Capítulo 6

Oportunidades y desafíos de la incorporación de algoritmos predictivos en el sistema de inteligencia estratégica de las Fuerzas Militares de Colombia*

https://doi.org/00.00000/0000000000000.06

Flor María Sánchez Castro

Francisco Javier Guevara Arismendy

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente capítulo, examina las oportunidades y desafíos de incorporar los algoritmos predictivos en los sistemas de inteligencia estratégica militar, identificando la interacción e impacto en la toma de decisiones. A través del análisis bibliométrico, con un enfoque cualitativo y un alcance descriptivo de modelos de inteligencia artificial en el área de algoritmos predictivos, se argumenta cómo apoyan el proceso de toma de decisiones, a través del procesamiento de altos volúmenes de datos provenientes de múltiples fuentes. Adicionalmente, se identifican las oportunidades relevantes en términos de una automatización de análisis complejos, presentando desafíos tales como la explicabilidad, la calidad de los datos, la fiabilidad de las decisiones que se toman de manera autónoma y las implicaciones legales de su implementación. Este análisis contribuye al fortalecimiento de las capacidades prospectivas y anticipativas de la inteligencia estratégica militar, proporcionando insumos técnicos y conceptuales para la toma de decisiones basada en evidencia.

Palabras clave: algoritmos predictivos; inteligencia artificial; inteligencia estratégica; prospectiva operativa; sistemas.

---

* Capítulo de libro resultado del proyecto de investigación "Desafíos contemporáneos en la investigación para la formación y la doctrina en seguridad y defensa de la Escuela Superior de Guerra: Reingeniería VINVE FASE I", del grupo de investigación "Centro de Gravedad" de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (Minciencias) y registrado con el código COL0104976. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Flor María Sánchez Castro

Capitán de Corbeta de la Armada Nacional de Colombia. Ingeniera industrial, Universidad Industrial de Santander, Colombia. Especialización en Gestión de Desarrollo Administrativo, Universidad Militar Nueva Granada. Estudiante de la Especialización Seguridad y Defensa Nacionales y estudiante del Curso de Información Militar, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

Orcid: https://orcid.org/0009-0001-0208-8371 - Contacto: flor.sanchez@esdeg.edu.co

Francisco Javier Guevara Arismendy

Capitán de Corbeta de la Armada Nacional de Colombia. Ingeniero de sistemas, Universidad de Antioquia, Colombia. Magíster en Seguridad Informática, UNIR. Estudiante de la Especialización Seguridad y Defensa Nacionales y estudiante del Curso de Información Militar, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

Orcid: https://orcid.org/0009-0004-6957-1984 - Contacto: francisco.guevara@esdeg.edu.co

Citación APA: Sánchez-Castro, F. M., & Guevara-Arismendy, F. J. (2025). Oportunidades y desafíos de la incorporación de algoritmos predictivos en el sistema de inteligencia estratégica de las Fuerzas Militares de Colombia. En J. Jiménez-Reina, A. Serrano-Cuervo, & C. P. Garay-Acevedo (Eds.), *Nuevas generaciones y Fuerzas Militares: Puentes estratégicos para la construcción de la Nación* (pp. XX-XX). Sello Editorial ESDEG. https://doi.org/00.00000/0000000000000.06

NUEVAS GENERACIONES Y FUERZAS MILITARES: PUENTES ESTRATÉGICOS PARA LA CONSTRUCCIÓN DE LA NACIÓN
ISBN impreso: 978-000-00000-0-0
ISBN digital: 978-000-0000-0-0
DOI: https://doi.org/00.00000/0000000000000.06
Colección Seguridad y Defensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Introducción

La inteligencia estratégica implica capacidades analíticas, anticipación y prospectiva, desarrollando la formulación de políticas de seguridad nacional, mediante la combinación de múltiples fuentes de información y análisis sistémicos (Phythian, 2021; Shapira, 2020a). En el contexto global, ha dejado de estar centrada en la obtención de información sobre capacidades militares de un adversario, para evolucionar hacia un proceso multidimensional adaptado a las nuevas amenazas híbridas, asimétricas y cibernéticas. Este cambio implica pasar de una recolección tradicional de información a un análisis sistémico (Shapira, 2020b).

