ESCUELA NAVAL DE CADETES "ALMIRANTE PADILLA" Honor y Tradición

DERROTERO

Artículo

Inteligencia estratégica y soberanía digital: Desafíos y oportunidades para la Armada Nacional de Colombia

Strategic Intelligence and Digital Sovereignty: Challenges and Opportunities for the National Navy of Colombia

Ricardo Heriberto Garate Vera
Universidad Mayor, Universidad de Concepción, Instituto Profesional CIISA y Academia Politécnica Militar de Chile.
Correspondencia: rgaratev@gmail

Resumen: La inteligencia estratégica y la soberanía digital se han convertido en ejes fundamentales para la defensa nacional y marítima de Colombia ante las amenazas emergentes del siglo XXI. En un entorno donde el ciberespacio constituye un nuevo dominio de confrontación global, la Armada Nacional enfrenta el reto de integrar la ciberdefensa marítima dentro de su doctrina, estructura organizacional y marco jurídico. A partir de las experiencias internacionales de EE.UU, China, Rusia, la Unión Europea y la OTAN, así como de los aportes de centros de pensamiento especializados, se identifican los principales desafíos y oportunidades que enfrenta el país en su tránsito hacia una arquitectura de seguridad multidominio, para consolidar una doctrina nacional de ciberseguridad marítima, articulada con la inteligencia estratégica y la soberanía digital, lo que permitirá fortalecer la resiliencia institucional y garantizar la protección de los intereses marítimos, económicos y de seguridad del Estado colombiano.

Palabras clave: Ciberdefensa marítima; inteligencia estratégica; soberanía digital; resiliencia; cooperación internacional.

Abstract: Strategic intelligence and digital sovereignty have become fundamental pillars of Colombia's national and maritime defense in the face of emerging twenty-first century threats. In an environment where cyberspace constitutes a new domain of global confrontation, the Colombian Navy faces the challenge of integrating maritime cyber defense into its doctrine, organizational structure, and legal framework. Drawing on the international experiences of the United States, China, Russia, the European Union, and NATO, as well as the contributions of specialized think tanks, this analysis identifies the main challenges and opportunities the country faces in its transition toward a multidomain security architecture. The consolidation of a national maritime cybersecurity doctrine—articulated with strategic intelligence and digital sovereignty—will strengthen institutional resilience and ensure the protection of Colombia's maritime, economic, and national security interests.

Keywords: Maritime cyber defense; strategic intelligence; digital sovereignty; resilience; international cooperation.

check for updates

Citación: Garate, R. Inteligencia estratégica y soberanía digital: Desafíos y oportunidades para la Armada Nacional de Colombia *DERROTERO* 2025, 19 N°2, 1–14. https://doi.org/

Recibido: 07/10/2025
Revisado: 25/11/2025
Aceptado: 16/12/2025

1. Introducción

Vivimos en una era en la que los límites tradicionales del conflicto se han difuminado progresivamente. Las guerras contemporáneas ya no se libran exclusivamente mediante medios cinéticos —tanques, aeronaves o fragatas—, sino también a través de algoritmos, campañas sistemáticas de desinformación y ciberataques capaces de paralizar infraestructuras críticas, desorientar sistemas de navegación o comprometer los datos estratégicos de un Estado. En este contexto, el ciberespacio se ha consolidado como un nuevo teatro de operaciones, donde el poder no solo se mide por la superioridad militar convencional, sino también por la capacidad de anticipar, defender y responder frente a agresiones que trascienden las dimensiones físicas tradicionales (terrestre, marítima y aérea) para integrarse plenamente en los dominios espacial y cibernético.

Para Colombia, en su condición de país marítimo y bioceánico, con una posición geoestratégica relevante en el hemisferio occidental, este escenario plantea desafíos de seguridad particularmente complejos. Por un lado, el Estado continúa enfrentando amenazas persistentes asociadas a dinámicas tradicionales de seguridad, como el narcotráfico y la presencia de grupos armados organizados que afectan la estabilidad interna. Por otro, debe adaptarse simultáneamente a amenazas emergentes propias del siglo XXI —entre ellas, ciberataques, espionaje digital, manipulación informativa y competencia tecnológica entre potencias—, sin descuidar la previsión estratégica frente a eventuales riesgos externos.

En este entorno de creciente competencia estratégica, caracterizado por la disputa por el control de la información, la superioridad tecnológica y la protección de infraestructuras críticas, la Armada Nacional de Colombia enfrenta un reto estructural: profundizar su transformación doctrinal, tecnológica y humana con horizonte al año 2042. Este proceso implica fortalecer capacidades de inteligencia estratégica multidominio e integrar la ciberdefensa naval como un componente esencial de la proyección del poder marítimo, reconociendo la soberanía digital como un elemento fundamental para la defensa integral del Estado y la protección de los intereses marítimos nacionales.

Bajo esta premisa, la Política de Seguridad, Defensa y Convivencia Ciudadana 2022–2026 incorpora una concepción de seguridad humana y multidimensional, en la cual el ciberespacio es reconocido explícitamente como un dominio de defensa y las infraestructuras críticas como activos estratégicos de interés nacional. En este marco, el presente ensayo examina el papel de la inteligencia estratégica y la soberanía digital en la proyección del poder marítimo colombiano, articulando lecciones derivadas de conflictos contemporáneos, desarrollos doctrinales internacionales y los lineamientos de transformación institucional establecidos en el Plan Armada 2042.

2. Materiales y Métodos

El estudio adoptó un diseño descriptivo–analítico con alcance exploratorio, sustentado en la revisión sistemática de literatura especializada y en el análisis documental de fuentes estratégicas y doctrinales. A partir de este enfoque se examinaron aportes de la literatura académica en estudios estratégicos, seguridad internacional, ciberseguridad y teoría del poder marítimo, así como documentos de política pública, estrategias de defensa y marcos doctrinales relacionados con la planificación de capacidades multidominio. De igual manera, se incorporaron lecciones derivadas de conflictos contemporáneos y experiencias internacionales en materia de guerra híbrida, ciberoperaciones y protección de infraestructuras críticas.

La investigación se apoyó en fuentes secundarias de carácter académico, institucional y doctrinal, recopiladas mediante búsquedas sistemáticas en bases de datos académicas internacionales y repositorios especializados en seguridad y defensa. Se priorizaron publicaciones indexadas, libros especializados, informes de centros de pensamiento y documentos estratégicos oficiales, seleccionados según criterios de pertinencia temática, actualidad y reconocimiento académico o institucional.

La información recopilada fue analizada mediante técnicas de análisis de contenido cualitativo, lo que permitió identificar categorías analíticas vinculadas con la inteligencia estratégica multidominio, la soberanía digital, la ciberdefensa naval, la protección de infraestructuras críticas y la proyección del poder marítimo en entornos híbridos. Estas categorías fueron posteriormente examinadas en relación con el contexto estratégico colombiano, con el fin de identificar convergencias y desafíos frente a los desarrollos doctrinales internacionales.

El alcance del estudio se circunscribe al análisis estratégico, doctrinal y conceptual basado en fuentes abiertas, sin incluir información clasificada ni la evaluación operativa de capacidades militares específicas. No obstante, este enfoque permite desarrollar una interpretación académicamente fundamentada de los desafíos que enfrenta Colombia en materia de seguridad multidominio y defensa del ciberespacio, contribuyendo al análisis de la evolución del poder marítimo en el siglo XXI.

