Inteligencia Artificial: oportunidades, desafíos y vulnerabilidades en la Armada Nacional de Colombia 2025 -2030.

Capitán de Corbeta Nelson Rodrigo Aldana Bohórquez

Artículo para optar al título profesional:

Magister en Seguridad y Defensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Capitán de Corbeta (ARC) Nelson Rodrigo Aldana Bohórquez
Identificación	**:**	88.033.398
Programa académico	**:**	Maestría en Seguridad y Defensa
Tutor metodológico	**:**	Jonathan Jiménez Reina
Tutor temático	**:**	Capitán de Navío (R) Héctor Rodríguez
Fecha de entrega	**:**	26 de agosto de 2025
Extensión	**:**	7955 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las FFMM de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-No Comercial-Sin Obras Derivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Inteligencia Artificial: oportunidades, desafíos y vulnerabilidades en la Armada Nacional de Colombia 2025 -2030.

Artificial Intelligence: opportunities, challenges and vulnerabilities for the Colombian Navy 2025-2030.

Nelson Rodrigo Aldana Bohórquez*

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este artículo analiza la integración de la inteligencia artificial (IA) en la Armada Nacional de Colombia (ARC), en el marco de la doctrina conjunta militar 2025-2030 y el entorno VICA-H (volatilidad, incertidumbre, complejidad, ambigüedad e hiperconectividad). El objetivo es evaluar las amenazas, oportunidades y desafíos que implica la adopción de IA en capacidades militares, tomando como referencia lecciones de la guerra ruso-ucraniana y el caso de ciberataques en Estonia. La metodología empleada consistió en un benchmarking de casos internacionales y una revisión documental de planes estratégicos y normativa vigente. Los resultados evidencian vulnerabilidades en comunicaciones y logística, así como la necesidad de optimizar los sistemas de información militar mediante infraestructura digital avanzada. Se concluye que la IA puede redefinir la superioridad operativa y requiere cerrar brechas tecnológicas, fortalecer la ciberseguridad y promover alianzas estratégicas para una transformación efectiva y ética en la defensa nacional.

Palabras clave: Benchmark, Doctrina Conjunta, Estrategia Militar, Inteligencia artificial, Joint Venture.

Abstract: This article examines the integration of artificial intelligence into the Surface Fleet in the National Navy of Colombia, within the framework of the joint military doctrine for 2025-2030 and the VICAH environment (volatility, uncertainty, complexity, ambiguity, and hyperconnectivity). The objective is to assess the threats, opportunities, and challenges associated with adopting AI in military capabilities, using lessons from the Russia-Ukraine war and the case of cyberattacks in Estonia as references. The methodology employed consisted of benchmarking international cases and conducting a documentary review of

*Capitán de Corbeta. Candidato a magíster en Seguridad y Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto". Magister en Administración de Negocios Universidad San Buenaventura, Especialista en Geopolítica y Estrategia de la Escuela Naval de Cadetes Almirante Padilla, Especialista en Gestión Gerencial de la Universidad de Cartagena e Ingeniero en Mecatrónica de la Universidad de Pamplona Colombia. https://orcid.org/0000-0003-2004-7466 - Contacto: nelson.aldana@esdeg.edu.co.

strategic plans and current regulations. The results highlight vulnerabilities in communications and logistics, as well as the need to optimize military information systems through advanced digital infrastructure. The study concludes that AI has the potential to redefine operational superiority, but it requires closing technological gaps, strengthening cybersecurity, and fostering strategic alliances for an effective and ethical transformation in national defense.

Keywords: Artificial Intelligence, Benchmark, Joint Doctrine, Joint Venture, Military Strategy.

Introducción

Alan Turing, en su artículo Computing Machinery and Intelligence (Turing, 1950), introdujo la idea de la capacidad de una máquina para exhibir un comportamiento inteligente equivalente o indistinguible de un humano.

La aceleración tecnológica transforma el entorno, optimiza procesos y redefine estilos de vida, afectando el equilibrio geopolítico global. La ley de Moore (Moore, 1965) anticipa un crecimiento exponencial en la potencia de cálculo, acercando la singularidad tecnológica y el desarrollo de una IA superior a la humana. Este escenario exige que Colombia y la ARC den un salto cuántico estratégico en el uso de IA y tecnologías emergentes, reduciendo la brecha tecnológica y fortaleciendo su competitividad. El dominio de esta tecnología será clave para la soberanía, la modernización operativa y la proyección regional.

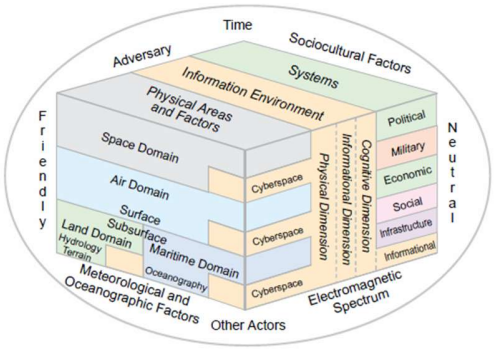
Es innegable que dichos desarrollos afectan la concepción clásica de la trilogía de Clausewitz (Clausewitz, 1977); la dinámica estratégica y la interacción entre el gobierno, las FFMM y la población al impactar nuevos dominios como: el ciberespacio y el espacio ultraterrestre, acelerando la toma de decisiones y requiriendo de una adaptación constante.

La Constitución Política de Colombia (Constituyente, 1991) establece en su artículo 217 que: "la Nación tiene unas Fuerzas Militares permanentes, que son el Ejército, la Armada y la Fuerza Aérea…" La visión es "ser una Armada de proyección e influencia regional, con tecnología y capacidades de avanzada para la defensa y seguridad, determinante para el desarrollo de los intereses nacionales, reconocida por su integridad y contribución al progreso del país". Es esencial establecer como la IA interactúa con la misión, la visión institucional y la estrategia naval militar al revolucionar la planificación y ejecución de operaciones navales del 2025 al 2030. De acuerdo con el Army War College en un entorno caracterizado

por ser volátil, incierto, complejo, ambiguo (Barber, 1992) y en concordancia con (Charlán, 2018) "el entorno VICA ha sido complementado con una "H" de Hiperconectividad… donde la tecnología ha cambiado casi todo y donde las capacidades digitales se han popularizado".

Comprender el Entorno Operacional exige una visión holística que integre sistemas, subsistemas y atributos PMESII políticos, militares, económicos, sociales, información, infraestructura (OTAN, 2014). figura1.

Figura 1. Visión holística del ambiente operacional



Fuente: JP 2-01.3

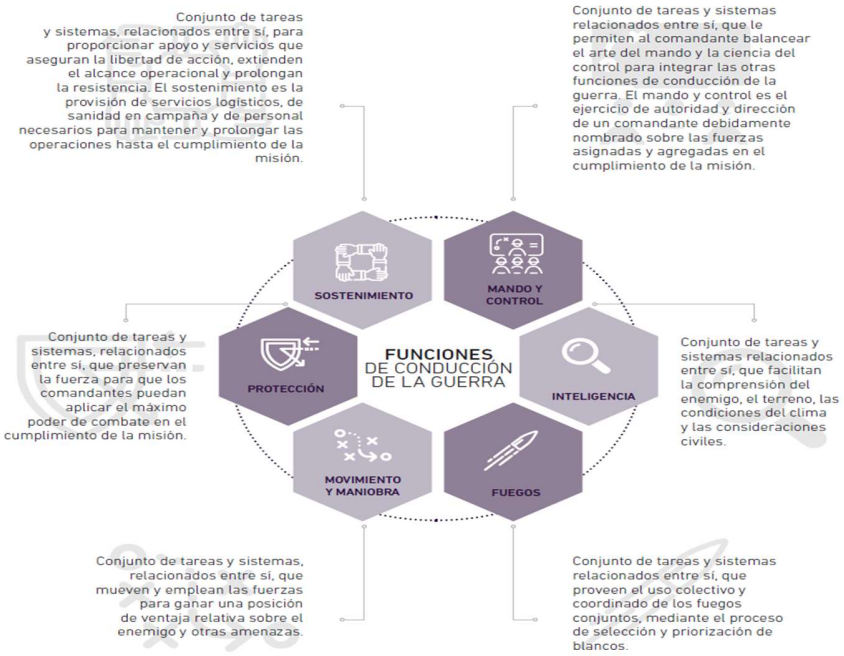
Según el MFC 1.0 (MDN, 2018), los dominios permiten describir y caracterizar el ambiente operacional. La IA fortalece todos los dominios de la guerra, optimizando la estrategia de la ARC. Figura 2.

Figura 2. Dominios de la guerra conjunta

Fuente: MFC 3-0

Las funciones de conducción de la guerra, definidas en el MFC 3-0 (FFMM, 2023), agrupan tareas, personas, procesos e información bajo un propósito común. Estas funciones están siendo transformadas por la acelerada evolución tecnológica, exigiendo adaptación doctrinal para garantizar eficiencia, respuesta oportuna y superioridad operacional.

Figura 3. Funciones de conducción de la guerra conjuntas



Fuente: Manual Fundamental Conjunto MFC 1-0

Durante la guerra del Golfo, EE.UU. empleó el sistema DART, una IA interactiva que permitió replanificar misiones militares en tiempo real, optimizando el despliegue de tropas y equipos en entornos de alta velocidad. El sistema pasó del concepto a la operación en solo 23 meses. Actualmente, la inversión global en IA militar se enfoca en mejorar la toma de decisiones, automatización y eficiencia operativa. Potencias como EE.UU, China y Europa priorizan sistemas autónomos, vigilancia, ciberseguridad y apoyo logístico para modernizar sus FFMM, expandir capacidades estratégicas y consolidar superioridad tecnológica en escenarios de combate dinámico. Según el Global Marketing Insights (Insights, 2025): "la inteligencia artificial global en tamaño del mercado militar fue valorada en USD 10.4 mil millones en 2024 y se estima que crecerá en 13,4% CAGR de 2025 a 2034". El creciente gasto militar es un factor clave para el crecimiento del mercado, ya que las

FFMM se centran en el análisis rápido de los datos para tomar decisiones rápidas en las operaciones.

Según (Martel-Carranza, 2023), "la IA es una tecnología fundamental en diversos sectores de la sociedad, la economía global e incluyendo la seguridad y defensa". Este articulo explora los aspectos más relevantes del estado actual de la IA, sus avances, aplicaciones, desafíos y como interactúa con la ARC, destacando las oportunidades, desafíos y vulnerabilidades para el 2025 - 2030.

Metodología

Con el fin de establecer las oportunidades, desafíos y vulnerabilidades de la ARC frente a la evolución de la IA en el 2025–2030, se efectuó desde un enfoque cualitativo, una revisión bibliográfica en diversas bases de datos científicas siguiendo la metodología formulada por Hernández-Sampieri, (Hernández et al., 2014), mediante un proceso no lineal, iterativo y recurrente para desarrollar la investigación.

Así mismo, se realizó un *benchmark* para identificar lecciones aprendidas que permitan afinar y mejorar la estrategia de la ARC frente a los avances en IA, tomando como referencia el conflicto entre Rusia y Ucrania, y el caso de Estonia, cuya infraestructura digital fue completamente paralizada por ciberataques en 2007.