Parte de los elementos de su evolución, es la incorporación de inteligencia artificial (IA), particularmente los algoritmos predictivos, modelos computacionales diseñados para identificar patrones en datos históricos y proyectar escenarios futuros, optimizando la anticipación de amenazas y oportunidades en contextos complejos, y tomar decisiones basadas en datos en entornos de alta incertidumbre (Rashid et al., 2022). Desde el punto de vista normativo, Colombia ha establecido la Política Nacional de Inteligencia Artificial 2023–2030, que busca incentivar el uso ético y estratégico de tecnologías emergentes. Sin embargo, enfrenta retos para su implementación debido a las brechas digitales, así como su debilidad en el marco normativo para las fuerzas militares (FF.MM.) (Zambrano González, 2025; Mindefensa, 2024).

Diversos estados han avanzado en la implementación de estas tecnologías. Por ejemplo, el Reino Unido ha definido la IA como una capacidad estratégica de defensa (Ministry of Defence (UK), 2022); Israel, ha desarrollado arquitecturas de defensa predictiva para sus fuerzas armadas en zonas de conflicto (Lappin, 2023); Estados Unidos, ha desarrollado el proyecto Maven del Departamento de Defensa para la identificación de amenazas mediante el procesamiento automático de imágenes satelitales (Allen, 2017; Pellerin, 2017).

En América Latina, países como Chile y Brasil han iniciado procesos de integración de IA en tareas de vigilancia fronteriza y análisis de amenazas internas (Quiñones-Sigala, 2023). Colombia, ha desarrollado iniciativas institucionales en el marco de su política nacional de transformación digital del sector defensa, con énfasis en la modernización de

sistemas C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), vigilancia predictiva, y análisis de datos masivos (NUVU, 2024; Mindefensa, 2024).

Sin embargo, su implementación enfrenta retos estructurales, tales como la falta de interoperabilidad entre plataformas tecnológicas, la formación y desarrollo de competencias del talento humano en analítica avanzada y ética de la IA, como también las restricciones y desarticulación en el ámbito legal y normativo (CONPES, 2020), aunado a la falta de integración doctrinal (Cancelado, 2019), dependencia tecnológica (Jaramillo, J. 2024), riesgos de ciberseguridad; factores que limitan la adopción de estas herramientas en ambientes operacionales críticos (Camacho et al., 2024; Bastos Martínez, 2019).

El análisis desde un enfoque de inteligencia estratégica global señala que la eficacia para la implementación de los algoritmos predictivos depende de su articulación con las estructuras de mando y control, para operar bajo principios de flexibilidad, interoperabilidad y procesamiento en tiempo real. Estas capacidades deben estar alineadas con doctrinas nacionales, políticas públicas de innovación y principios éticos internacionales, particularmente a los derechos humanos, la privacidad y la transparencia (Jaramillo, 2024; McDowell et al., 2024). La implementación efectiva, requiere una visión integral que combine infraestructura tecnológica, talento humano capacitado, doctrina adaptativa, normatividad clara y articulada con los avances tecnológicos y voluntad política sostenida.