3. Resultados

El ciberespacio como nuevo escenario estratégico

Desde inicios del siglo XXI, el ciberespacio dejó de ser un dominio exclusivamente civil para transformarse en un campo de competencia estratégica entre los Estados, donde la disuasión, la inteligencia y la tecnología convergen en la redefinición del poder militar contemporáneo. La militarización del ciberespacio se ha materializado a través de la creación de comandos cibernéticos nacionales y la incorporación del dominio digital en las doctrinas de defensa y disuasión de las principales potencias mundiales.

Tal como sostiene Thomas Rid (2013), el ciberespacio "no ha sustituido la guerra, pero ha redefinido sus métodos", diluyendo la frontera entre espionaje, sabotaje y conflicto armado, generando un entorno híbrido donde la información se convierte en un instrumento de poder. Esta evolución demuestra que la guerra moderna ya no se libra únicamente en el terreno físico, sino también en las redes, sistemas y narrativas digitales, donde las ofensivas cibernéticas buscan paralizar la infraestructura del adversario antes de la primeras operaciones militares.

Los conflictos actuales en Ucrania y Medio Oriente confirman esta transformación estructural. En el caso de Ucrania (2022–presente), la guerra no comenzó con misiles, sino con ataques masivos de malware contra redes eléctricas, bancarias y sistemas de mando y control militar. Según informes de la Cyber Peace Institute y la CNA Corporation (2023), más del 70 % de las operaciones cibernéticas rusas se dirigieron contra infraestructuras civiles, evidenciando cómo el ciberespacio se ha convertido en una herramienta de guerra psicológica, logistica y moral. Sin embargo, la resiliencia digital ucraniana, basada en alianzas con actores privados y organizaciones internacionales como Microsoft, Starlink y la OTAN, permitió sostener la conectividad y el mando estatal durante la ofensiva rusa, demostrando que la redundancia tecnológica y la cooperación internacional son hoy tan determinantes como la artillería o la aviación (Microsoft, 2023; NATO CCDCOE, 2023).

En el conflicto entre Israel y Hamas (2023 - presente), la dimensión de la información ha alcanzado un protagonismo sin precedentes. La batalla no solo se libra en los cielos y las calles, sino también en las plataformas digitales, donde ambos actores han empleado ciberataques, propaganda y manipulación informativa para controlar la narrativa pública y moldear la percepción internacional del conflicto.

La superioridad en el ámbito comunicacional se ha consolidado como un factor decisivo, y la guerra de la información como un frente operacional legítimo. La lección estratégica para Colombia radica en la necesidad de desarrollar capacidades de inteligencia comunicacional y defensa cognitiva, orientadas a neutralizar campañas de desinformación, proteger la moral institucional y fortalecer la cohesión nacional (RAND Corporation, 2024).

Del mismo modo, las operaciones híbridas globales recientes, como el sabotaje de cables submarinos en el Mar del Norte, los ciberataques a infraestructuras energéticas europeas o el espionaje industrial a gran escala, confirman que la tendencia contemporánea busca "paralizar sin disparar", degradando las capacidades del enemigo mediante acciones encubiertas en dominios digitales y físicos interconectados. En este contexto, Colombia debe avanzar hacia una doctrina de seguridad multidominio, que incorpore la ciberdefensa marítima, el monitoreo del tráfico digital portuario, la protección de buques y la vigilancia satelital, fortaleciendo la resiliencia de su entorno estratégico marítimo y logístico (ENISA, 2023; EU Council, 2024).

En síntesis, la lección global es inequívoca, la ciberdefensa no puede ser reactiva. Las naciones que han resistido con éxito las agresiones híbridas son aquellas que cuentan con inteligencia anticipatoria, resiliencia tecnológica y cooperación internacional activa. Tal como advierte Ben Buchanan (2020), "la superioridad en el ciberespacio no radica en el ataque, sino en la anticipación". Para Colombia, ello implica consolidar un sistema de ciberinteligencia estatal integrado, que articule capacidades militares, civiles y privadas bajo un marco legal coherente con el Derecho Internacional Humanitario y los principios de los Manuales de Tallinn 1.0 y 2.0, garantizando que la defensa digital del Estado sea eficaz, legítima y sostenible.

De los conflictos contemporáneos se desprenden cinco lecciones relevantes para Colombia:

- La información es poder: la superioridad en la obtención, proceso, análisis y difusión de inteligencia oportuna determina la iniciativa estratégica, operacional y táctica de las Fuerzas Militares.
- La resiliencia digital salva vidas: Ucrania ha resistido porque tiene redundancia tecnológica y alianzas internacionales que suministran apoyo tecnológico y capacitación.
- La comunicación estratégica es defensa: controlar la narrativa reduce el impacto psicológico del enemigo en la comunidad internacional y la opinión pública nacional.
- Las alianzas son esenciales: ningún país puede defenderse solo en el ciberespacio.

- La ética en la inteligencia es un multiplicador de legitimidad: la defensa digital debe respetar la ley para sostener la confianza ciudadana y credibilidad.

Inteligencia estratégica y soberanía digital

La inteligencia estratégica representa el faro que guía la toma de decisiones en entornos de incertidumbre. Michael Lowenthal (2019) define la inteligencia como el proceso de convertir información dispersa en conocimiento útil para la toma de decisiones y accionar político y militar. En el siglo XXI, este proceso se amplía al dominio digital, el análisis de datos, patrones de comportamiento en redes, señales satelitales y las amenazas cibernéticas se convierten en antecedentes imprescindibles para la defensa nacional.

La soberanía digital, concepto trabajado por Laura DeNardis (2020), implica la capacidad del Estado para ejercer control sobre su información, infraestructuras críticas y datos. No solo se trata de proteger servidores, sino que de asegurar la autonomía del país frente a injerencias externas. En Colombia, esta soberanía desde el punto de vista naval, está estrechamente ligada al control marítimo, el sistema de vigilancia costera, los satélites de observación y las redes logísticas de los puertos forman parte de un ecosistema digital que sostiene la economía nacional. Una vulneración a estos sistemas podría paralizar el comercio, afectar la seguridad alimentaria o incluso comprometer operaciones militares. Por tanto, la inteligencia estratégica debe tener la capacidad de anticipar ciberamenazas marítimas, identificar actores hostiles y fortalecer la resiliencia digital de la nación.

El ciberespacio marítimo: frontera invisible de la defensa nacional

El concepto de ciberespacio marítimo ha cobrado relevancia en las últimas dos décadas, especialmente en la doctrina de la OTAN y la International Maritime Organization (IMO). Este término alude a la red de infraestructuras digitales que sustentan el dominio marítimo como sistemas de navegación (GNSS), sensores costeros, radares, buques autónomos, bases logísticas y comunicaciones navales.

La OTAN, en su Cyber Defence Pledge (2021), reconoce que los mares y el ciberespacio están interconectados, y un ataque a un puerto o a un sistema de navegación satelital puede tener el mismo impacto que una incursión armada. Las lecciones aprendidas en ejercicios como Locked Shields (Cooperative Cyber Defence Centre of Excellence, Estonia) han demostrado que la protección del entorno marítimo requiere coordinación entre inteligencia, ciberdefensa y seguridad portuaria.