Benchmark Rusia Ucrania

El conflicto iniciado en 2014 con la anexión de Crimea e intensificado en 2022 ha redefinido la guerra moderna, combinando fuerzas convencionales y no convencionales, propaganda, ciberataques y actores irregulares (Galeotti, 2016). Ha generado una crisis global y reactivado la amenaza nuclear (Cortes, 2023). Para el FMI la guerra en Ucrania se

ha convertido en terreno de ensayo tecnológico, evidenciando el uso eficaz de IA y drones, así como deficiencias en su adopción (Wagstaff, 2023). Las guerras de sexta generación integran tecnología avanzada y medios no cinéticos (Freedman, 2019). Para la ARC, este escenario ofrece lecciones clave en guerra híbrida, ciberseguridad y modernización operacional, especialmente ante amenazas como drones armados en el Catatumbo y Cauca, y campañas de deslegitimación en redes sociales.

Lecciones estratégicas

Integración de tecnologías avanzadas: los drones y herramientas de ciberseguridad optimizan la vigilancia de fronteras y fortalecen la protección de infraestructura crítica ante amenazas crecientes (minería y cultivos ilícitos).

Guerra híbrida: Implica la alfabetización mediática de la sociedad, el análisis y mitigación de vulnerabilidades y una gestión efectiva de crisis frente a ciberataques y campañas de desinformación.

Colaboración internacional: fortalecer y diversificar alianzas estratégicas, explotar la condición de socio global OTAN, revitalizar acuerdos de cooperación militar para acceder a tecnologías, entrenamiento especializado e impulsar clústeres de la industria de defensa.

Adaptabilidad y flexibilidad institucional: se debe promover para responder ágilmente a entornos cambiantes y amenazas de grupos criminales que aplican sistemas adaptativos complejos, fomentando una cultura de innovación, objetividad y apertura al pensamiento disruptivo.

Implicaciones para las ARC

La guerra ruso-ucraniana representa un laboratorio clave para el desarrollo y aplicación de nuevas tecnologías militares, el uso de IA, drones y municiones autónomas. Resulta urgente modernizar las capacidades de la ARC mediante la adopción de tecnologías avanzadas en robótica, big data, ciberdefensa, ciberataque, protección de infraestructuras críticas y computación cuántica.

Impacto los dominios de la guerra

Marítimo

El uso de drones por parte de Ucrania ha transformado los conflictos navales, afectando el control ruso en el mar Negro. Su eficacia, bajo costo y dificultad de detección fueron evidentes en el hundimiento del crucero Movska (News, 2022). Esta evolución exige que la ARC, como marina de proyección regional, reoriente sus capacidades hacia porta drones, como el modelo portugués, para proyectar poder, neutralizar amenazas y brindar cobertura de fuego. Además, se propone que Cotecmar desarrolle nuevas líneas de negocio en el Gesed, enfocadas en el diseño y construcción de flotas de drones no tripulados para fortalecer la soberanía marítima.

Terrestre

La guerra en Ucrania evidencia el impacto logístico y tecnológico en la defensa territorial. Rusia busca consolidar un corredor entre Crimea y Donbas, empleando incluso convictos a través del grupo Wagner, con más de 40.000 bajas reportadas (DW, 2023). La respuesta ucraniana combina estrategia, drones y defensa territorial activa. En Colombia, los grupos ilegales actúan como fuerzas proxy, representando una amenaza a la seguridad

nacional. Es imperativo afinar la estrategia militar, neutralizar estas estructuras y ampliar el uso de drones para reconocimiento, ataque y guerra electrónica, fortaleciendo así la capacidad operativa.

Aéreo

En un entorno de negación aérea, Rusia inició con ventaja numérica; sin embargo, Ucrania respondió con innovación tecnológica y uso masivo de drones. Las operaciones aéreas buscan destruir capacidades enemigas mediante ataques precisos. Según (CNN, 2025), el 1 de junio: "el ataque con drones de Ucrania contra aeródromos rusos fue audaz y osado", alcanzando 41 aeronaves, incluidos bombarderos estratégicos. Esta ofensiva demuestra cómo la tecnología puede compensar desventajas convencionales. Colombia debe fortalecer su superioridad aérea, reemplazar la flota Kfir, adquirir enjambres de drones con IA y actualizar doctrina y estrategia para garantizar una respuesta efectiva ante amenazas futuras.

Espacial

Aunque Ucrania no posee satélites propios, ha recibido apoyo occidental en inteligencia y reconocimiento, lo que ha sido clave para planificar operaciones y obtener ventajas tácticas. La guerra ha impulsado el desarrollo de tecnologías espaciales e IA, transformando la vigilancia y verificación mediante imágenes satelitales. Colombia debe reformular su estrategia de seguridad nacional, impulsar el sector privado para aprovechar la órbita geoestacionaria y crear una agencia espacial pública independiente de la FAC. Esta entidad gestionaría satélites propios con aplicaciones en defensa, agricultura, pesca, minería, gestión del riesgo y atención de desastres, fortaleciendo la soberanía tecnológica.

Ciberespacial (información)

La guerra moderna exige adaptación cibernética y cognitiva. Ucrania ha demostrado capacidades ofensivas y defensivas, integrando voluntarios en un ciber ejército que ubica y neutraliza mandos rusos mediante señales móviles. Rusia fracasó en su intento inicial de desactivar sistemas ucranianos. Paralelamente, la guerra cognitiva manipula percepciones, narrativas y apoyo internacional mediante IA y redes sociales. Colombia enfrenta polarización y desinformación diaria, por lo que debe fortalecer su liderazgo militar, crear una especialidad cibernética en la ARC y FFMM, impulsar la colaboración público-privada, y desarrollar contrainteligencia informativa y campañas de concientización nacional para proteger su soberanía estratégica.

Caso Estonia

El ciberataque de Rusia a Estonia en la primavera del 2007 afectó bancos, medios de comunicación y sitios gubernamentales. Ofrece un ejemplo de la naturaleza de la ciberguerra y la incertidumbre y ambivalencia existentes dentro de la comunidad internacional sobre cómo responder a esta clase de ataques (Barletta, 2017). Fue el primer ciberataque conocido contra la totalidad de un país, exponiendo las vulnerabilidades del país báltico a las disrupciones cibernéticas y a su vez poniendo en relieve las capacidades ofensivas de Rusia en el campo ciberespacial que dieron lugar a otros ataques posteriores como el de Georgia en 2008 y Ucrania. Previo al ataque, los ataques cibernéticos no habían sido considerados como una amenaza inminente para el Estado y/o sus ciudadanos. Este hecho marcó un punto de inflexión en la percepción del ciberespacio como un potencial dominio de operaciones y es relevante para interpretarlo como un antecedente que manifestó la necesidad de adoptar

medidas y desarrollar una estrategia de ciberdefensa, principalmente en el marco de la Unión Europea y específicamente en el de la Organización del Tratado del Atlántico Norte (OTAN).

Actualmente, Estonia ejecuta proyectos como X-Road (Xroad, 2025), que facilita el intercambio seguro de datos entre los sectores público y privado, constituyéndose en un ejemplo destacado de transformación digital inclusiva.

Resumen de Políticas y Estrategias sobre IA en Colombia

Se revisaron los documentos de políticas y estrategias públicas de IA y su interacción con la ARC. Los resultados obtenidos reflejan la creciente necesidad de integrar la IA dentro de las estrategias nacionales y su papel en la transformación tecnológica del país. Así mismo, se evidenció que la institución carece de políticas claras al respecto y cuenta tan sólo con algunos lineamientos en IA; lo que implica la necesidad de abordar el tema para gestionar los recursos que permitan la adopción de esta tecnología en los diferentes procesos de la Armada.

Tabla 1. Políticas y estrategias sobre IA en Colombia

Documento de Política Pública	Eje Central y Objetivo	Aplicación de la IA
Plan Nacional de Desarrollo 2022-2026 *"Colombia potencia mundial de la vida"*	**Fortalecimiento institucional y lucha contra la corrupción** Recuperar la confianza y fortalecer el vínculo entre el Estado y los ciudadanos.	**Detección de corrupción** Adopción de tecnologías disruptivas (Big data, IoT, blockchain) para identificar anomalías en la contratación pública.
Política de Seguridad, Defensa y Convivencia Ciudadana 2022-2026 *"Garantías para la Vida y la Paz"*	**Seguridad humana y protección de la vida** Desarrollar acciones multisectoriales, contextualizadas e integrales para proteger entornos rurales y urbanos.	**Fortalecimiento de la inteligencia** Uso de IA para potenciar la función de inteligencia y contrainteligencia, con el fin de desarticular grupos armados organizados y grupos delictivos.
Plan de Desarrollo Naval 2042 *"Una Armada innovadora para la defensa, la seguridad y el desarrollo de los intereses marítimos y fluviales del país"*	**Innovación tecnológica para la defensa, seguridad y desarrollo marítimo.** Adaptación a la cuarta revolución industrial y avances tecnológicos globales.	**Sistemas autónomos y análisis de datos** Implementación de buques con sistemas autónomos y semiautónomos para reducir accidentes, automatización de puertos y uso de Big data para mejorar la competitividad.
CONPES IA 4144	**Estrategia nacional de IA para el desarrollo sostenible.** Establecer un marco de política pública para convertir la IA en una herramienta clave para el desarrollo del país.	**Transformación social y económica** Medidas para el desarrollo sostenible y la transformación social a través de IA, con un presupuesto asignado de 479 mil millones de pesos.
Estrategia Nacional Digital 2023-2026	**Visión y prioridades en el uso de datos y tecnologías digitales:** Articular iniciativas para una transformación digital integral en el Gobierno.	**Integración y coherencia:** Contribución a los objetivos del PND, coordinación de iniciativas de política pública y seguimiento a la implementación de tecnologías digitales.

Fuente: elaboración propia

Desarrollo del objetivo 1 - Identificar las oportunidades que ofrece la evolución de la IA para la ARC 2025 –2030.

1.1 Madurez tecnológica

La ARC en su plan estratégico de tecnologías de la información y de las comunicaciones – (PETIC, 2023) determinó de acuerdo con el Marco de Transformación Digital para el Estado Colombiano, que su madurez tecnológica se encuentra iniciando el proceso de transformación digital; razón por la cual la adopción de la IA, la educación del talento humano especializado para su operación y la inversión en su infraestructura son una oportunidad de oro para dar el salto al nivel 4 "mejora continua", para lo cual se debe explorar diferentes fuentes de financiación, crear la especialidad militar de IA, así como la adquisición de equipos y redes para integrarla a todos los sistemas de comunicaciones, armas y Unidades.