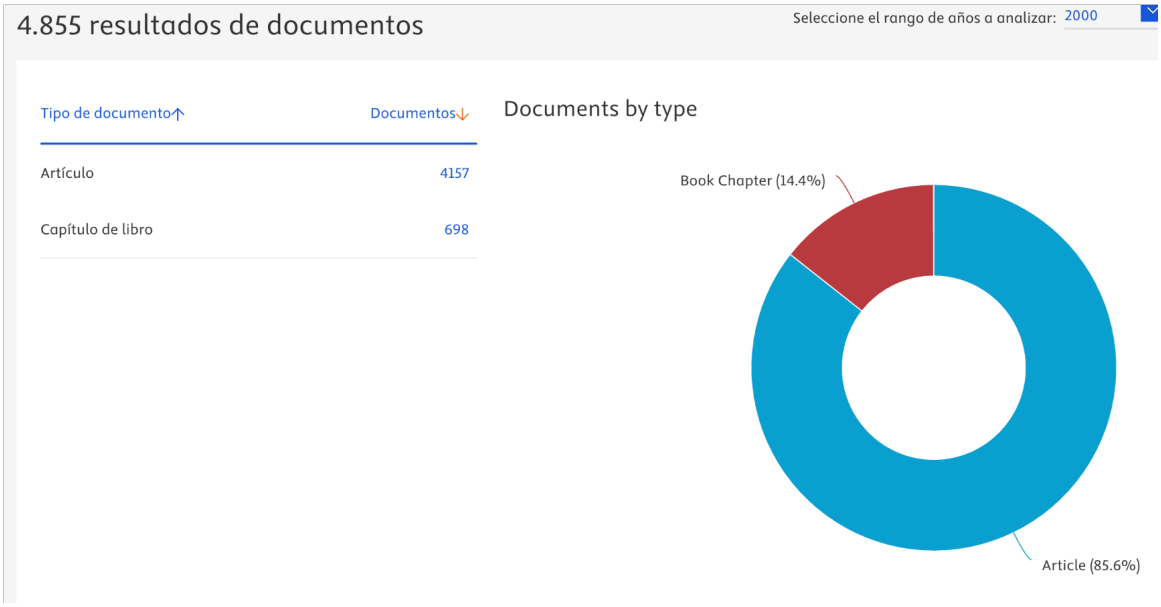
El método de aprendizaje es mediante un enfoque cualitativo de alcance descriptivo, orientado al objetivo de analizar oportunidades y desafíos de la incorporación de algoritmos predictivos en los sistemas de inteligencia estratégica de las FF.MM. de Colombia, se examinan conceptos, significados, comportamiento y dinámicas de fenómenos asociados al uso de inteligencia artificial en el ámbito militar; mientras que el alcance descriptivo, permite caracterizar el estado del arte y las prácticas emergentes en este ámbito (Villamin et al., 2024). Complementariamente, se utilizó la revisión bibliográfica sistemática, con apoyo de herramientas como VOSviewer de análisis bibliométrico y búsqueda de información, realizada en bases de datos científicas de alto impacto (Scopus, Web of Science, IEEE Xplore y SpringerLink), permitió seleccionar artículos publicados entre 2020 y 2025, en inglés y español, con el fin de asegurar el rigor académico y pertinencia temática.

A continuación, se presenta en primera lugar los fundamentos teóricos y modelos de algoritmos predictivos relevantes para su incorporación en sistemas de inteligencia estratégica; posteriormente, se abordará la clasificación de los tipos de algoritmos predictivos aplicados en sistemas de inteligencia estratégica, destacando su utilidad en la toma de decisiones a nivel estratégico; y finalmente, se caracterizaran las capacidades institucionales y los factores organizacionales que condicionan la integración de algoritmos predictivos en el sistema de inteligencia estratégica de las FF.MM. de Colombia.

Teorías de Algoritmos Predictivos para la incorporación dentro de los sistemas de Inteligencia Estratégica en las Fuerzas Militares

En los años recientes, específicamente en el periodo entre 2020 y 2025, se evidencia un creciente interés y consolidación sostenida de estudios científicos para la implementación de la inteligencia artificial (IA), el área de los algoritmos predictivos, aplicados en la toma de decisiones de contextos estratégicos. Un análisis bibliométrico realizado sobre una muestra de 4.855 publicaciones indexadas en Scopus (4.157 artículos y 698 capítulos de libro) como se ve en la Figura 1, permitió evidenciar una producción científica en crecimiento sostenido desde el 2020 (210 documentos) hasta alcanzar un máximo en el 2024 con 1.119 documentos, la Figura 2 refleja una estructura densa de colaboración internacional con clústeres de investigación que giran principalmente en torno a inteligencia artificial, aprendizaje de máquinas y modelos predictivos, los cuales conectan con áreas aplicadas como ciberseguridad, inteligencia multifuente y toma de decisiones en tiempo real.