En el caso colombiano, esta perspectiva cobra una relevancia crítica. Los puertos de Cartagena, Buenaventura y Santa Marta son nodos estratégicos de comercio y defensa; y al mismo tiempo, son potenciales blancos de espionaje económico o sabotaje digital.

Junto a lo anterior, no hay que dejar de lado la posición geoestratégica de Colombia, la cual con el acceso al Mar Caribe y Océano Pacífico, la convierte en un punto de conexión ideal para la infraestructura de cables submarinos para la conectividad global, existiendo a la fecha diez puntos de aterrizaje operativos de estos cables y se proyectan en incremento aun mayor en los próximos años.

Por tanto, proteger el ciberespacio marítimo significa proteger la soberanía económica, la defensa territorial y la integridad nacional.

Amenazas híbridas en el ciberespacio marítimo

En los últimos años, el dominio marítimo se ha consolidado como uno de los entornos más vulnerables frente a las amenazas cibernéticas emergentes. La creciente digitalización de los sistemas portuarios, buques y cadenas logísticas ha generado un aumento de los ciberataque sin precedentes, transformando la seguridad marítima en un desafío tanto tecnológico como estratégico. Diversos informes y estudios académicos coinciden en que los ciberataques en este sector han evolucionado desde incidentes de bajo impacto hacia operaciones complejas dirigidas contra infraestructuras críticas, redes de control industrial (OT/ICS) y sistemas de navegación satelital (GNSS) (Meland, 2020; MDPI, 2024).

Casos emblemáticos como el ataque de ransomware a Transnet en 2021, que paralizó los puertos sudafricanos de Durban y Ciudad del Cabo, demuestran la capacidad disruptiva de este tipo de agresiones sobre la economía marítima global (Wikipedia, 2021). Asimismo, el informe de la United States Coast Guard (USCG) advierte que actores estatales como China y Rusia, así como organizaciones criminales transnacionales, han incrementado su actividad ofensiva en este ámbito, aprovechando la dependencia tecnológica de los sistemas de transporte marítimo (U.S. GAO, 2024).

A nivel técnico, los ataques más frecuentes incluyen la infección por vectores de ataque como malware, denegación de servicio (DDoS), manipulación de datos AIS, suplantación de señales GNSS y sabotaje de redes portuarias (MDPI, 2024; ArXiv, 2023). Estos incidentes revelan la brecha existente entre la digitalización del sector y su preparación cibernética, pues gran parte de las navieras y terminales portuarios aún carecen de protocolos sólidos de gestión de riesgos o mecanismos de intercambio de inteligencia (CyberOwl, 2023).

En consecuencia, los analistas del Atlantic Council y del Center for Naval Analyses (CNA) insisten en la necesidad de una estrategia internacional de ciberseguridad marítima basada en la cooperación público-privada, la resiliencia estructural y la protección del comercio marítimo global.

En suma, los ciberataques en el ámbito marítimo no solo representan una amenaza operativa, sino que se han convertido en un vector geopolítico de poder y coerción que redefine la seguridad marítima contemporánea (Atlantic Council, 2022; CNA, 2021).

En el caso colombiano, los grupos armados al margen de la ley y el narcotráfico sigue siendo las principales amenazas a la seguridad nacional de Colombia. Sin embargo, su evolución tecnológica los convierte hoy en actores híbridos. Los grupos criminales utilizan sistemas de comunicación cifrada, inteligencia de fuente abierta (OSINT), manipulación de señales satelitales (spoofing) para evadir la detección de las autoridades, y en los últimos años, drones con explosivos para atacar a las Fuerzas Militares. Además, emplean redes financieras digitales y criptomonedas para lavar activos a escala global.

El ciberespacio marítimo es una extensión natural de su operación. Los narcosubmarinos y las embarcaciones rápidas usan tecnologías GPS alteradas, drones y sistemas autónomos para el transporte de drogas. La inteligencia naval, por tanto, debe incluir la ciberinteligencia operativa que permita analizar patrones de tráfico digital, intercepción de comunicaciones en red, rastreo financiero y análisis de datos marítimos.

En regiones como el Pacífico y el Caribe, los grupos armados también buscan controlar rutas marítimas y puertos, financiando sus actividades mediante el narcotráfico. De allí que la defensa del ciberespacio marítimo no sea solo una cuestión tecnológica, sino un asunto de seguridad nacional y soberanía económica.

Experiencia Internacional

En el contexto estratégico de los Estados Unidos, la ciberdefensa marítima es concebida como un componente esencial dentro de una estrategia multidominio, en la que las capacidades cibernéticas respaldan la superioridad naval, la protección de la cadena logística global y la resiliencia de las fuerzas marítimas ante amenazas híbridas.

El Departamento de Defensa (DoD) y el Departamento de la Marina (U.S. Navy) han institucionalizado diversas estrategias y líneas de esfuerzo orientadas a integrar el ámbito cibernético con las operaciones marítimas tradicionales, reconociendo que el dominio digital es hoy un factor determinante para garantizar la ventaja operativa en el teatro naval (U.S. Department of War, 2021).

Entre los principales objetivos de esta política destacan el aseguramiento de la disponibilidad y resiliencia de los sistemas C4ISR navales que comprenden las redes de mando, control, comunicaciones, inteligencia, vigilancia y reconocimiento, la protección de infraestructuras críticas tales como puertos, sistemas de control industrial (OT/ICS), enlaces satelitales y sistemas globales de navegación (GNSS), y el mantenimiento de capacidades de atribución y respuesta que permitan disuadir, responder y neutralizar acciones hostiles en el ciberespacio marítimo (U.S. Department of War, 2021).

En el plano operativo, la estrategia estadounidense impulsa acciones prácticas de ciberresiliencia como la implementación de principios de “defensa por diseño” en plataformas navales, buques y redes de mando; el fortalecimiento de los equipos de respuesta a incidentes (CSIRT/NCIRC) y de los mecanismos de colaboración público–privada entre la Guardia Costera (USCG), el Departamento de Seguridad Nacional (DHS) y la industria marítima; así como la ejecución de ejercicios conjuntos y de cooperación internacional con aliados estratégicos para asegurar la interoperabilidad tecnológica y doctrinal en escenarios marítimos de conflicto. En su conjunto, estas acciones reflejan un enfoque integral de seguridad cibernética marítima, que trasciende la protección de sistemas informáticos para convertirse en un elemento estructural de la doctrina naval y de la política de defensa global de los Estados Unidos (U.S. Department of War, 2021).

En la doctrina y el análisis estratégico ruso, el ciberespacio se conceptualiza como una extensión natural del combate y guerra de información, integrado en un entorno de herramientas de presión híbrida que potencia la eficacia de las fuerzas navales y militares convencionales.

Moscú privilegia el empleo de ciberoperaciones como elementos de coerción, espionaje y sabotaje técnico, buscando denegar servicios, manipular percepciones y degradar infraestructuras críticas adversarias. Esta aproximación enfatiza la convergencia de capacidades informacionales, guerra electrónica y operaciones cibernéticas con campañas de desinformación y el uso de actores estatales y paraestatales para ampliar el espectro operativo más allá del campo de batalla tradicional.

En el ámbito marítimo, las prioridades rusas incluyen técnicas destinadas a degradar sensores y sistemas de vigilancia, desde interferencias en comunicaciones y GNSS hasta ataques a cables submarinos y plataformas de monitoreo, con el objetivo de minar la conciencia situacional adversaria y asegurar ventajas operativas en entornos de baja visibilidad jurídica y política.