Figura 4. Madurez digital ARC

Cuestionario para identificar la madurez																	
Tipo	#	Nombre Proceso	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17
Estratégicos	1	Comunicaciones estratégicas	1	2	2	1	1	4	1	2	2	2	1	1	1	1	0	1	1
	2	Planeamiento institucional	2	2	1	2	2	2	2	1	2	2	2	2	2	2	1	1	1
Misionales	3	Inteligencia Naval	2	3	1	1	1	4	1	2	1	2	1	1	1	3	3	1	1
	4	Operaciones Navales	1	2	1	2	1	3	2	2	3	3	3	1	2	0	0	1	0
	5	Acción Integral	2	3	1	3	2	2	2	3	2	3	4	2	2	2	2	2	2
Apoyo	6	Adquisiciones	3	3	4	3	3	3	4	2	2	3	4	4	3	4	4	3	4
	7	Financiero	2	2	2	2	2	2	3	2	3	3	2	2	3	2	2	2	2
	8	Servicios Apoyo	1	2	2	2	2	2	2	1	1	2	2	1	2	2	1	2	2
	9	Gestión Jurídica	3	3	2	3	3	2	2	2	2	3	3	2	2	3	2	2	1
	10	Educación	2	2	2	2	1	2	2	1	2	2	2	1	2	2	2	2	1
	11	Abastecimientos	1	2	2	1	1	4	2	1	2	2	2	1	1	1	1	1	1
	12	Mantenimiento	2	3	1	2	1	3	2	2	1	3	1	0	0	2	1	4	2
	13	Gestión TIC	2	2	1	3	2	1	2	2	2	3	3	2	2	2	1	2	1
	14	Administración Talento Humano	1	2	2	0	1	4	0	1	2	2	4	1	1	2	1	2	0
	15	Evaluación Independiente	1	2	2	3	1	3	2	2	2	2	2	2	2	2	3	2	2
		PROMEDIO ARMADA NACIONAL	*2*	*2*	*2*	*2*	*2*	*3*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*1*

Fuente: PETIC (2023)

1.2 Dominios y funciones de la guerra

La IA está transformando radicalmente las estrategias, tácticas y capacidades operacionales de las FFMM. Su aplicación se describe a continuación:

1.2.1 Dominio Marítimo

Mando y control

Los Centros de Comando y Control (C2) con IA predictiva superan las capacidades humanas, ofreciendo conciencia situacional superior, análisis de escenarios complejos y decisiones estratégicas rápidas (Aguilar, 2023) La velocidad en el tratamiento de información operacional online permite evaluar alternativas tácticas con precisión. La ARC debe integrar estas tecnologías sin abandonar herramientas como el ciclo OODA, que fortalece la toma de decisiones y el aprendizaje automático. El análisis en tiempo real de datos provenientes de satélites, sensores e inteligencia permite predecir movimientos enemigos y optimizar estrategias navales mediante modelos de Machine Learning, consolidando una ventaja competitiva en entornos de alta exigencia operativa.

A. Tipos de Aprendizaje Automático Aplicables

Para la planificación estratégica naval, donde el foco es la optimización dinámica y la toma de decisiones secuencial, hay tres tipos de aprendizaje automático cruciales, de acuerdo con (Sutton R. S., 2020).

B. Modelos de ML Específicos

Los modelos que se pueden desarrollar o aplicar para la planificación naval se centran en la predicción del futuro y la optimización de las acciones:

Tabla 2. Modelos de Machine Learning

Tipo de ML	Modelo Específico	¿Qué Hace? (Aplicación Naval)
RL	Deep Q Networks (DQN) / Proximal Policy Optimization (PPO)	Entrena a un agente para elegir la mejor secuencia de movimientos de una unidad militar bajo condiciones dinámicas, optimizando la probabilidad de alcanzar un objetivo o minimizar bajas.
Supervisado	Redes Neuronales Recurrentes (RNN/LSTM)	Analiza trayectorias históricas de buques o aeronaves para predecir su posición futura y posible destino, informando las decisiones estratégicas de intercepción o disuasión.
Supervisado	Clasificadores (Random Forest o SVM)	Identifica rápidamente la naturaleza de una amenaza a partir de firmas de sensores (radar, sonar, electromagnéticas), clasificando la emisión como buque de pesca, buque mercante, o buque de guerra hostil.
No Supervisado	Algoritmos de *Clustering* (DBSCAN o K-Means)	Agrupa datos de inteligencia (reportes, comunicaciones) para descubrir redes de apoyo logístico o patrones de despliegue del adversario que no estaban previamente definidos por analistas humanos.
Híbrido	Modelos Gráficos Probabilísticos (Bayesian Networks)	Combina conocimiento experto con datos para modelar la relación de causalidad entre múltiples factores (clima, posición adversaria, recursos propios), calculando la probabilidad de éxito de diferentes planes.

Fuente: elaboración propia

C. Síntesis para la Optimización Estratégica

La planificación de estrategias navales optimizadas con ML se materializa mediante el uso de modelos de Aprendizaje por Refuerzo en entornos simulados, que en este contexto permiten:

- **Exploración de Estrategias:** El sistema explora millones de combinaciones de movimientos y respuestas que un planificador humano no podría considerar.

- **Descubrimiento de Tácticas:** El modelo descubre tácticas no intuitivas que son óptimas bajo las reglas del entorno (por ejemplo, rutas más eficientes para evadir detección o la asignación más efectiva de recursos para una operación conjunta).
- **Adaptación Dinámica:** Los modelos de RL pueden reajustar un plan de misión en tiempo real, en segundos, basándose en la nueva información recibida (detección de un nuevo contacto, cambio meteorológico).

En esencia, la optimización se logra al entrenar al modelo para que elija la mejor acción en el presente que garantice el mejor resultado acumulado en el futuro.

Inteligencia

La IA potencia cada fase del ciclo de inteligencia militar, mejorando velocidad, eficiencia y eficacia (Heller, June 2019). Su aplicación en la inteligencia naval se evidencia en el uso de drones autónomos para reconocimiento y ataques de precisión (Porcelli, 2022), sensores inteligentes para rastreo marítimo, procesamiento de imágenes satelitales y de radar, y detección temprana de amenazas mediante análisis en tiempo real. Estas tecnologías permiten ampliar el campo de vigilancia, reducir bajas, optimizar la toma de decisiones y fortalecer los centros de operaciones navales. La IA se consolida como herramienta estratégica para apoyar a los comandantes en entornos operativos complejos y dinámicos.

Fuegos

Sistemas de guerra naval autónomos: los barcos, submarinos y drones acuáticos pueden realizar misiones de patrullaje, vigilancia y ataques sin intervención humana, aumentando la capacidad operativa mientras reducen la exposición al peligro para la tripulación.

Sistemas de armas autónomos: drones equipados con IA realizan operaciones ofensivas, atacando objetivos específicos con una mejor relación costo beneficio, mayor precisión y autonomía. Incluye misiles inteligentes, torpedos autónomos, sistemas de defensa antimisiles capaces de identificar blancos, seleccionar y atacar objetivos sin intervención humana.

Movimiento y maniobra.

La inteligencia artificial optimiza misiones navales mediante navegación autónoma, evasión de obstáculos y rutas basadas en patrones históricos de amenazas. Según (Mazza, 2023), los drones son empleados en todos los niveles de conducción para tareas activas y pasivas. En búsqueda y rescate, la IA mejora tiempos de respuesta al generar patrones especializados. En ISR, analiza datos de sensores, imágenes satelitales y señales para identificar amenazas y rastrear movimientos enemigos con precisión. Además, simula escenarios de combate complejos para entrenar al personal y evaluar estrategias. Estas capacidades fortalecen la eficacia operativa y la toma de decisiones en entornos dinámicos.

Protección

Mejora la seguridad mediante vigilancia inteligente, monitoreo en tiempo real y análisis de datos de múltiples fuentes para detectar amenazas. Facilita la gestión estratégica en salas de control virtuales, mejora la navegación autónoma y fortalece la defensa contra ciberdelitos. Además, optimiza las rutas marítimas y reduce las vulnerabilidades, contribuyendo a una respuesta proactiva y efectiva que protege los activos estratégicos.

Sostenimiento

La inteligencia artificial transforma la gestión de activos navales mediante sensores que predicen fallas, optimizan el mantenimiento y automatizan la logística. La ARC puede

migrar del mantenimiento reactivo al predictivo y prescriptivo, mejorando la disponibilidad operativa y la eficiencia de la Cadena de Suministro (CS). Según (Chopra, 2016), los modelos de Simulación de Eventos Discretos y Monte Carlo permiten crear gemelos digitales logísticos, esenciales para evaluar la variabilidad en tiempos de entrega y definir niveles óptimos de inventario. Estas herramientas fortalecen la resiliencia logística, permiten una planificación precisa y aseguran el sostenimiento estratégico de las unidades navales en operación.

- **Algoritmos Predictivos**

El corazón de la predicción en el sostenimiento Mantenimiento Predictivo (MP) se basa en dos categorías principales de algoritmos:

Tabla 3. Algoritmos predictivos

TIPO DE ALGORITMO	FOCO DE APLICACIÓN	FUNCIÓN
Clasificación (SVM, Bosques Aleatorios)	Probabilidad de Falla	Clasifican el estado de un activo (e.g., motor) en categorías de riesgo (Bajo, Medio, Alto) basándose en datos de sensores.
Regresión (RNN/LSTM)	Tiempo Restante de Vida Útil	Analizan series temporales complejas de datos operacionales para pronosticar con precisión cuántos días u horas le quedan a un componente antes de que falle. (Goodfellow I. B., 2016).

Fuente: elaboración propia

- **Mantenimiento predictivo**.

La evolución hacia una logística predictiva, prescriptiva y automatizada permite minimizar el mantenimiento correctivo, optimizando el ciclo de vida de las unidades (Hernández A., 2023). El monitoreo continuo mediante gemelos digitales permite prever

averías en tiempo real, como lo demuestra la Armada Española con sistemas desarrollados junto a Indra. La IA analiza desviaciones en motores y componentes, facilitando la planificación precisa de misiones. Las tecnologías de la Industria 4.0 integran datos físicos y digitales para optimizar decisiones logísticas, rutas de navegación y gestión de suministros, reduciendo costos operativos y mejorando la disponibilidad de los activos navales de forma proactiva.

1.2.2 Dominio terrestre

Automatización y vehículos autónomos

La IA facilita el desarrollo de vehículos terrestres autónomos, drones y robots de combate, que pueden realizar misiones de patrullaje, desactivación de minas o ataques directos sin la intervención humana.

Toma de Decisiones en Tiempo Real

La resolución de problemáticas en tiempo real en la ARC requiere que la IA funcione como un motor cognitivo capaz de transformar datos heterogéneos y masivos en un plan de acción óptimo en cuestión de segundos. Esto se logra mediante la Fusión de Datos y el Razonamiento Prescriptivo basado en *Machine Learning*. El primer paso para la toma de decisiones es la integración de la información. La IA resuelve este desafío a través de la Fusión de Datos Multifuente (*Multisource Data Fusion*), esencial para construir y mantener el Panorama Operacional Común:

- **Recolección Heterogénea:** Los datos se recopilan en tiempo real desde múltiples fuentes (radares, sonares, Guerra Electrónica, imágenes satelitales, reportes de inteligencia).

- **Alineación y Filtrado:** La IA utiliza algoritmos de clustering y clasificación para limpiar, correlacionar y alinear estos datos (ej. identificar que una traza de radar y una emisión de radio corresponden al mismo activo).
- **Fusión Probabilística:** Se emplean Redes Bayesianas o Lógicas Difusas para calcular la probabilidad de la intención de un contacto o la veracidad de una amenaza, incluso con datos incompletos (Waltz, 2023). Este proceso transforma la información cruda en conocimiento procesable para el comandante.
- **Algoritmos para la Resolución de Problemáticas (Decisión Prescriptiva)**

Una vez que la IA ha fusionado los datos y ha evaluado el riesgo (decisión descriptiva), el sistema debe determinar la mejor acción a seguir (decisión prescriptiva). Esto se logra mediante el Aprendizaje por Refuerzo (RL).