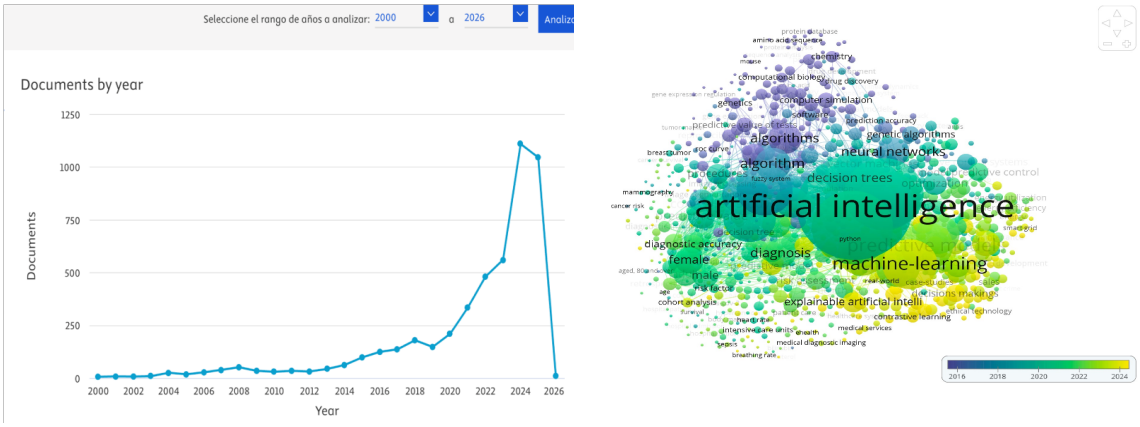
Figura 1. Tipos de Documento en el Estudio Bibliométrico.



Fuente: Resultados Estudio Bibliométrico Scopus.

Adicionalmente, la concentración de publicaciones en torno a los conceptos de inteligencia artificial, algoritmos predictivos, seguridad estratégica y aprendizaje de máquinas (machine learning), así como también una red de conocimiento distribuido en 4.813 autores únicos y 1.331 revistas científicas especializadas, evidencia una consolidación teórica y práctica en torno al desarrollo de capacidades predictivas en escenarios complejos.

Figura 2. Producción Científica en Crecimiento Sostenido por Año y Palabras Claves.

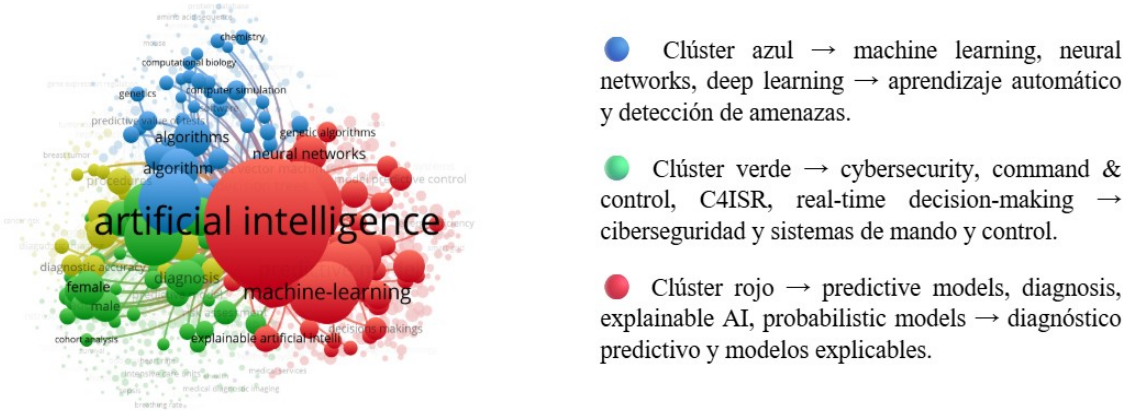


Fuente: Resultados Estudio Bibliométrico Scopus y VOSviewer.

Los mapas bibliométricos revelaron tres clústeres principales, Figura 3: (i) uno centrado en aprendizaje automático y redes neuronales con aplicaciones en la detección de amenazas, (ii) un segundo enfocado en ciberseguridad y sistemas C4ISR, y (iii) un tercero orientado a diagnóstico predictivo y modelos explicables. En paralelo, el análisis por países mostró la concentración de la producción en Estados Unidos, China, India y Reino Unido, mientras que en América Latina destacan Brasil y Chile como polos emergentes de investigación.

