanamericanos de Lima 2019 ofrece importantes lecciones sobre la integración de ciberdefensa y ciberseguridad en el Perú. Una de las principales lecciones es la necesidad de colaboración constante entre el sector público, privado y las Fuerzas Armadas para enfrentar los riesgos del ciberespacio de forma unificada. Si bien el caso demostró la eficacia de esta colaboración, también resaltó la necesidad de desarrollar protocolos más detallados para la cooperación en eventos futuros y la protección de infraestructuras críticas permanentes (Clarke, 2011, p. 75).

A nivel internacional, varios países han adoptado enfoques similares para integrar la ciberdefensa y la ciberseguridad en la protección de sus activos digitales. Países como Estados Unidos y el Reino Unido, han implementado comandos de ciberdefensa que colaboran directamente con agencias de ciberseguridad para proteger infraestructuras críticas. El caso peruano, aunque aún en desarrollo, muestra un progreso significativo hacia esta integración y plantea la posibilidad de ampliar estas capacidades en el futuro, especialmente en sectores vulnerables como energía, telecomunicaciones y banca (Sáinz, 2016, p. 124).

5. CONCLUSIÓN Y RECOMENDACIÓN

Los hallazgos de esta investigación demuestran que las capacidades de ciberdefensa pueden fortalecer significativamente las actividades de ciberseguridad en el Perú. La integración de procedimientos operativos de ciberdefensa en el contexto de los Juegos Panamericanos y Parapanamericanos de Lima 2019, optimizó el tiempo de respuesta frente a incidentes y aumentó la resiliencia del SOC de los juegos ante diversas ciberamenazas. Esta colaboración entre ciberseguridad y ciberdefensa subraya la importancia de una estrategia nacional coordinada, que permita enfrentar de manera efectiva los riesgos y amenazas del ciberespacio.

Se recomienda que el Estado peruano refuerce la colaboración entre entidades públicas y privadas en el campo de la ciberseguridad, promoviendo la participación de actores relevantes en los esfuerzos de ciberdefensa. Es crucial continuar fortaleciendo la capacitación y los recursos tecnológicos de los SOC´s, de modo que los protocolos de ciberdefensa puedan integrarse de manera efectiva en la ciberseguridad. Las lecciones aprendidas del caso de los Juegos Panamericanos, sugieren que una estrategia coordinada y adaptada a las necesidades de la ciberseguridad y ciberdefensa es fundamental para proteger los activos críticos nacionales.

Referencias

Baca, G. (2016). Introducción a las Seguridad Informática. México: Grupo Editorial Patria.

Bello, E. (2020). Ciberseguridad: Tipos de ataques y en qué consisten. Recuperado de: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Cari, P. (2013). Ciberdefensa – Ciberseguridad, Riesgos y Amenazas. Definición del concepto de ciberseguridad.

Clarke, R. & Knake, R. (2011). Guerra en la red, los nuevos campos de batalla. Barcelona. Editorial Planeta.

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

Cubeiro, E. (2021). Unidades de ciberinteligencia y ciberguerra al servicio de Estados. Consultado el 7 de enero del 2022. Recuperado de ATALAYAR: https://atal.ayar.com/content/unidades-de-ciberinteligencia-y-ciberguerra-al-servicio-de-estados

DU N° 007-2020, El Peruano. (2020). Decreto de Urgencia N° 007-2020, Gobierno del Perú.

Faesen, L., Torossian, B., Mayhew, E. (2020). Conflicto en el ciberespacio Análisis de las amenazas y el estado del orden internacional en el ciberespacio. Recuperado de: https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/conflict-in-berspace/11

Faliero, R. (2020). "Cybersecurity Defense Strategies". *International Journal of Cyber Defense.*

Garzón, D., Ratkovich, J. C. y Vergara, A. (2017). Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala. Bogotá: Pontifica Universidad Javariana.

Ley N° 30999, El Peruano. (2019). Ley de Ciberdefensa, Gobierno del Perú.

Ministerio de Defensa (2019). Lineamientos para la ciberdefensa en el Perú. Lima: Ministerio de Defensa.

Puime, J. (2009). El ciberespionaje y la ciberseguridad.

Rodríguez, M. (2020). *El reto de la ciberseguridad en América Latina*. Editorial Seguridad Digital.

Rufián, N. (31 de agosto del 2020). La importancia del ciberespacio y de la ciberseguridad en las organizaciones. Segurilatam. Recuperado de: https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/la-importancia-del-ciberespacio-y-de-la-ciberseguridad-en-las-organizaciones_20200831.html

Sáinz, M. (2016). Ciberseguridad: Estrategias y desafíos. Editorial Seguridad Global.

Virilio, P. (1995). Cyber War and the Need for a Cyberdefense Strategy. *Defense and Security Journal.*


MARINA DE GUERRA DEL PERÚ
AGNITIO OMNIA VINCET
ESCUELA SUPERIOR DE GUERRA NAVAL