Por su parte, en la doctrina militar de la República Popular China, la guerra cibernética y la guerra electrónica se conciben como componentes centrales de lo que el Ejército Popular de Liberación (EPL) define como "guerra informatizada" y, más recientemente, "guerra inteligente". Bajo esta visión, el poder naval chino, integra de manera sinérgica las capacidades cibernéticas, electrónicas y espaciales con el propósito de garantizar la superioridad informacional en el dominio marítimo y negar al adversario el uso efectivo de sus sensores, sistemas de mando y comunicaciones. Este enfoque, descrito como una estrategia de "control y denegación por capas", busca crear un entorno operativo donde China pueda proteger sus líneas marítimas de suministro y, simultáneamente, degradar la conciencia situacional y la capacidad de reacción de fuerzas hostiles en escenarios de crisis regional o global (U.S. Army Training and Doctrine Command [TRADOC], 2021).

Entre sus principales objetivos estratégicos, la doctrina china prioriza la protección de sus rutas marítimas críticas, la interrupción de la cadena de mando enemiga y el desarrollo de capacidades ofensivas y defensivas integradas, que combinen acciones cibernéticas, electrónicas y cinéticas para lograr la supremacía informacional. En el ámbito práctico, ha invertido de forma sostenida en guerra electrónica naval, ciberinteligencia y protección de activos espaciales y marítimos, incluyendo constelaciones satelitales, plataformas de reconocimiento y sistemas autónomos de vigilancia.

Asimismo, la estrategia china enfatiza el fortalecimiento de su industria tecnológica nacional, con el objetivo de desarrollar soluciones de defensa integradas y reducir la dependencia de tecnologías extranjeras, reforzando así su autonomía estratégica y su capacidad para sostener operaciones multidominio en entornos disputados.

En conjunto, la política cibernético-marítima de China refleja una proyección de poder sustentada en la información, la resiliencia tecnológica y la disuasión activa, componentes esenciales de su ascenso como potencia global (TRADOC, 2021).
Otros actores internacionales como la Unión Europea (UE) y la Organización Marítima Internacional (IMO) han adoptado un enfoque regulatorio y de gestión del riesgo frente a las amenazas cibernéticas que afectan al transporte marítimo global.

A diferencia de las estrategias de defensa militar o de proyección geopolítica, la aproximación conjunta de la Unión Europea privilegia la seguridad, continuidad y resiliencia del comercio y la navegación marítima, considerando la ciberseguridad como un componente esencial de la protección del tráfico marítimo civil y de la infraestructura logística global.

La IMO, como organismo especializado de las Naciones Unidas, ha desarrollado un marco normativo que obliga a los Estados miembros y a las empresas navieras a incorporar la gestión del riesgo cibernético dentro de los sistemas de seguridad de buques y puertos, integrando medidas de prevención, detección y respuesta ante incidentes que puedan afectar la navegación, los sistemas de control industrial (OT/ICS) y las cadenas logísticas portuarias (Organización Marítima Internacional, 2021).
Los objetivos estratégicos de este enfoque se centran en la homologación de estándares internacionales de gestión de riesgo, la reducción de la superficie de ataque

en los sistemas tecnológicos marítimos y la promoción de la colaboración público–privada mediante esquemas de certificación y auditoría de buenas prácticas. En ese sentido, tanto la IMO como la UE han elaborado y difundido guías y recomendaciones específicas**,** como las *IMO Guidelines on Maritime Cyber Risk Management* y el *EU Maritime Cyber Security Guidance*, orientadas a fortalecer la cultura de seguridad digital en el sector marítimo. Estas directrices establecen procedimientos para la evaluación y mitigación de riesgos, la elaboración de inventarios de activos críticos, la realización de auditorías periódicas de seguridad cibernética y la implementación de protocolos de respuesta y recuperación ante incidentes en puertos y buques.

En el caso europeo, la Estrategia de Ciberseguridad de la UE (2020) y la Directiva NIS2 consolidan este marco mediante la obligación de adoptar políticas de protección digital en el transporte marítimo, garantizando la interoperabilidad normativa entre los estados miembros y su alineación con los estándares técnicos internacionales definidos por la IMO. En conjunto, este enfoque regula la ciberseguridad marítima como una responsabilidad compartida entre autoridades, operadores y proveedores de servicios, buscando salvaguardar no solo la navegación, sino la estabilidad económica y logística del comercio global (Organización Marítima Internacional, 2021; European Union Agency for Cybersecurity [ENISA], 2022).

Por su parte, la Organización del Tratado del Atlántico Norte (OTAN), desde 2016 ha consolidado la ciberdefensa como uno de los pilares estratégicos de su estructura de seguridad colectiva. En su NATO Cyber Defence Strategy (2023), la Alianza Atlántica reconoce formalmente que los ciberataques pueden, bajo determinadas circunstancias, activar el Artículo 5 del Tratado del Atlántico Norte (OTAN) de 1949, referido al principio de defensa colectiva, equiparándolos a un ataque armado contra todos los Estados miembros. Este reconocimiento marcó un punto de inflexión doctrinal al situar el ciberespacio como un dominio operativo autónomo, al mismo nivel que los dominios terrestre, aéreo, marítimo y espacial (NATO, 2023). En consecuencia, la OTAN ha desarrollado uno de los modelos más avanzados de defensa cibernética del mundo, cuya estructura, enfoque y

resultados ofrecen lecciones directamente aplicables a las fuerzas armadas latinoamericanas, en particular a la Armada Nacional de Colombia.

La primera gran lección del modelo OTAN es la integración multinivel. La Alianza entiende la ciberdefensa como una responsabilidad compartida entre actores militares, civiles y privados. Los Estados miembros coordinan fuerzas armadas, agencias gubernamentales, academia e industria tecnológica bajo una arquitectura común de seguridad digital. Este esquema supera la fragmentación institucional tradicional y permite una respuesta unificada y sinérgica frente a amenazas híbridas. En el contexto colombiano, esta experiencia resulta especialmente relevante: la integración del Comando Conjunto Cibernético (CCOCI) con la Armada, las demás Fuerzas Militares, la Policía Nacional, el Ministerio de Defensa, la Dirección Nacional de Inteligencia y el sector tecnológico permitiría articular un ecosistema de ciberseguridad nacional con visión estratégica y de defensa integral**.**

El segundo aprendizaje deriva del modelo de capacitación continua desarrollado por el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE), con sede en Tallin, Estonia. Allí, la OTAN entrena permanentemente a sus especialistas mediante ejercicios multinacionales como Locked Shields o Cyber Coalition, que simulan escenarios reales de ataque y respuesta. Este enfoque formativo demuestra que la preparación constante es la forma más eficaz de disuasión. Siguiendo esta línea, Colombia podría implementar un Centro de Entrenamiento en Ciberdefensa en el marco del CCOCI, orientado a la simulación de incidentes, análisis de inteligencia técnica y operaciones híbridas, fortaleciendo así la capacidad doctrinal, técnica y operativa del personal de las Fuerzas Militares.