Tabla 4. Algoritmos para la resolución de problemáticas

Modelo de ML	**Función en Tiempo Real**	**Aplicación a la Problemática**
Aprendizaje por Refuerzo (RL)	Optimización Dinámica y Secuencial	Dada una situación de crisis, el RL simula millones de secuencias de acción posibles (asignación de unidades, cambio de rumbo, uso de armamento) y propone la **ruta de acción óptima** que maximiza la probabilidad de éxito (recompensa) en función de los parámetros.
Modelos de Regresión/Predicción	Proyección de Escenarios	Predicen el **movimiento futuro** del adversario y el impacto de los factores ambientales (clima, estado del mar), permitiendo al sistema evaluar las consecuencias de cada opción de RL antes de ser ejecutada.

Fuente: elaboración propia

Este enfoque permite que la IA genere un árbol de decisiones en tiempo real que es constantemente actualizado con nuevos datos, resolviendo la problemática actual mediante la recomendación de la acción más ventajosa.

Escenarios de Aplicación Naval

- **Operaciones de Interdicción Marítima (Lucha contra Narcotráfico):**
  - **Problemática:** Detección de una lancha rápida y asignación de activos de intercepción (Guardacostas, aeronave).
  - **Solución IA:** El sistema RL, alimentado por la posición de la lancha, condiciones meteorológicas, autonomía de los activos propios, calcula la trayectoria de intercepción más rápida y el activo más eficiente para maximizar la probabilidad de éxito antes de que la lancha escape de la Zona de Responsabilidad.
- **Gestión Táctica de Crisis (Maniobra en combate):**
  - **Problemática:** Un buque es atacado y necesita una respuesta táctica inmediata (cambio de formación, contramedidas).
  - **Solución IA:** El sistema evalúa instantáneamente el tipo de amenaza (clasificación supervisada), el riesgo de la posición actual y propone la maniobra evasiva más segura y la contramedida más efectiva mediante RL para minimizar el daño y mantener la capacidad operativa.

1.2.3 Dominio aéreo

La implementación de la IA en el dominio aéreo de la ARC para espionaje, reconocimiento y defensa debe alinearse con un marco estratégico claro.

Marco Político

Aunque no exista una política pública explícita de "Espionaje Aéreo con IA" a 2025, el uso de la tecnología se sustenta en:

- **Política de Seguridad y Defensa Nacional:** Legitima el uso de capacidades de inteligencia y la búsqueda de superioridad tecnológica para proteger la soberanía y los intereses marítimos ((MDN)., 2020).
- **Planes de Desarrollo del Sector Defensa:** Priorizan la inversión en tecnologías disruptivas (*Machine Learning*) para aumentar la efectividad operacional y reducir la asimetría tecnológica.

Objetivos Militares y Diferenciación con *Machine Learning*

El impacto se reconoce en el ámbito marítimo y fluvial, con objetivos que son inalcanzables sin el aprendizaje automático:

Tabla 5. Objetivos Militares y Diferenciación con Machine Learning

Misión	Objetivo Militar	Diferenciación con ML
Espionaje (ISR)	Detección, Identificación y Caracterización Automática (DICAT).	Algoritmos de Aprendizaje Profundo (CNN) procesan la inteligencia al instante con precisión superior, identificando amenazas o activos pequeños en tiempo real. (Zhang, 2021).
Defensa Aérea	Compromiso y Enganche Predictivo.	El Aprendizaje por Refuerzo (RL) permite que los sistemas no solo rastreen la amenaza (misil/aeronave), sino que predigan su movimiento evasivo, optimizando la respuesta táctica y minimizando el tiempo de decisión (Sutton & Barto, 2020).

Fuente: elaboración propia

Efectos Estratégicos

La política comparada exige que los planes de desarrollo de la ARC aborden el efecto de la IA en el personal y la doctrina:

- **Desplazamiento del Analista:** El militar pasa de ser un observador de datos a un supervisor de algoritmos y un tomador de decisiones éticas. (RAND, Artificial intelligence and the future of defense: Strategy and policy considerations., 2022)
- **Doctrina Basada en Máquinas:** La velocidad de la guerra es dictada por la IA, obligando a integrar el uso de la IA Ofensiva y Defensiva en los procedimientos operativos estándar.

Drones y aviones no tripulados.

Misiones de espionaje, ataque y reconocimiento sin poner en peligro a los pilotos, mejorando la precisión de los ataques, optimizando las rutas y la gestión de la munición.

Sistemas de defensa aérea inteligentes.

La IA se utiliza para mejorar la detección, el seguimiento de misiles y aeronaves enemigas analiza patrones de amenazas y toman decisiones autónomas para interceptar ataques.

1.2.4 Dominio cibernético

Las tecnologías disruptivas han intensificado las amenazas cibernéticas, generando riesgos críticos para la Seguridad y Defensa Nacional (Realpe, 2020),. Colombia cuenta con una estructura de Ciberdefensa en niveles estratégico, operacional y táctico, respaldada por Mintic y batallones especializados de las Fuerzas Militares. El ciberespacio sigue siendo vulnerable a ataques latentes o emergentes, con potenciales pérdidas en sectores clave. Se requiere una estrategia integral para mitigar riesgos y fortalecer la resiliencia nacional frente

a amenazas disruptivas y destructivas. Las ciber amenazas latentes y emergentes se identifican mediante el instrumento denominado Ventana AREM así:

Tabla 6. Ventana AREM. Ciber menazas latentes y emergentes.

Amenaza Latente	**Amenaza Emergente**
Ciberguerra	Guerra Autónoma
LAWS Lethal Autonomous Weapons (Robots Militares, embarcaciones de superficie y submarinas, drones autónomos, sistemas satelitales autónomos).	Ciberarmas de destrucción masiva
Sistemas Autónomos	

Fuente: M. E. Realpe1 y J. Cano

Ciberseguridad.

La inteligencia artificial fortalece la ciberseguridad de la ARC al detectar anomalías y responder a ciberataques sofisticados. En un entorno digital interconectado y volátil, donde los datos fluyen constantemente, proteger redes y sistemas es crucial. Según (Flashpoint, 2025), el aumento exponencial de amenazas exige un enfoque proactivo e integral que garantice la seguridad institucional mediante capacidades tecnológicas avanzadas.

Ciberdefensa y ciberataques

Se ha integrado en las estrategias de defensa cibernética, ayudando a detectar ataques antes de que se lleven a cabo, respondiendo a amenazas con gran velocidad y precisión. También se utiliza en ofensivas cibernéticas, mejorando las capacidades de penetración y desestabilización de las infraestructuras enemigas.

Guerra de información

Se utiliza para manipular información, creando "deepfakes", desinformación y propaganda sofisticada dirigida, lo que influye en la opinión pública o desestabiliza las

sociedades enemigas, al poder diseminar campañas de desinformación altamente personalizadas y efectivas, impactando la moral del enemigo.

1.2.5. Dominio espacial

Inteligencia

Su uso en satélites mejora la capacidad de monitoreo para vigilancia marítima, recopilación de información y comunicación de manera más eficiente. Incluye la detección de misiles balísticos, el seguimiento de naves espaciales y la precisión de las misiones de lanzamiento.

Defensa espacial

La IA permite anticipar amenazas y coordinar acciones defensivas y ofensivas en el espacio, incluyendo ataques contra satélites enemigos. La eficiencia naval en monitoreo, inteligencia y comunicaciones depende del uso de satélites en Órbita Terrestre Baja (LEO), ya que los satélites en Órbita Geoestacionaria (GEO) de Colombia no cumplen funciones de observación terrestre ni adquisición de inteligencia detallada. Para la vigilancia marítima, se requiere una constelación LEO que ofrezca alta resolución espacial y temporal. La ARC debe impulsar esta capacidad, integrando IA y tecnología espacial para fortalecer su soberanía, proyección regional y respuesta estratégica en el dominio aeroespacial.

Tabla 7. Tipos de satélite y funciones

Tipo de Satélite/Sensor	**Órbita**	**Función Estratégica**
Observación de la Tierra Óptica	LEO (300-1000 km)	Recopilación de Inteligencia: Genera imágenes de alta resolución (ISR) para identificar, clasificar y seguir activos en tiempo diurno y buenas condiciones climáticas (Mcdowell, 2022).
Radar de Apertura Sintética (SAR)	LEO (300-1000 km)	Vigilancia Marítima (MDA): Es crucial para la seguridad nacional, ya que penetra nubes y opera de noche. Detecta anomalías en el tráfico marítimo y buques de interés en cualquier condición meteorológica.
Cubesats (Plataformas Pequeñas)	LEO	Comunicaciones y Relevo de Datos: Sirven como nodos de comunicación de bajo costo y rápido despliegue, facilitando la transmisión de inteligencia y la mejora de la cobertura en áreas marítimas sin infraestructura (Weeden, 2017).

Fuente: elaboración propia

El desafío de implementación realista de la ARC no es el lanzamiento inmediato de una constelación de propiedad total, sino la adquisición de la capacidad de acceso y procesamiento de datos.

Tabla 8. Implementación y alineación

Estadio de Implementación	**Alineación con Planes de Desarrollo**
Fase I: Acceso Comercial y Alianzas (2026-2027)	En lugar de la adquisición, la ARC debe asegurar contratos de acceso prioritario a datos de constelaciones LEO comerciales de SAR y Ópticas. Esto es una solución concreta y de bajo riesgo que habilita la capacidad de Monitoreo para Vigilancia Marítima de inmediato, sin esperar al desarrollo de una plataforma satelital propia (Valeriano, 2021).
Fase II: Desarrollo de Capacidad Nacional (2028-2030)	La ARC puede impulsar un plan de desarrollo de micro o nanosatélites (Cubesats) a través de la industria y la academia nacional. Estos tendrían tareas específicas, como la comunicación táctica y la experimentación de sensores, construyendo progresivamente la experiencia nacional en el dominio espacial.

Fuente: elaboración propia

El entrelazamiento con la Seguridad Nacional del uso estratégico de los satélites LEO genera Conciencia del Dominio Marítimo. Esta información es crucial ya que permitiría mejorar a la ARC:

- **El Combate de Actividades Ilícitas:** Identificar en tiempo real buques de narcotráfico, pesca ilegal y contrabando fuera de la zona económica exclusiva.
- **Protección de Activos Estratégicos**: Monitorear la infraestructura petrolera y de comunicaciones submarinas, alertando sobre actividades sospechosas.

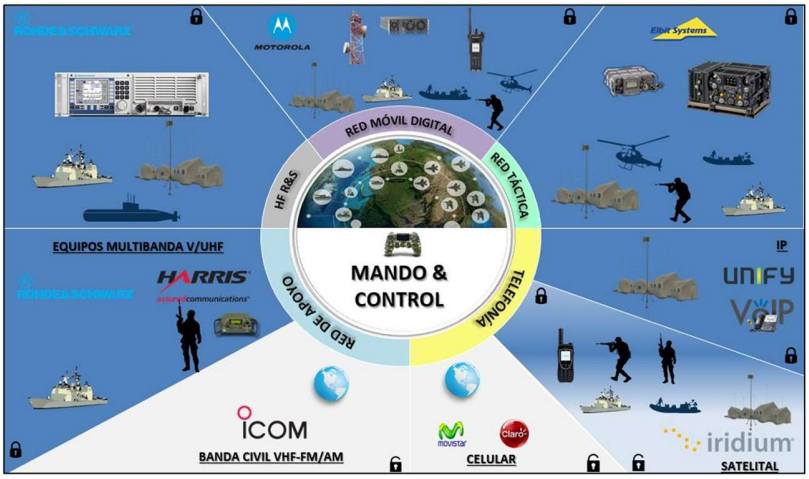
Esta aproximación permite aterrizar la implementación mediante un enfoque de adquisición de servicios y desarrollo incremental de capacidades, logrando soluciones concretas que impactan directamente los planes estratégicos de la Fuerza.