Estas evidencias reflejan cómo la literatura científica está consolidando un ecosistema digital interdependiente, donde la analítica predictiva y la inteligencia computacional se integran progresivamente en los sistemas de defensa y seguridad estratégica (Ayub et al., 2022; Sarker et al., 2023; Habeeb, 2024; Danish, 2024).

Figura 3. Mapas Bibliométricos Tres Clústeres y Producción en Estados.



Fuente: Resultados Estudio Bibliométrico Scopus y VOSviewer.

Esta revisión bibliográfica fue posible mediante la aplicación de la herramienta VOSviewer, evidenciando patrones de colaboración y temáticas emergentes en áreas como aprendizajes automáticos, ciberseguridad y análisis de inteligencia multifuente, facilitando la visualización de redes de coautoría, co-citación y clústeres temáticos, mostrando una estructura densa de colaboración científica en torno a estos temas (Van Eck & Waltman, 2010).

Uno de los enfoques o métodos más frecuentes en la producción académica es el uso de técnicas de aprendizaje automático, ya sea supervisado o no, en combinación con modelos de aprendizaje profundo y probabilísticos. Estas tecnologías, permiten extraer patrones desde grandes volúmenes de datos y construir sistemas de alerta temprana con capacidades de simulación prospectiva. La red de términos clave obtenida con VOSviewer, mostró una fuerte conexión entre estos enfoques y áreas aplicadas, como inteligencia multifuente y análisis de amenazas, lo cual valida su aplicabilidad directa a la inteligencia estratégica en el contexto militar (He et al., 2020; Preece et al., 2019; Autio et Al., 2020).

De igual forma, se observa un fuerte vínculo entre la inteligencia computacional y la ciberseguridad, especialmente en contextos operacionales. El análisis de frecuencia de autores y términos, basado en las métricas de Scopus, permite identificar nodos centrales en la literatura que conectan analítica predictiva, ciberdefensa y toma de decisiones en tiempo real. Estas relaciones bibliográficas, evidencian una tendencia clara hacia la construcción de ecosistemas digitales interdependientes, donde la capacidad de procesamiento de información se integra con las estructuras de mando y control (Ayub et al., 2022; Danish, 2024; Sarker et al., 2023; Habeeb, 2024; Creswell & Creswell, 2018).

Finalmente, el concepto de data-driven decision-making (DDDM), emerge como hilo conductor de las tendencias bibliográficas recientes. La minería de texto sobre los títulos de publicaciones reveló una preocupación por fortalecer los sistemas de inteligencia a partir de evidencia empírica y analítica. Adicionalmente, el análisis de coautoría evidencia que en países como Colombia se requiere fortalecer la producción científica en esta área. Este hallazgo señala la necesidad de consolidar capacidades institucionales que integren tecnologías emergentes, infraestructura interoperable, y talento humano con formación ética y técnica, como condición necesaria para transitar de un enfoque reactivo a uno verdaderamente anticipativo (Camacho et al., 2024; Jaramillo, 2024).

Inteligencia estratégica

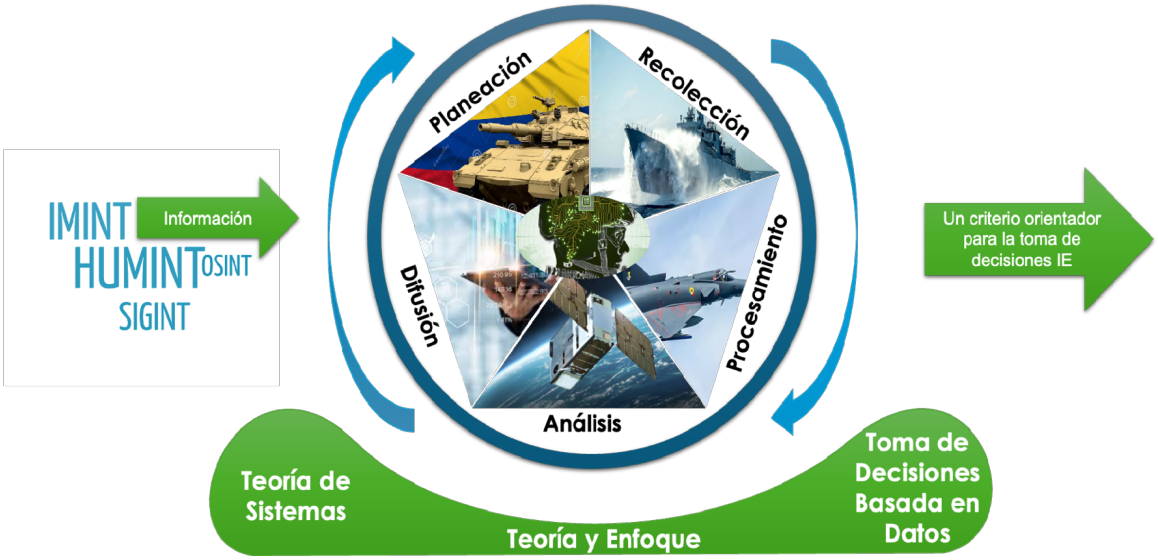
La inteligencia estratégica constituye una función crítica dentro de los sistemas de seguridad y defensa, orientada a anticipar amenazas, identificar riesgos sistémicos y apoyar la toma de decisiones al más alto nivel. Ardila-Castro y Jiménez (2020) definen la