La tercera lección clave de la OTAN es la interoperabilidad doctrinal y tecnológica entre aliados. La Alianza ha desarrollado normas comunes que aseguran que las capacidades digitales de cada nación puedan operar conjuntamente, desde los estándares de cifrado y comunicación segura hasta los protocolos legales y operacionales de respuesta conjunta. En el caso colombiano, la adopción progresiva de doctrinas interoperables con la OTAN, especialmente en los ámbitos de inteligencia marítima y ciberdefensa naval, fortalecería su cooperación internacional y aumentaría su capacidad de disuasión estratégica en escenarios regionales y globales.

En suma, la experiencia OTAN ofrece un modelo integral que combina doctrina, tecnología y gobernanza multinivel, capaz de traducirse en un marco adaptativo para las fuerzas navales y de defensa cibernética de Colombia (AP News, 2023; NATO, 2023). Y para Colombia, país socio global de la OTAN desde 2018, estas lecciones son valiosas. La Armada puede fortalecer su cooperación técnica, intercambio de inteligencia y participación en ejercicios multinacionales, aumentando así su resiliencia y capacidad de respuesta.

En el contexto regional, la Junta Interamericana de Defensa (JID), órgano técnico asesor de la Organización de los Estados Americanos (OEA) en materia de defensa y seguridad hemisférica, conceptualiza la ciberdefensa en forma integral y no hace diferencias entre los dominios operacionales (terrestre, marítimo, aéreo, espacio y ciberespacio). No obstante lo anterior, ha promovido una guía práctica de ciberdefensa militar orientada a fortalecer las capacidades institucionales de los Estados miembros frente al creciente espectro de amenazas en el ciberespacio.

La JID concibe la ciberdefensa como un componente esencial del proceso de transformación militar, donde la interoperabilidad, la cooperación regional y el respeto a las normas del Derecho Internacional y los Derechos Humanos son pilares fundamentales. Bajo este enfoque, se busca no solo modernizar las fuerzas armadas, sino también asegurar que sus capacidades cibernéticas sean proporcionales, coordinadas y legítimas, en consonancia con los principios democráticos y de transparencia regional (JID, 2023).

Los objetivos estratégicos incluyen el establecimiento de directrices comunes para el desarrollo de capacidades de ciberdefensa militar ajustadas al nivel de riesgo y madurez tecnológica de cada país; la promoción de ejercicios conjuntos y multilaterales que faciliten el intercambio de experiencias y buenas prácticas; y la consolidación de principios legales y éticos que orienten las operaciones cibernéticas de las fuerzas armadas en entornos complejos. De este modo, la JID impulsa un marco cooperativo que busca armonizar los esfuerzos nacionales y promover la confianza mutua en el dominio cibernético, aspecto crítico en un hemisferio caracterizado por diferentes niveles de desarrollo tecnológico y capacidades defensivas.

En el plano operativo, ha implementado cursos, programas de entrenamiento y guías técnicas destinados a fortalecer las competencias de los mandos militares, analistas de inteligencia y equipos técnicos encargados de la defensa digital. Además, fomenta la planificación de ejercicios bilaterales y multilaterales para el manejo coordinado de incidentes cibernéticos, así como la elaboración de planes nacionales de preparación y respuesta que integren los ámbitos civil, militar y académico. Estas acciones reflejan un esfuerzo sostenido por consolidar una cultura de ciberdefensa cooperativa en América, basada en la formación continua, la interoperabilidad tecnológica y el alineamiento doctrinal con los estándares internacionales en materia de seguridad digital y defensa colectiva (OEA, 2023).

En el ámbito de la reflexión estratégica y la investigación aplicada, diversos centros de pensamiento y análisis militar, como el Atlantic Council, el Center for Naval Analyses (CNA), el Center for Strategic and International Studies (CSIS) y el Cooperative Cyber Defence Centre of Excellence (CCDCOE), han contribuido de manera decisiva a la construcción del concepto de "maritime cyber domain". Este enfoque concibe al entorno marítimo digital como un sistema socio-técnico interconectado, en el que los subsistemas, buques, puertos, redes logísticas, sistemas de carga y cables submarinos, forman parte de una arquitectura de "sistema de sistemas" cuya seguridad depende de la cooperación integral entre actores públicos y privados. Desde esta perspectiva, la ciberseguridad marítima no puede abordarse como una función aislada de defensa, sino como un ecosistema global que requiere políticas coordinadas, inteligencia compartida y mecanismos de resiliencia transnacional.

Autores de la literatura académica contemporánea, como Thomas Rid y Ben Buchanan, complementan este marco al ofrecer modelos analíticos sobre la atribución, la disuasión y la normatividad jurídica aplicable a las operaciones cibernéticas, introduciendo la noción de "guerra informacional marítima" como un fenómeno híbrido que combina dimensiones técnicas, legales y estratégicas. Estos aportes teóricos han permitido comprender con mayor precisión los desafíos de la atribución técnica en incidentes cibernéticos, especialmente en espacios marítimos internacionales, así como la necesidad de reglas de comportamiento responsable y transparencia operativa entre los Estados (Rid, 2013; Buchanan, 2020).

Los objetivos estratégicos identificados por estos think-tanks apuntan, en primer lugar, a reducir la superficie de ataque a lo largo de la cadena logística marítima (buques, puertos y sistemas de carga), adoptando un enfoque preventivo de seguridad por diseño. En segundo lugar, proponen mejorar las capacidades de atribución y el intercambio de inteligencia entre sectores público y privado, fomentando la cooperación internacional para la identificación temprana de amenazas. Finalmente, enfatizan el fortalecimiento de la resiliencia y redundancia operativa, promoviendo el uso de sistemas alternativos al GNSS, soluciones de respaldo satelital y la segmentación entre redes OT e IT, como medidas de mitigación ante ataques disruptivos (Atlantic Council, 2022).

Entre las acciones y prácticas recomendadas, destacan la implementación de auditorías periódicas, la realización de ejercicios de simulación y respuesta a incidentes, la formalización de acuerdos público–privados para la protección de infraestructuras críticas y el desarrollo de programas de formación especializada en ciberseguridad marítima y logística digital. Estas medidas reflejan una visión pragmática orientada a la construcción de resiliencia estructural dentro de la economía marítima global, entendiendo que el dominio cibernético es ya un componente inseparable del poder marítimo y de la seguridad colectiva internacional (Atlantic Council, 2022; CNA, 2021).

Una Armada Nacional multidominio para el Siglo XXI

El Plan de Transformación Naval 2042 de la Armada Nacional proyecta una fuerza moderna, interoperable y tecnológicamente avanzada. Plantea la necesidad de desarrollar capacidades en el dominio marítimo, aéreo, espacial y cibernético.

Dentro de esta visión, la inteligencia estratégica adquiere una función transversal orientada a la toma de decisiones, integrar fuentes y fortalecer la seguridad de la información.

Este plan contempla:

- Modernización tecnológica integral, con énfasis en sistemas autónomos, inteligencia artificial y ciberseguridad operacional.
- Integración de la doctrina relacionada con la ciberdefensa marítima, orientada a proteger el ciberespacio marítimo, las comunicaciones satelitales y la infraestructura portuaria.
- Reingeniería organizacional, donde la inteligencia estratégica se consolida como eje de planeamiento y apoyo a operaciones.
- Fomento del talento humano especializado, formando oficiales y analistas en ciberinteligencia, derecho cibernético y análisis de amenazas híbridas.