Desarrollo del objetivo 2 - Analizar los desafíos que presenta la evolución de la IA para la ARC 2025 - 2030.

2.1 Comunicaciones: Impacto de la IA en Redes Tácticas y Estrategia de Inversión

El análisis en comunicaciones debe centrarse en cómo la IA supera las limitaciones de ancho de banda y seguridad de las redes existentes, y cómo la ARC se alinea con la estrategia de transformación del MDN. De acuerdo con el plan estratégico de tecnologías de la información y de las comunicaciones (PETIC), la ARC cuenta con sistemas de comunicaciones militares, organizados así:

Figura 5. Sistemas de Comunicaciones Militares de la ARC



Fuente: PETIC (2023)

La IA es un factor de mitigación de riesgos y optimización en las comunicaciones navales:

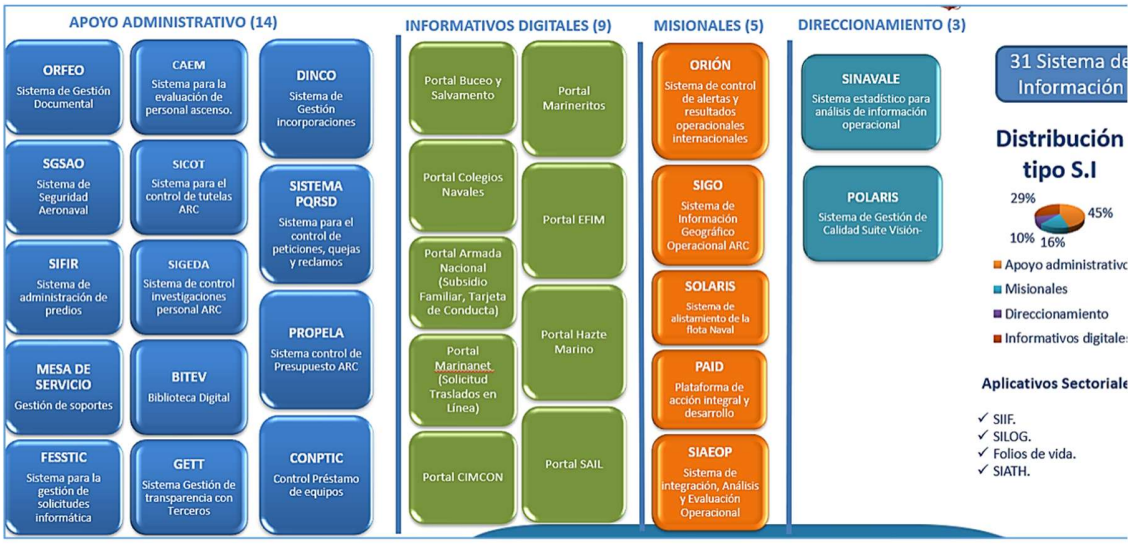
- Red HF (Alta Frecuencia): Se caracteriza por transmitir datos e intercambiar información a través de medios o módulos de encriptación, con geoposicionamiento, digitalización de voz, transmisión de datos, sistemas de gestión e interoperabilidad. Es esencial para el largo alcance, pero inestable. La IA, mediante algoritmos de Aprendizaje por Refuerzo (RL), permite la Radio Cognitiva. El sistema predice y selecciona dinámicamente el canal de transmisión más confiable y libre de interferencia en tiempo real, maximizando la tasa de éxito en la transmisión de datos críticos (Ghasemi, 2021).

- Seguridad de Voz y Red Táctica: permiten obtener un sistema de enlace efectivo con seguridad de voz en las gamas de HF y VHF para el desarrollo de operaciones propias y conjuntas. La IA utiliza el Aprendizaje Profundo para la detección de anomalías en

el espectro, identificando y mitigando automáticamente intentos de *jamming*, ataques de suplantación (*spoofing*) o patrones de tráfico anómalos, fortaleciendo la seguridad de voz y la integridad de la red (Li, 2023).

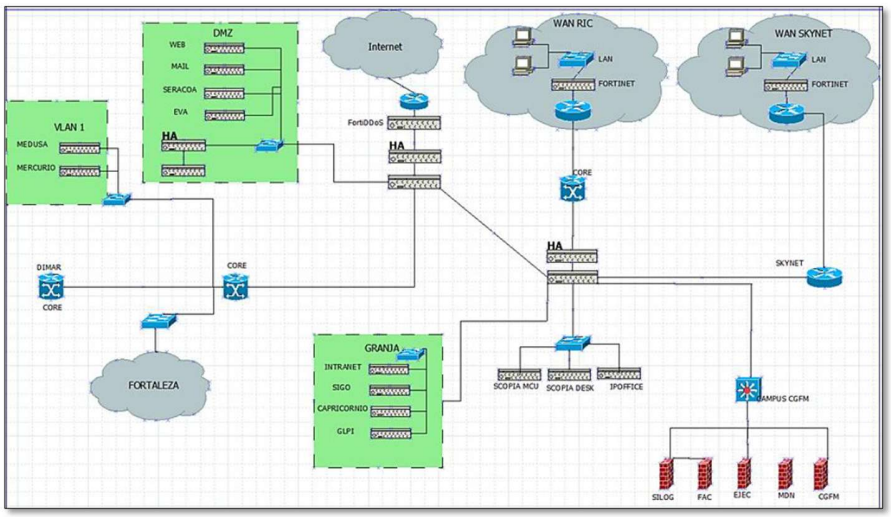
La IA logrará la concordancia entre la red lenta (HF) y la táctica (alta velocidad) al garantizar la Calidad del Servicio (QoS) y la interoperabilidad. Un sistema basado en RL prioriza de forma autónoma el tráfico de datos críticos sobre el tráfico secundario, esencial para la Toma de Decisiones en Tiempo Real.

Figura 6. Sistemas de información ARC



Fuente: PETIC (2023)

Figura 7. Arquitectura general red WAN/LAN ARC



Fuente: PETIC (2023)

2.2 Proyectos de Inversión, *Software* (Estrategia)

Para potencializar estos desafíos, la ARC debe formalizar un plan que integre la IA basándose en los lineamientos de Transformación Digital del MDN:

Tabla 9. Eje estratégico MDN -Desafíos ARC

Eje Estratégico MDN (Proyección)	**Desafío de la ARC**	**Solución Concreta con IA**
Modernización de *Software*	El *software* C4ISR es obsoleto y cerrado.	Inversión para transversalizar plataformas abiertas que permitan la integración de módulos de ML para el procesamiento de señales y datos (MDN, 2020).
Ética y Confianza	Riesgo de sesgo algorítmico y falta de transparencia en la decisión.	Desarrollo de estándares éticos para la IA en comunicaciones, priorizando la IA Explicable (XAI) para justificar la selección de canales y las alertas de seguridad (Sharkey, 2017)
Proyectos de Inversión	Necesidad de financiar I+D.	Formalizar un proyecto para un "Laboratorio de Radio Cognitiva" que investigue y desarrolle soluciones de RL aplicadas a las bandas HF, asegurando el sostenimiento de las comunicaciones de largo alcance de la Fuerza.

Fuente: elaboración propia

2.3 Sostenimiento

Se debe impulsar la IA para mejorar la disponibilidad del material (logística) y del personal (capital humano), ambos transversales a la conducción de la guerra, cuyo desafío se resolvería implementando un Ecosistema de Sostenimiento Cognitivo que fusione la información del estado de la flota con la capacidad del personal para realizar las reparaciones.

2.3.1 Prospectiva del Material (Logística Naval)

- **Implementación:** Se adopta el concepto de Gemelo Digital (*Digital Twin*) de los activos (buques, sistemas de armas).

- **Función Clave:** El Mantenimiento Predictivo usa algoritmos como las redes LSTM (series de tiempo) para pronosticar el Tiempo Restante de Vida Útil de los componentes (Tao, 2017).
- **Resultado Misional:** El sistema no solo detecta, sino que realiza Sostenimiento Prescriptivo. Simula las fallas predichas para optimizar la cadena de suministro y definir el momento ideal de la parada técnica, maximizando la disponibilidad operacional de la flota.

2.3.2 Prospectiva del Personal

- **Implementación:** Se utilizan modelos de Aprendizaje Supervisado (Clasificación/Regresión) aplicados a la gestión del talento humano.
- **Función Clave:**
    - **Predicción de Competencias:** Identifican la Brecha de Habilidades y generan Rutas de Capacitación Personalizadas para el personal técnico (Peñaloza, 2022).

      Disponibilidad Operativa: Predicen el riesgo de fatiga del personal clave.
- **Resultado Misional:** El sostenimiento del personal se enfoca en la Predicción de la Disponibilidad de Competencias, asegurando que el técnico certificado esté disponible en el momento exacto en que el Gemelo Digital predice una necesidad de mantenimiento.

Figura 8. Logística operacional

Fuente: Oficina de Planeación Logística JOLAN ARC

2.3.3 Sanidad Naval

La aplicación de la IA busca acelerar la toma de decisiones clínicas y epidemiológicas en entornos de alta exigencia, transformando los datos médicos en acciones prescriptivas. Se aplicaría en la salud operacional, promoción y prevención; a través del desarrollo de algoritmos enfocados en modelos de Aprendizaje Supervisado y Aprendizaje Profundo, fundamentales para la construcción colectiva de diagnósticos, los planes de respuesta y que faciliten la toma de decisiones. Su capacidad para procesar grandes volúmenes de datos permite mejorar diagnósticos y tratamientos. De acuerdo con (Linares, 2022) "los principales ámbitos de salud en los que la IA sería útil son: a) diagnóstico, análisis de patrones e investigación de causas y evolución de enfermedades; b) prevención y educación para la salud; c) atención e intervención médicas (consulta, prescripción de medicamentos, dosificación y cirugías robóticas)".

Tipos de Algoritmos para el Desarrollo en Sanidad Naval

Tabla 10. Algoritmos para el desarrollo en Sanidad Naval

Dominio de Decisión	Algoritmo Principal	Función Estratégica
Clínica (Diagnóstico y Pronóstico)	Redes Neuronales Convolucionales (CNN)	Análisis rápido de imágenes médicas (radiografías, ecografías) en telemedicina y Clasificación predictiva de lesiones y patologías (Ker, 2017).
Epidemiológica (Vigilancia)	Redes de Memoria a Corto y Largo Plazo (LSTM)	Análisis de series de tiempo para la predicción temprana de brotes de enfermedades infecciosas en áreas de despliegue, facilitando medidas preventivas (Adhikari, 2021).
Recursos (Asignación Óptima)	Aprendizaje por Refuerzo (RL)	Utilizado para la optimización prescriptiva de la distribución de suministros médicos, personal y evacuaciones, maximizando el bienestar del paciente con recursos limitados.

Fuente: elaboración propia

Algoritmos para la Construcción Colectiva

Se refieren a la integración de la información heterogénea y la generación de confianza, mediante Redes Bayesianas, fusionando datos clínicos específicos (certeza) con datos epidemiológicos y ambientales (incertidumbre) para generar una probabilidad colectiva del estado de salud del personal o del riesgo de una amenaza sanitaria (Liu, 2020).