El Plan 2042 reconoce explícitamente el ciberespacio como un "campo de operaciones emergente" y propone consolidar la doctrina de Ciberdefensa Marítima, que combine ciberinteligencia, guerra electrónica, vigilancia marítima y operaciones especiales. Esta transformación está alineada con la tendencia global hacia las operaciones multidominio, donde el mar, la tierra, el aire, el espacio y el ciberespacio se integran en un único teatro de operaciones.

Retos estratégicos y jurídicos

Colombia cuenta con un marco jurídico relevante en materia de inteligencia, ciberseguridad y ciberdefensa, sustentado en instrumentos como la Ley 1621 de 2013 sobre inteligencia y contrainteligencia, el CONPES 3701 de 2011 y la Política de Seguridad Digital y Ciberdefensa 2022–2026 (PSDCC).

Sin embargo, persisten vacíos estratégicos y jurídicos sustanciales que limitan la capacidad del Estado para enfrentar con eficacia los desafíos del ciberespacio. Uno de los principales problemas radica en la ambigüedad normativa sobre el uso de la fuerza en el ciberespacio y los mecanismos de atribución de ataques, ya que no contempla expresamente las operaciones defensivas, de inteligencia en el ciberespacio o de respuesta cibernética, lo que genera incertidumbre sobre la legitimidad del empleo de medios militares en dominios digitales. Esta falta de claridad obstaculiza tanto la acción jurídica como la operativa, dejando al Estado en una posición de vulnerabilidad ante ciberagresiones externas y/o internas.

En consecuencia, resulta imperativo actualizar el marco legal nacional a la luz de los principios de los Manuales de Tallinn y la Guía Hemisférica de Ciberdefensa de la Junta Interamericana de Defensa (JID), los cuales establecen criterios de proporcionalidad, necesidad, atribución responsable y respeto al derecho internacional humanitario (JID, 2023; Schmitt, 2017).

Otro desafío estratégico se relaciona con la fragmentación institucional del ecosistema de ciberdefensa colombiano, actualmente dividido entre el sector militar, civil y privado. La Armada Nacional, las demás fuerzas militares, el Comando Conjunto Cibernético (CCOCI), la Policía Nacional y la Dirección Nacional de Inteligencia (DNI) operan bajo agendas parciales y canales limitados de interoperabilidad, lo que dificulta una respuesta articulada frente a incidentes cibernéticos complejos. Ante ello, la creación de un Centro Nacional de Inteligencia Cibernética Marítima, bajo liderazgo conjunto, permitiría integrar capacidades, optimizar recursos, fortalecer alertas tempranas y facilitar el intercambio de conocimiento técnico y doctrinal entre fuerzas, alineando la política nacional con los modelos de cooperación hemisférica impulsados por la OEA y la JID (OEA, 2023).

Asimismo, la escasez de talento humano especializado en ciberinteligencia, análisis de datos, inteligencia artificial y derecho digital constituye un obstáculo estructural para la consolidación de una defensa cibernética integral. La formación de oficiales, suboficiales y analistas en estos campos sigue siendo limitada, a pesar de iniciativas como el Plan de Capacitación en Ciberinteligencia de la Armada 2023–2030, que promueve la profesionalización del personal militar en alianzas con universidades, centros tecnológicos y think tanks estratégicos. Este esfuerzo debe intensificarse, incorporando perspectivas éticas, jurídicas y tecnológicas que aseguren la responsabilidad y legitimidad del accionar cibernético estatal.

Finalmente, en el plano internacional, la adhesión de Colombia a los principios de la OTAN establecidos en sus Manuales de Tallinn y la Guía de la JID podría fortalecer la legitimidad, transparencia y coherencia de sus operaciones digitales dentro del marco del Derecho Internacional Humanitario (DIH), consolidando así su posición como actor responsable en la gobernanza global del ciberespacio.

Implementación de una Ciberseguridad Marítima en Colombia: Desafíos y Oportunidades

Para la Armada Nacional de Colombia, la implementación de una doctrina de ciberseguridad marítima representa tanto un desafío estructural como una oportunidad histórica para fortalecer su papel en la defensa nacional y regional. A partir de un enfoque multidimensional, estratégico, organizacional, tecnológico, jurídico, humano, cooperativo y de resiliencia, el país puede transitar de un modelo reactivo a una arquitectura de defensa digital proactiva, integrada y legítima frente al Derecho Internacional.

En ese contexto, se estima y propone que la implementación de una ciberseguridad marítima debe considerar a lo menos los siguientes siete factores o dimensiones:

Dimensión estratégica y doctrinal

El principal desafío estratégico para Colombia radica en la ausencia de una doctrina nacional de ciberdefensa marítima que reconozca el ciberespacio como un dominio operativo equiparable al terrestre o aéreo. Esta falta de definición limita la capacidad de coordinación entre la Armada, el Ministerio de Defensa y las agencias civiles. Sin embargo, esta brecha doctrinal constituye también una oportunidad única; la posibilidad de que la Armada lidere la formulación de una doctrina de ciberdefensa marítima, que integre soberanía digital, defensa nacional y seguridad marítima, permitiría consolidar una visión de ciberdefensa como elemento de soberanía, posicionando a Colombia como referente regional en la protección del dominio marítimo digital.

Dimensión organizacional y operativa

Desde el punto de vista organizacional, la fragmentación institucional entre la Armada, el Comando Conjunto Cibernético (CCOCI), la DIMAR y otras entidades militares y civiles dificulta una respuesta unificada ante incidentes cibernéticos. No obstante, esta misma situación abre la puerta para reconfigurar el sistema de defensa marítima mediante la creación de un Comando Naval de Ciberdefensa, con capacidad permanente de detección, respuesta y atribución de ataques. Tal estructura permitiría a la Armada liderar la interoperabilidad entre fuerzas, agencias y sector privado, convirtiéndose en el núcleo coordinador de la ciberinteligencia marítima nacional.

Dimensión tecnológica

El avance y continuo cambio tecnológico en materia de ciberseguridad naval, especialmente en la protección de redes C4ISR, sistemas GNSS, AIS y satelitales, constituye un desafío estructural. Sin embargo, la acelerada digitalización de las operaciones navales ofrece una oportunidad para implementar un modelo de "seguridad por arquitectura", integrando la ciberseguridad desde el diseño de cada sistema. La Armada puede promover el desarrollo de tecnologías soberanas y alianzas con universidades y empresas nacionales en inteligencia artificial, análisis predictivo o blockchain logístico, generando independencia tecnológica y fortaleciendo la autonomía estratégica digital del país.

Dimensión legal y normativa

El marco jurídico actual, centrado en la Ley 1621 de 2013 y el CONPES 3701, no regula con precisión las operaciones militares en el ciberespacio ni los criterios de atribución de ataques. Este vacío normativo limita la capacidad del Estado para actuar legítimamente en escenarios de conflicto híbrido. Pero también representa una oportunidad para la Armada de convertirse en actor técnico-jurídico clave en la actualización de la legislación nacional, incorporando principios de los manuales de Tallinn, la Guía de la Junta Interamericana de Defensa (JID) y los estándares de la OTAN. Ello fortalecería la legalidad, proporcionalidad y legitimidad de las operaciones digitales bajo el amparo del Derecho Internacional Humanitario.

Dimensión humana y formativa

La carencia de personal especializado en ciberinteligencia marítima, derecho digital y gestión de incidentes es un desafío que afecta la sostenibilidad operativa de la defensa cibernética. No obstante, esta situación se convierte en una oportunidad estratégica para que la Armada Nacional impulse la creación de centros de formación y certificación en ciberseguridad naval, integrando su Escuela Naval "Almirante Padilla" y la Escuela Naval de Suboficiales "ARC Barranquilla" con universidades, centros tecnológicos y aliados internacionales. La consolidación de una cultura institucional de seguridad de la información, en la que cada tripulante y analista asuma un rol activo en la defensa digital, puede convertir al factor humano en la primera línea de protección.

Dimensión de cooperación y alianzas internacionales

Aunque Colombia mantiene vínculos con la OTAN y la OEA, su participación en ejercicios internacionales de ciberdefensa marítima sigue siendo incipiente y limitada. Este déficit, sin embargo, ofrece una oportunidad valiosa para profundizar su cooperación multilateral. La Armada podría ampliar su participación en ejercicios conjuntos, programas de intercambio doctrinal y transferencia tecnológica, así como promover la creación de un Observatorio Hemisférico de Amenazas Cibernéticas Marítimas. Fortalecer la interoperabilidad doctrinal y técnica con aliados consolidaría a Colombia como socio confiable en la defensa regional del ciberespacio marítimo, más aún por si posición geoestratégica y acceso bioceánico.

Dimensión de desempeño y resiliencia

La falta de un sistema nacional de resiliencia digital marítima es uno de los desafíos más urgentes. Las infraestructuras portuarias y navales aún carecen de protocolos robustos de estandarizados de continuidad operativa y recuperación ante ataques cibernéticos. No obstante, la Armada tiene la oportunidad de diseñar una política de resiliencia adaptativa, basada en auditorías periódicas, simulacros y redundancia tecnológica. Adoptar métricas internacionales como NIST, ISO o ENISA permitiría medir la madurez institucional y proyectar a la Armada como modelo regional de resiliencia digital en defensa.

4. Discusión

El análisis realizado evidencia que el ciberespacio se ha consolidado como un dominio estratégico que transforma la naturaleza del conflicto contemporáneo, integrándose con los ámbitos terrestre, marítimo, aéreo y espacial. Los conflictos recientes demuestran que las operaciones militares actuales se desarrollan simultáneamente en dimensiones físicas, informacionales y digitales, donde los ciberataques, la manipulación de la información y las operaciones de inteligencia desempeñan un papel decisivo para afectar infraestructuras críticas, influir en la percepción pública y debilitar la resiliencia institucional de los Estados.

En este contexto, la superioridad informacional y tecnológica se configura como un factor central de la seguridad nacional. Las experiencias internacionales muestran que los países capaces de anticipar amenazas mediante inteligencia estratégica, mantener resiliencia tecnológica y fortalecer alianzas internacionales logran enfrentar con mayor eficacia las operaciones híbridas. En este escenario, la soberanía digital adquiere una importancia creciente, especialmente para aquellos Estados cuya economía depende de las redes logísticas y del comercio marítimo internacional. La interconexión entre puertos, sistemas de navegación, satélites y redes de comunicaciones conforma un ecosistema digital crítico cuya vulneración puede afectar la continuidad del comercio, la seguridad energética y la capacidad de respuesta del Estado.

Asimismo, el estudio destaca que el ciberespacio marítimo constituye una extensión emergente del dominio naval, donde convergen infraestructuras digitales, sistemas de navegación satelital, redes portuarias y cables submarinos de comunicaciones. La creciente digitalización del transporte marítimo ha ampliado las vulnerabilidades frente a actores estatales, criminales e híbridos, lo que evidencia la necesidad de fortalecer las capacidades de ciberseguridad en este entorno estratégico.

El análisis comparado de doctrinas internacionales muestra que las principales potencias y organismos multilaterales han incorporado el ciberespacio como un componente central de sus estrategias de seguridad, promoviendo modelos basados en resiliencia tecnológica, interoperabilidad y cooperación internacional. Estas experiencias resaltan la importancia de articular capacidades militares, civiles y privadas dentro de una arquitectura de seguridad digital integrada.

En el caso colombiano, la convergencia entre amenazas tradicionales —como el narcotráfico y los grupos armados ilegales— y amenazas emergentes de carácter tecnológico configura un escenario de riesgo híbrido que exige fortalecer las capacidades de inteligencia naval y ciberdefensa. En este marco, la transformación institucional proyectada en el Plan de Transformación Naval 2042 representa una oportunidad estratégica para integrar inteligencia estratégica, tecnologías emergentes y ciberseguridad en un enfoque multidominio.

No obstante, persisten desafíos asociados a la fragmentación institucional y a los vacíos normativos en materia de operaciones en el ciberespacio. La actualización del marco jurídico y la adopción de estándares internacionales resultan fundamentales para garantizar la legitimidad y eficacia de las operaciones de defensa digital.

En síntesis, la investigación concluye que la ciberseguridad marítima debe ser concebida como un componente esencial de la estrategia de defensa nacional, orientado a proteger la soberanía económica, la continuidad del comercio y la capacidad operativa del Estado. En este sentido, el fortalecimiento de la inteligencia anticipatoria, la resiliencia tecnológica y la cooperación internacional permitirá a Colombia avanzar hacia una arquitectura de ciberdefensa marítima integrada, capaz de responder a los desafíos de seguridad del siglo XXI.

5. Conclusiones

La transformación del entorno estratégico internacional evidencia que el ciberespacio se ha consolidado como un dominio central de la seguridad y la defensa contemporáneas. En este contexto, la defensa nacional colombiana enfrenta el desafío de adaptarse a un escenario en el que la competencia estratégica se desarrolla simultáneamente en los planos físico, informacional y digital. Bajo estas condiciones, la inteligencia estratégica y la soberanía digital emergen como componentes fundamentales para salvaguardar los intereses marítimos del Estado, garantizar la continuidad de las infraestructuras críticas y preservar la autonomía tecnológica nacional. En este proceso, la Armada Nacional de Colombia, dada su condición bioceánica y su responsabilidad en la protección del dominio marítimo, se perfila como un actor clave para liderar la construcción de una doctrina integral de ciberdefensa marítima que articule capacidades de inteligencia, disuasión, cooperación internacional y legitimidad jurídica en el entorno digital.

Los resultados del análisis indican que los desafíos identificados —entre ellos la ausencia de una doctrina consolidada de ciberdefensa marítima, la fragmentación institucional y los vacíos normativos existentes— no constituyen únicamente limitaciones estructurales, sino también oportunidades estratégicas para impulsar procesos de innovación doctrinal, organizacional y tecnológica. En este sentido, el fortalecimiento de estructuras especializadas de coordinación e inteligencia cibernética permitiría integrar de manera más eficaz las capacidades militares, civiles y académicas, favoreciendo una arquitectura de seguridad digital coherente y compatible con los estándares internacionales de interoperabilidad.

La evidencia comparada demuestra asimismo que la resiliencia digital, la cooperación multinivel y el intercambio de inteligencia constituyen factores determinantes para enfrentar las amenazas híbridas del siglo XXI. En este ámbito, Colombia dispone de un marco favorable para fortalecer sus capacidades mediante la profundización de la cooperación con aliados y organismos internacionales, así como mediante la adopción de estándares jurídicos y doctrinales compatibles con el derecho internacional aplicable al ciberespacio. Estos elementos contribuyen a consolidar la legitimidad y la eficacia de las operaciones de defensa digital dentro de un marco normativo transparente y predecible.