2.4 Investigación y Desarrollo

La ARC debe fortalecer su independencia tecnológica mediante el desarrollo de armas innovadoras: energía dirigida, sistemas hipersónicos, láser, satélites y pulsos electromagnéticos. Esto requiere nuevas tecnologías y materiales que mejoren la

protección y movilidad de tropas. Ante los desafíos emergentes, es urgente prepararse para la guerra autónoma y la robótica naval. La I+D debe enfocarse en migrar de sistemas remotos a plataformas autónomas y colaborativas, empleando Aprendizaje por Refuerzo (RL) como motor cognitivo para decisiones tácticas avanzadas.

- **Alcances de la Guerra Autónoma y Robótica Naval**

La integración de la IA en la robótica naval (USV y UUV) busca tres alcances estratégicos:

Tabla 11. Alcance robótica naval

Alcance Estratégico	Implicación Misional	Motor de IA Requerido
Autonomía Cognitiva de Tarea	Permite que un UUV navegue, detecte minas y las neutralice sin intervención humana constante, tomando decisiones tácticas inmediatas.	Aprendizaje por Refuerzo Profundo (DRL): El agente aprende a ejecutar tareas secuenciales que maximizan una recompensa (ej. éxito en la misión, bajo consumo energético) (Sutton & Barto, 2020).
Colaboración Heterogénea (MUM-T)	Integración de equipos tripulados y no tripulados (*Manned-Unmanned Teaming*). Una fragata coordina de forma autónoma un enjambre de USV para vigilancia o ataque.	RL Multi-Agente (MARL): Los agentes individuales (USVs) aprenden a cooperar y coordinarse para lograr un objetivo común, incluso si hay fallas en la comunicación.
Guerra Autónoma (Ética)	Desarrollo de sistemas con capacidad de *enganche* autónomo (uso de fuerza). La I+D debe incorporar sensores éticos y de IA Explicable (XAI) para garantizar que el humano mantenga el Control Cognitivo de la decisión final (Sharkey, The ethical case against killer robots., 2017).	

Fuente: elaboración propia

- **Integración de Equipos y Lenguajes de Aprendizaje Automático**

La integración de sistemas autónomos exige un lenguaje común de comunicación y programación. En I+D, se debe estandarizar Python para aprendizaje automático, utilizando librerías como TensorFlow y PyTorch. En robótica naval, el software embarcado de UUV/USV se desarrolla en C++ por su eficiencia. El reto es crear interfaces robustas que permitan la interacción fluida entre modelos Python y hardware C++, mediante entornos como ROS, minimizando la latencia en decisiones operativas. La I+D debe centrarse en lograr interoperabilidad entre el hardware naval legado y los nuevos cerebros cognitivos, fortaleciendo la capacidad tecnológica y la respuesta táctica de la ARC.

2.5 Costos de Implementación y Ciclo de Vida de los Sistemas de IA

La implementación de sistemas de IA en la ARC enfrenta el desafío de financiación, al requerir inversión inicial significativa. Es necesario proyectar su ciclo de vida, mantenimiento, actualización tecnológica y modernización de infraestructura, garantizando conectividad, redundancia e interoperabilidad sin afectar la operatividad. Esta inversión no debe verse como un gasto, sino como una optimización estratégica que reduce costos logísticos a largo plazo y exige una gestión adaptada al ritmo acelerado de la evolución tecnológica.

Indexación de los Costos Logísticos en la Aplicación de IA

La implementación de la IA no genera nuevos costos logísticos, sino que los transforma y los reduce significativamente.

Tabla 12. Costos logísticos

Costo Logístico Tradicional	**Impacto de la IA (Reducción/Transformación)**
Inventario Excesivo (*Buffer Stock*)	Reducción del *Stock*: El Mantenimiento Predictivo (PdM) reduce la necesidad de mantener grandes inventarios de seguridad. La IA permite la reposición *justo a tiempo* de piezas, minimizando el capital inmovilizado y los costos de almacenamiento (Chopra, Supply chain management: Strategy, planning, and operation (6th ed.)., 2016).
Tiempo de Inactividad (*Downtime*)	Máxima Disponibilidad: La IA (mediante LSTM y Gemelo Digital) predice fallas antes de que ocurran. El costo de una reparación planificada es hasta 10 veces menor que el costo de una falla catastrófica no planificada y el impacto en la misión (Lee, 2018.).
Mantenimiento (Mano de Obra)	Eficiencia en la Mano de Obra: La IA Generativa puede automatizar la creación de manuales de mantenimiento y la IA Explicable (XAI) guía a los técnicos menos experimentados en diagnósticos complejos, reduciendo errores y el tiempo de reparación.
Costos de Falla Catastrófica	Mitigación de Riesgos: La predicción temprana evita la pérdida de activos de alto valor (buques, aeronaves), cuyo costo de reemplazo supera con creces la inversión en *software* de IA.

Fuente: elaboración propia

La inversión inicial en IA (infraestructura de datos, *data scientists* y *hardware* de computación) se amortiza con creces al reducir los costos operativos y aumentar la disponibilidad de la flota, factor esencial para la conducción de la guerra.

Ciclo de Vida de los Sistemas Basados en IA (S-AI)

Las políticas institucionales deben reconocer que el Ciclo de Vida S-AI difiere radicalmente del ciclo de vida de *software* tradicional.

Tabla 13. Ciclo de vida

Etapa del Ciclo de Vida	Enfoque Institucional para la Modernización de IA
Desarrollo y Entrenamiento	Estandarización de Datos: Políticas que exijan el etiquetado y la gobernanza de datos como activo fundamental. El costo principal es la adquisición y limpieza de los datos, no el *hardware* inicial.
Operación y Monitoreo (Mantenimiento)	Monitoreo Continuo: A diferencia del *software* tradicional, los modelos de IA experimentan "Deriva del Modelo" (*Model Drift*). La política debe incluir ciclos de reentrenamiento continuo (cada 6-12 meses), no solo corrección de *bugs* (Breck, 2017).
Modernización y Disposición	Arquitectura Modular: La ARC debe adoptar arquitecturas Modulares y Abiertas (basadas en *Microservicios*) que permitan reemplazar rápidamente un algoritmo obsoleto (ej. reemplazar un SVM por un modelo de *Deep Learning*) sin desmantelar todo el sistema (MDN, 2020).

Fuente: elaboración propia

La clave para la modernización es indexar el costo de la IA en la categoría de "Gasto de Capital Recurrente" (por reentrenamiento y actualización de modelos), más que en la categoría de "Adquisición Única" de *software*.

2.6 Educación y Reentrenamiento: Modelación y Entornos Sintéticos para la IA

Se debe apoyar en los Entornos Sintéticos y el Aprendizaje por Refuerzo (RL). El objetivo es crear un Gemelo Digital Operacional donde el personal y los agentes de IA aprendan de forma segura y acelerada.

Tipos de Modelación y Plataformas

La simulación requerida no es solo para entrenamiento humano, sino para la generación de datos sintéticos y el entrenamiento de algoritmos:

Tabla 14. Modelación

Tipo de Modelación	Descripción	Propósito Estratégico
Simulación Basada en Agentes (ABS)	Modelos donde múltiples agentes (buques, aeronaves, misiles, AI adversaria) interactúan bajo reglas de comportamiento realistas.	Evaluar estrategias tácticas complejas y entrenar la coordinación multi-agente (*enjambres* de USV/UUV).
Simulación de Alto Realismo (Gemelo Digital)	Réplicas virtuales de plataformas físicas con alta fidelidad en la física, sensores y comportamiento del mar.	Permite la Transferencia al Mundo Real (*Sim-to-Real*). Es el banco de pruebas para los modelos de PdM y Guerra Autónoma.

Fuente: elaboración propia

Plataformas y Lenguajes:

- **Plataforma Base:** Motores de juego de alta fidelidad como Unreal Engine o Unity proporcionan el entorno gráfico y físico.
- **Integración y Robótica:** La plataforma ROS (*Robot Operating System*) es esencial para conectar la lógica del simulador con los modelos de IA, permitiendo que el *software* de control de un robot real se pruebe en el entorno virtual.
- **Algoritmos de ML:** El Aprendizaje por Refuerzo Profundo (DRL), específicamente algoritmos como PPO (*Proximal Policy Optimization*), es el método para que la IA aprenda a tomar decisiones tácticas en el simulador (Sutton R. S., 2020).

Integración Transversal con Análisis Predictivos

La integración transversal de IA y personal se fortalece al incorporar análisis predictivos en simulaciones. Si un modelo anticipa una falla del radar con 30% de probabilidad, la simulación replica esa condición, obligando a operadores e IA a adaptarse. Esto entrena

resiliencia cognitiva y valida planes de misión bajo escenarios degradados, mejorando la preparación operativa y la toma de decisiones.

Componentes Clave de los Entornos Virtuales

Para lograr una operacionalización estructurada, el entorno virtual debe incluir:

Tabla 15. Componente clave entornos virtuales

Componente Clave	Función Estratégica en I.A.
Diseño Medioambiental de Alta Fidelidad	Proporcionar datos de sensores y física realistas (oleaje, ruido, clima) para que la IA no sea frágil ante la variabilidad del mundo real.
Gerencia de Datos Sintéticos	Generar automáticamente datos etiquetados de alta calidad (ej. clasificaciones de amenazas). Estos datos se usan para entrenar algoritmos de Aprendizaje Supervisado de forma eficiente.
Módulos de Formación Adaptativa	Interfaces que ajustan la dificultad del escenario para el militar o el agente de IA, basándose en el rendimiento en tiempo real (evaluación continua).
Pruebas y Validación (Transferencia al Mundo Real)	Métricas que aseguren la fidelidad (*Sim-to-Real*). La IA solo se transfiere a un activo real si demuestra un rendimiento predecible en el Gemelo Digital.

Fuente: elaboración propia

Ventajas de Entrenar la IA en Entornos Virtuales

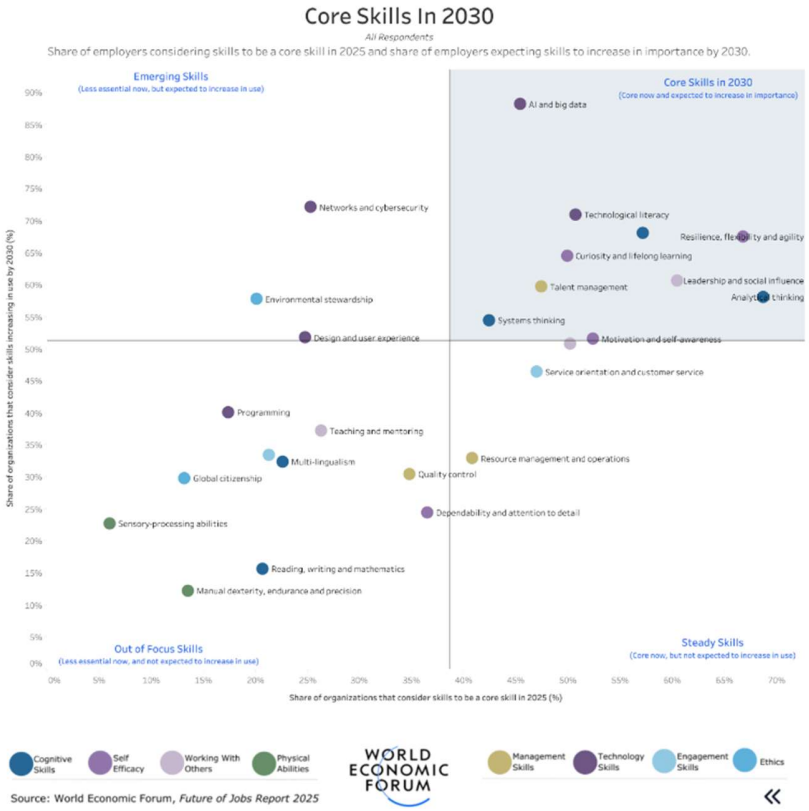
El uso de entornos virtuales ofrece ventajas decisivas sobre los métodos tradicionales de entrenamiento:

- **Costo y Seguridad:** El entrenamiento es costo-efectivo y libre de riesgo físico para el personal y el material de alto valor (Mnih, 2015). Se pueden simular fallas catastróficas o escenarios de combate sin implicaciones reales.