Desde la dimensión tecnológica, la creciente digitalización de los sistemas navales, portuarios y logísticos plantea simultáneamente nuevos riesgos y oportunidades. La incorporación de principios de ciberseguridad desde el diseño de las arquitecturas tecnológicas, junto con la adopción de herramientas avanzadas como inteligencia artificial, análisis predictivo y sistemas autónomos, puede fortalecer significativamente la resiliencia de la infraestructura marítima crítica. Del mismo modo, la articulación con universidades, centros de investigación y el sector tecnológico resulta esencial para impulsar capacidades nacionales de innovación y reducir la dependencia tecnológica externa.

En paralelo, el fortalecimiento del capital humano constituye un elemento estratégico para la consolidación de una arquitectura efectiva de ciberdefensa. La formación especializada en ciberinteligencia, análisis de datos, derecho digital y gestión de amenazas híbridas debe ocupar un lugar central en la planificación institucional, complementada por el desarrollo de una cultura organizacional orientada a la protección de la información y la seguridad digital.

En síntesis, la evolución del entorno estratégico confirma que la seguridad marítima contemporánea debe ser concebida desde una perspectiva multidominio, en la cual la información, la resiliencia tecnológica y la legitimidad jurídica adquieren una importancia comparable al poder naval convencional. En este marco, la consolidación de una doctrina nacional de ciberseguridad marítima, articulada con la inteligencia estratégica y la soberanía digital, representa una oportunidad para fortalecer la defensa integral del Estado y proyectar a Colombia como un actor relevante en la protección del dominio marítimo digital en el contexto regional e internacional.

Referencias

AP News. (2023, June). *NATO to strengthen cyber defence commitments after series of hybrid threats*. Associated Press.

Atlantic Council. (2022a). *Securing the maritime cyber domain: Policy recommendations for a connected ocean*. Atlantic Council Cyber Statecraft Initiative.

Atlantic Council. (2022b). *The cyber strategy and operations of Hamas: Green flags and green hats* (S. Handler). Atlantic Council.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Center for Naval Analyses. (2021). *Maritime cybersecurity: A systems approach to critical infrastructure protection*. CNA.

CNA Corporation. (2023). *Assessing Russian cyber and information warfare in Ukraine: Expectations, realities, and lessons*. CNA.

Cooperative Cyber Defence Centre of Excellence. (2022). *Tallinn papers on maritime cyber defence*. CCDCOE.

DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch*. Yale University Press.

European Commission. (2020). *The EU cybersecurity strategy for the digital decade*. Publications Office of the European Union.

European Union Agency for Cybersecurity. (2022). *Maritime cybersecurity: Good practices for cyber risk management and threat mitigation*. ENISA.

International Maritime Organization. (2021). *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3/Rev.2). IMO.

Junta Interamericana de Defensa. (2020). *Guía de ciberdefensa para las Américas*. Organización de los Estados Americanos.

Junta Interamericana de Defensa. (2023). *Guía hemisférica para el fortalecimiento de las capacidades de ciberdefensa militar*. Organización de los Estados Americanos.

Kania, E. B. (2019). *Battlefield singularity: Artificial intelligence, military revolution, and China's future military power*. Center for a New American Security.

Lowenthal, M. M. (2019). *Intelligence: From secrets to policy* (8th ed.). CQ Press.

Ministerio de Defensa Nacional de Colombia. (2022). *Política de seguridad, defensa y convivencia ciudadana 2022–2026*. Gobierno de Colombia.

North Atlantic Treaty Organization. (2023). *NATO cyber defence strategy 2023*. NATO Headquarters.

North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. (2023). *Locked Shields and Cyber Coalition exercises: Building resilience through practice*. CCDCOE.

Office of the Secretary of Defense. (2023). *Military and security developments involving the People's Republic of China 2023: Annual report to Congress*. U.S. Department of Defense.

Organización de los Estados Americanos. (2023). *Plan de acción del Comité Interamericano contra el Terrorismo (CICTE) sobre ciberseguridad y ciberdefensa*. OEA.

Organización de los Estados Americanos – Junta Interamericana de Defensa. (2022). *Memoria anual de la Junta Interamericana de Defensa 2022*. OEA.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

U.S. Army Training and Doctrine Command. (2021). *Chinese military power: Modernizing a force to fight and win*. TRADOC G-2.

U.S. Department of Defense. (2023). *2023 DoD cyber strategy*. U.S. Department of Defense.

U.S. Department of War. (2021). *Maritime cyber defense strategy and multidomain integration framework*. U.S. Government Printing Office.

Contribuciones de los autores:

Declaro haber realizado el total de las actividades inherentes a la concepción, diseño, recolección de datos, análisis e interpretación de resultados, y la redacción del manuscrito final. De tal manera, asumo la responsabilidad total del contenido aquí presentado en este trabajo de investigación.

Financiación: Declaro que esta investigación no recibió financiación externa.

Conflicto de Intereses: el autor declara no tener conflictos de interés alguno.

Biografía del Autor

Coronel (R) del Ejército de Chile del arma de Infantería. Es Licenciado en Ciencias Militares, Oficial de Estado Mayor, Especialista en Inteligencia Básica, Especialista en Inteligencia Especializada mención drogas, Especialista en Inteligencia Especializada mención técnicas especiales de investigación, Profesor Militar de Academia mención Geografía Militar y Geopolítica, Profesor Militar de Escuela mención conocimiento de armas y tiro y Profesor honorario de las Fuerzas Militares de Colombia.
Posee el título profesional de Abogado. Es licenciado en Ciencias Jurídicas, Magister en Planificación y Gestión estratégica, especialista en Docencia Universitaria, Diplomado en Seguridad Internacional y Estudios Estratégicos, Diplomado en Ciberseguridad, Diplomado en Geopolítica, Diplomado en gestión y Administración de Recursos y Proyectos de Defensa, Diplomado en Administración de Empresas y Diplomado en Docencia Universitaria Virtual.
Ha realizado Cursos de Capacitación Pedagógica, Investigación Profesional, Historia Militar, Orientación en Defensa Nacional y Toma de decisiones estratégicas comunicacionales en Seguridad y Defensa.
Ha ejercido la docencia por más de 20 años en instituciones de educación superior de pre y post grado en Chile y Colombia destacando:
En Chile: Escuela Militar, Escuela de Suboficiales, Escuela de Inteligencia, Academia de Guerra y Academia Politécnica Militar del Ejército de Chile. Universidad Mayor, Universidad de Concepción, Instituto de Estudios Internacionales de la Universidad de Chile, Instituto de Formación Técnica DUOC - UC de la Universidad Católica de Chile e Instituto Profesional San Sebastián de la Universidad San Sebastián.
En Colombia: Escuela Superior de Guerra, escuela de Inteligencias y Contrainteligencia del Ejército Nacional, Escuela de Inteligencia de la Fuerza Aeroespacial Colombiana y Universidad Externado.
Se ha especializado en las áreas de investigación del Derecho informático, planificación estratégica, geopolítica, inteligencia, ciberseguridad y ciberdefensa.