- **Escalabilidad y Velocidad:** Un agente de IA puede ejecutar el equivalente a 100 años de experiencia táctica en simulaciones en una sola noche, explorando millones de escenarios (*edge cases*) imposibles de recrear físicamente.
- **Reproducibilidad:** Las simulaciones permiten la reproducción exacta de una falla o un error táctico para su análisis y corrección, un proceso esencial para mejorar la IA y la doctrina.

Según el MFC 3-0, las decisiones son el núcleo del Mando y Control, guiando la misión y los objetivos. Para ello, comandantes y estados mayores requieren conocimiento profundo, no solo información. La IA potencia este proceso al transformar datos en sabiduría organizacional, personalizar el aprendizaje, fomentar la colaboración y apoyar decisiones estratégicas. La ARC debe integrar IA en su formación, liderazgo y cultura naval, promoviendo habilidades humanas como juicio, empatía y pensamiento crítico. Al 2030, estas competencias serán clave. Aprender IA no basta: lo esencial será cómo se usa, con visión, criterio y un faro ético superior.

Figura 11. Núcleo habilidades en 2030



Fuente: World Economic Forum

El foro económico mundial (FEM, 2025) indica que para el 2030 se requiere de humanos que piensan con datos, que deciden con cabeza y corazón, que no solo construyan productos, sino sistemas con propósito. No se trata de contar solo con un talento humano totalmente profesional en IA, sino de contar con una ARC que construya y desarrolle permanentemente sus habilidades para dar cumplimiento a su misión constitucional.

Desarrollo del objetivo 3 - Determinar las vulnerabilidades que genera la evolución de la IA para la ARC en el 2025-2030.

3.1 Riesgos geopolíticos

lm Este entorno requiere la adopción de un enfoque de Smart Power, adaptando las visiones geopolíticas clásicas a los desafíos y oportunidades del ciberespacio, caracterizados por la inmaterialidad y la ruptura de barreras geográficas. Actualmente se presentan diferentes conflictos internacionales, la guerra y las tensiones geopolíticas pueden incrementar los riesgos para la ARC, incluyendo ataques directos y ciber ataques.

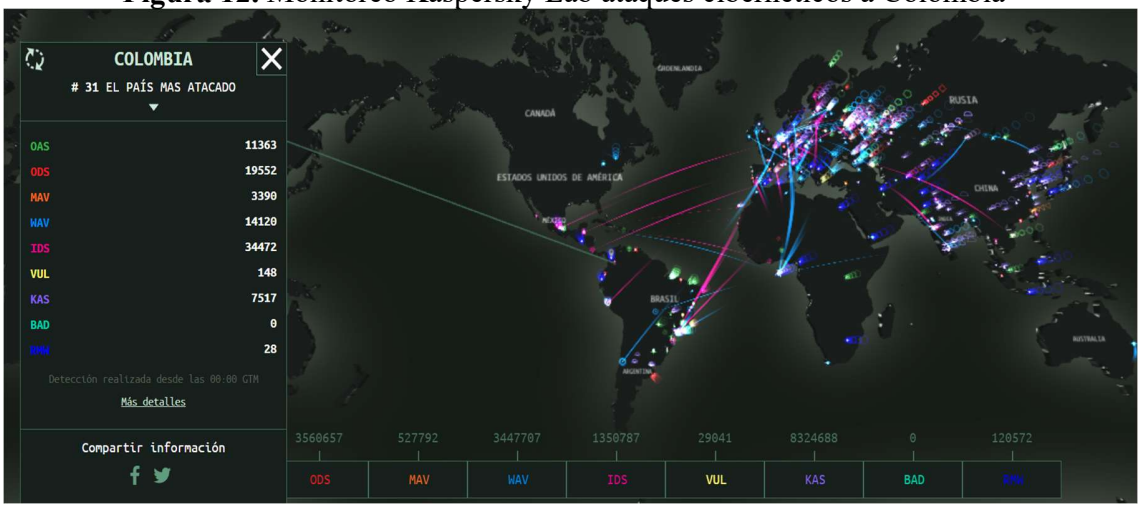
Se observa una carrera tecnológica entre China y Estados Unidos, Asia-Pacífico y Occidente y entre las grandes empresas tecnológicas de la economía digital y las empresas multinacionales de la revolución industrial, la cual conlleva el diseño e implementación de estrategias y políticas de desarrollo tecnológico. Para (Arteaga, 2019), "la adopción de medidas proteccionistas o de competencia desleal para denegar o retrasar el acceso de los rivales a la superioridad tecnológica, como revela el caso de Huawei y las plataformas digitales de quinta generación (5G). La búsqueda de la superioridad militar a través de la IA podría desencadenar una carrera de armamentos global, aumentando la inestabilidad y el riesgo de conflicto.

3.2 Dominio ciberespacial.

La ARC enfrenta una creciente vulnerabilidad en el dominio ciber ante IA enemiga capaz de manipular datos, inducir decisiones erróneas y aprender tácticas institucionales. La alta interconectividad y dependencia digital amplían la superficie de ataque, favoreciendo acciones como la denegación de servicio. En escenarios de guerra cibernética avanzada, una IA superinteligente podría superar la capacidad humana en ofensiva y defensa. La falta de infraestructura digital robusta y políticas claras expone aún más a la institución a riesgos estratégicos y operativos. El monitoreo de

(Karspersky, 2025), evidencia que Colombia es el país N° 22 en el ranking global de ciber ataques.

Figura 12. Monitoreo Kaspersky Lab ataques cibernéticos a Colombia



Fuente: Ciber amenazas Kaspersky lab

3.3 Mando y control

La ARC enfrenta vulnerabilidades ante ataques de IA enemiga, capaces de explotar debilidades en sus sistemas de Mando y Control (C2). El riesgo principal radica en la manipulación de datos mediante modelos predictivos que generan inteligencia errónea, afectando la percepción del comandante y comprometiendo la toma de decisiones. Esta exposición cibernética permite al adversario interferir en la cadena de mando con ataques complejos y coordinados, aprovechando la confianza excesiva en la veracidad del dato.

3.4Vulnerabilidades Clave y Explotación por ML Adversario

El adversario utiliza ML para llevar a cabo ataques cognitivos que comprometen la toma de decisiones, sin necesariamente destruir la red.

Manipulación de Datos y Fusión

- **Vulnerabilidad:** Confianza de Sensores y Fusión de Datos. Los algoritmos de la ARC confían en que las entradas de radar o sonar son correctas.
- **Explotación (Ataques de Evasión):** El ML adversario genera cambios mínimos e indetectables en las firmas electrónicas (ej. un buque), haciendo que los algoritmos de clasificación de la ARC identifiquen erróneamente a un activo hostil como uno neutral. Esto es un ataque directo a la percepción del sistema (Goodfellow, 2015)

Mando y Control

- **Vulnerabilidad:** Latencia en la Verificación Humana. La velocidad de la amenaza impide que el comandante verifique manualmente la información.
- **Explotación (Inteligencia Errónea):** El ML adversario contamina los *feeds* de inteligencia con datos sintéticos falsos que simulan un despliegue de fuerza enemigo incorrecto. Esto obliga al sistema C2 de la ARC a asignar recursos erróneamente (desinformación), logrando el efecto deseado sin un ataque físico.

Exposición Operacional

La exposición principal es la filtración de las bases de datos operacionales históricas de la ARC. Si el adversario obtiene estos datos de entrenamiento, puede:

- Crear un "Modelo de Defensa" que simula el comportamiento de la IA de la ARC.
- Predecir con alta precisión las tácticas preferidas y los tiempos de respuesta de la Armada (Sutton & Barto, 2020).

Desafío y Vulnerabilidad Institucional

La dependencia de *software* y *hardware* de IA de origen extranjero plantea el riesgo de Soberanía Tecnológica.

- **Efecto de Vulnerabilidad:** La adquisición de sistemas de IA "caja negra" expone el Mando y Control (C2) a sesgos programados o puertas traseras (*backdoors*), que podrían manipular una decisión crítica en un conflicto (Singer, 2021). La ARC queda a merced de la obsolescencia y los intereses geopolíticos de terceros, no de sus propias necesidades operacionales.

Brecha Tecnológica y Estrategia Asimétrica

La desigualdad tecnológica no se resuelve igualando la inversión en *hardware*, sino generando una ventaja en el *software*. Los países que logren alcanzar la singularidad en el ámbito militar podrían obtener una ventaja estratégica abrumadora, creando una profunda desigualdad en el poderío militar global.

- **Estrategia Asimétrica:** La ARC debe concentrar sus limitados recursos en algoritmos de fusión, procesamiento y guerra de la información desarrollados localmente, en lugar de replicar el *hardware* de potencias mundiales (RAND, Artificial intelligence and the future of defense: Strategy and policy considerations., 2022). Esto le permite crear una ventaja asimétrica en el ámbito cognitivo.
- **Enfoque de Desarrollo:** La solución es invertir en soberanía de *software*. Esto implica usar plataformas de código abierto e impulsar la formación de talento humano con capacidad para auditar y crear modelos de ML propios, mitigando así el riesgo de vulnerabilidades heredadas de la cadena de suministro tecnológica global.

La implementación de esta estrategia cierra la brecha de forma viable y protege al C2 de la manipulación externa.

3.5 Implicaciones Éticas

La IA mejora procesos como la optimización de recursos, diagnóstico médico, asignación de financiación y control administrativo. Sin embargo, enfrenta críticas éticas y exige supervisión humana (González Esteban, 2023). Su uso plantea desafíos sobre privacidad, sesgos y responsabilidad, especialmente en contextos militares. El empleo de sistemas autónomos en conflictos genera interrogantes sobre el cumplimiento del Derecho Internacional Humanitario. Organizaciones como RAND Corporation analizan sus riesgos (Forrest E. Morgan, 2020.). A medida que la IA se vuelve omnipresente, se requiere una reflexión ética profunda y marcos normativos claros para orientar su aplicación responsable en ámbitos civiles, institucionales y estratégicos como los de la ARC.

Tabla 16. Riesgos de la IA

Ético y legal	**Operacional**	**Estratégico**
Derecho de los conflictos armados Rendición de cuentas y responsabilidad moral Dignidad humana Derecho humano	Piratería informática, envenenamiento de datos y ataques adversarios. Accidentes y riesgos emergentes.	Umbrales Escalada Gestión Proliferación Estabilidad estratégica

Fuente: RAND Corporation

3.6 Financiación

Para materializar la implementación de la IA en la ARC se plantea su financiamiento, a través de los siguientes mecanismos:

1. Concentrar las compensaciones industriales (OFFSET) en materia de defensa nacional, estableciendo para las compras militares o de defensa una compensación

industrial de un 10% de transferencia de tecnología a la industria y a los actores del sistema nacional de ciencia, tecnología e innovación, liderados y seleccionados por la ARC para lograr su proceso de transformación y evolución tecnológica.

2. Llevar a cabo un Join venture (JV), mediante una colaboración estratégica entre entidades del sector privado (empresas tecnológicas, universidades, startups de IA) y el sector público (MDN, FFMM). Tendría como objeto aprovechar las tecnologías avanzadas para mejorar: la eficiencia operativa, seguridad nacional, análisis de datos y capacidades estratégicas colombianas. La ARC lideraría este salto cuántico tecnológico, estableciendo necesidades y supervisando su implementación con empresas tecnológicas especializadas como Google, IBM, Tesla, o startups locales y la participación de Universidades y centros de investigación, las cuales pueden contribuir con el desarrollo de algoritmos, investigaciones y prototipos, así como contar con contratistas de Defensa y empresas con experiencia en tecnologías militares y sistemas de defensa avanzados a nivel global.

   Un proyecto similar es el estadounidense JADC2 (Joint All-Domain Command and Control), donde la IA mejora la interoperabilidad de las FFMM. Existen colaboraciones internacionales entre la OTAN y algunos países de la Unión Europea, que están invirtiendo en IA aplicada a la seguridad y defensa, lo que podría ser un modelo para Colombia.

Conclusiones

1. La metodología empleada con un enfoque cualitativo, la revisión bibliográfica en fuentes científicas, políticas públicas y estrategias sobre la IA en Colombia, la realización de un

benchmark internacional a partir de los casos del conflicto ruso-ucraniano y la estrategia digital de Estonia permitió establecer de manera integral los desafíos, oportunidades y vulnerabilidades que enfrenta la ARC frente a la evolución de la IA, identificando las lecciones estratégicas y sus implicaciones en los dominios de la guerra.

2. La integración de la IA en la ARC es crucial para cerrar la brecha tecnológica y enfrentar amenazas en los diferentes dominios entre 2025 y 2030. Esta tecnología redefinirá la doctrina y fortalecerá las capacidades operativas, posicionándose como habilitador estratégico para la defensa y modernización institucional. Se propone financiar su implementación mediante compensaciones industriales (OFFSET) y Joint Venture, que articulen al sector privado (empresas, universidades, startups) con el público (MDN, FFMM, ARC).

3. La IA ofrece a la ARC oportunidades únicas para transformar sus operaciones, destacándose el salto hacia la digitalización, la mejora continua y la optimización de funciones como mando y control, inteligencia, sostenimiento, entre otras. Esto permitiría una mayor eficiencia en la toma de decisiones, optimización logística y capacidad operativa superior ante amenazas.

4. Los desafíos identificados requieren una respuesta sistémica: desde la modernización urgente de los sistemas de comunicaciones y logística, el fortalecimiento de la investigación y desarrollo para reducir la dependencia tecnológica, hasta la formación y reentrenamiento del capital humano. Los altos costos, la adaptación institucional y la ciberseguridad se consolidan como retos críticos para la implementación exitosa de soluciones de IA.

5. La investigación revela en prospectiva vulnerabilidades cibernética, por dependencia tecnológica, riesgos geopolíticos y brechas tecnológicas. La ARC debe enfocar sus esfuerzos

en robustecer la infraestructura digital, establecer nuevas estrategias para evitar posibles pérdidas de control operativo y enfrentar con éxito las amenazas híbridas en un entorno VICA-H.

REFERENCIAS

(MDN)., M. d. (2020). *Plan estratégico de desarrollo sectorial 2020-2024: Transformación y futuro de la seguridad y defensa.* Bogotá D.C.

Aguilar. (2023). La inteligencia artificial como herramienta del proceso de comando y control del comandante del teatro de operaciones. *https://cefadigital.edu.ar/bitstream/1847939/2929/1/TFI%2001-2023%20AGUILAR.pdf*.

Armada, M. -V. (06 de 2025). Obtenido de https://ventanillavirtual.armada.mil.co/es/content/mision-y-vision-armada-nacional-0.

Arteaga. (2019). Disrupción tecnológica y orden global. [Technological Disruption and Global Order. *Revista UNISCI https://www.proquest.com/scholarly-journals/disrupción-tecnológica-y-orden-global/docview/2407031098/se-2*, 109.

Barber, H. A. (1992). Desarrollo de liderazgo estratégico: La experiencia de la Escuela de Guerra del Ejército de los Estados Unidos. *Journal of Management Development*, 11.

Barletta, W. (2017). Cyberwar or Cyber-terrorism: The Attack on Estonia. *Cambridge: Massachusetts Institute of Technology*.

CEPAL. (2018). Datos, algoritmos y políticas: La redefinición del mundo digital. *Comisión Económica para América Latina*.

Charlán, J. (Noviembre de 2018). *https://www.esic.edu/rethink/tecnologia/vuca-h-sabes-lo-significa.* Obtenido de ¿Qué es el entorno VUCA + H y cómo afecta a las empresas?

Chopra, S. &. (2016). *Supply chain management: Strategy, planning, and operation (6th ed.).* Pearson.

Clausewitz, C. V. (1977). *De la Guerra.*

CNN. (2025). Así fue el audaz ataque con drones de Ucrania contra bases aéreas de Rusia. *CNN*.

Constituyente, A. A. (1991). *Constitución Política de Colombia, Artículo 217.* Bogotá D.C.

Cortes, V. F. (2023). Tácticas de guerra híbrida perpetradas por rusia contra ucrania desde el realismo defensivo y ofensivo. [tactics of hybrid warfare perpetrated by russia against ukraine from defensive and offensive realism]. *Revista Enfoques, 21(39), 73-101. https://www.proquest.com/scholarly-journals/tácticas-de-guerra-híbrida-perpetradas-por-rusia/docview/2915121959/se-2*.

DW. (2023). El grupo Wagner recluta a ucranianos presos en Rusia. *DW*.

FEM. (2025). *Informe sobre el futuro del empleo 2025: Perspectivas de competencias.*

FFMM. (febrero de 2023). *Manual Conjunto Fundamental 3.0: Operaciones Conjuntas.* Centro de Doctrina Conjunta FFMM.

Flashpoint. (2025). *Navegando las amenazas de mitad de año en 2025: Perspectivas del Índice de Inteligencia Global de Flashpoint*. Obtenido de https://flashpoint.io/blog/flashpoint-2025-global-threat-intelligence-index-midyear/?CRO3=%233007_control.

Forrest E. Morgan, B. B. (2020.). Aplicaciones militares de la inteligencia artificial. *https://www.rand.org/pubs/research_reports/RR3139-1.html*.

Freedman, L. (2019). Robots y drones. En La guerra futura: Un estudio del pasado y el presente. 495-522; 569-588.

Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? Small Wars & Insurgencies, 27(2), 282–301.

Ghasemi, A. &. (2021). Deep learning for cognitive radar and spectrum sharing. *IEEE Transactions on Cognitive Communications and Networking.*, 1-14.

González Esteban, E. &. (2023). Ética aplicada para una Inteligencia Artificial confiable. [Applied Ethics for Trutstworthy Artificial Intelligence] Daimon. . *https://doi.org/10.6018/daimon.577651*, 97-98.

Goodfellow, I. J. (2015). Explaining and harnessing adversarial examples. *Arxiv preprint*.

Heller, C. (June 2019). The Future of Naval Intelligence isArtificial. Vol 145/6/1,396. *https://www.usni.org/magazines/proceedings/2019/june/future-*.

Hernández Sampieri, R. F.-C. (2014). *Metodología de la investigación (6ª ed.).* . McGraw-Hill Education.

IBM. (2024). ¿Qué es la singularidad tecnológica? . *https://www.ibm.com/es-es/think/topics/technological-singularity.*

Insights, G. M. (Marzo de 2025). Inteligencia Artificial en el tamaño del mercado militar. *Global Market Insights Inc*.

Karspersky. (2025). *https://cybermap.kaspersky.com/es*. Obtenido de Ciberamenazas live map.

Li, Z. Z. (2023). Deep reinforcement learning for dynamic spectrum access in cognitive radio networks: A survey. . *Digital Communications and Networks.*, 448-460.

Linares. (2022). Principios éticos para el desarrollo de la inteligencia artificial y su aplicación en los sistemas de salud. *Artefactos https://doi.org/10.14201/art2022112137161*, 137-161.

Liu, B. Z. (2020). Bayesian network-based reasoning for clinical decision support systems: A systematic review. . *Artificial Intelligence in Medicine*, 106.

Mantilla, A. (2024). Disrupción de la inteligencia artificial en las ciencias náuticas. . *Observador del conocimiento, 9.*

Martel-Carranza, C. (2023). Inteligencia artificial vs. crecimiento económico. *Revista Innovación Empresarial (jul-dic) Universidad de Huanuco*, https://doi.org/10.37711/rcie.2023.3.2.28.

Mazza. (2023). *TECNOLOGÍA UAV (AERONAVES NO TRIPULADAS) PARA APLICARSE EN LA DEFENSA, VIGILANCIA Y CONTROL DE LOS ESPACIOS MARÍTIMOS.*

MDN. (2018). *Manual fundamental conjunto MFC 1.0: Doctrina conjunta.*

Mnih, V. K. (2015). Human-level control through deep reinforcement learning. *Nature*, 529–533.

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics, Volume 38, Number 8, April 19*.

News, B. (2022). Rusia y Ucrania: así era el Moskva, el buque insignia ruso hundido tras una explosión. *BBC NEWS.*

OTAN, J. 2.-0. (2014). *Estado Mayor Conjunto. Preparación de Inteligencia Conjunta del Entorno Operacional.*

Peñaloza, I. P. (2022). Artificial intelligence applications in military human resources management: A systematic review. . *Military Psychology*, 175-189.

PETIC, A. D. (2023). *Plan Estratégico de Tecnologías de la Información y de las Comunicaciones.*

Porcelli, A. (2022). La inteligencia artificial aplicada a la robótica en los conflictos armados. Debates sobre los sistemas de armas letales autónomas y la insuficiencia de los estándares del derecho internacional humanitario. *Estudios Socio-Jurídicos*.

RAND. (2022). *Artificial intelligence and the future of defense: Strategy and policy considerations.*

RAND. (2022). Artificial intelligence and the future of defense: Strategy and policy considerations.

Realpe. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. *Dialnet*.

Singer, P. W. (2021). *Ghost fleet: A novel of the next world war. Eamon Dolan/Houghton Mifflin Harcourt.*

Sutton, R. S. (2020). *Reinforcement learning: An introduction (2nd ed.).* The MIT Press.

Sutton, R. S. (2020). *Reinforcement learning: An introduction (2nd ed.). .* The MIT Press.

Tao, F. &. (2017). Digital twin shop-floor: A new way to smart manufacturing. . *IEEE/ASME Transactions on Mechatronics.*, 2401-2411.

Turing, A. (1950). Computing Machinery and Intelligence. *Revista MIND Oxford Academics*.

Wagstaff, J. (2023). Fondo Monetario Internacional, un nuevo modelo de ejército. *https://www.imf.org/es/Publications/fandd/issues/2023/12/Case-Studies-New-model-army-Jeremy-Wagstaff*.

Waltz, E. &. (2023). *Multisensor data fusion.* Artech House.

Xroad. (2025). *Historia X-road Estonia*. Obtenido de https://x-road.global/xroad-history.