inteligencia estratégica como un proceso de gestión del conocimiento que integra fuentes multiescalares de información con el objetivo de producir análisis prospectivos para la formulación de políticas y acciones de seguridad.

Las funciones de la inteligencia estratégica incluyen: la recolección y procesamiento de información multifuente, como la inteligencia humana (HUMINT), de señales (SIGINT), de imágenes (IMINT) y de fuentes abiertas (OSINT); el análisis de escenarios geopolíticos y amenazas híbridas, como el terrorismo transnacional, el crimen organizado o los ciberataques; y la generación de productos de inteligencia que apoyen la toma de decisiones en los niveles operacional, táctico y estratégico (Joint Chiefs of Staff, 2022).

Desde el punto de vista doctrinal, la inteligencia estratégica se estructura mediante el ciclo de inteligencia, compuesto por las fases de planeación y dirección, recolección, procesamiento y explotación, análisis y producción, y diseminación de la información, (ver Figura 4). Este ciclo, es recogido tanto en doctrinas OTAN (NATO, 2016) como en la Ley 1621 de 2013 de Colombia, donde se establece un marco normativo para la actividad de inteligencia y contrainteligencia del Estado.

Figura 4. Sistema de inteligencia estratégica basado en datos.



Fuente: Elaboración propia basada en la Teoría General de Sistemas (Bertalanffy, 1968) y el enfoque de Toma de Decisiones Basada en Datos (Provost & Fawcett, 2013).

En cuanto a metodologías, la inteligencia estratégica incorpora enfoques mixtos de análisis, combinando técnicas cualitativas (análisis de redes sociales, discursos y matrices de actores) y cuantitativas, haciendo uso de herramientas y/o metodologías tales como modelos estadísticos, minería de datos y aprendizaje automático, con el fin de construir escenarios robustos de anticipación. Modelos como el Análisis de Indicadores y Advertencias (I&W), el Análisis de Hipótesis Múltiples (ACH), o la metodología Structured Analytic Techniques (SATs) proponen marcos rigurosos para reducir el sesgo cognitivo y aumentar la fiabilidad del producto de inteligencia (Heuer, 1999; Pherson & Pherson, 2021).

La incorporación de modelos predictivos apoyados en inteligencia artificial permite analizar patrones de comportamiento, anticipar movimientos de actores hostiles, y generar alertas tempranas en escenarios altamente dinámicos y volátiles (Bello et al., 2024; Hilton-Shomron, 2024). Estas técnicas se alinean con la metodología de DDDM, que enfatiza la toma de decisiones sustentadas en evidencia empírica procesada mediante IA (Provost & Fawcett, 2013).

En el plano procedimental, los sistemas C4ISR permiten la integración en tiempo real de las fuentes de datos estratégicas y tácticas. Esta arquitectura soporta tecnológicamente la inteligencia estratégica multiescala, promoviendo interoperabilidad entre unidades y acceso instantáneo a los productos de inteligencia (He et al., 2020; Preece et al., 2019). La correcta operación de estos sistemas requiere procedimientos para proteger la información, la trazabilidad de los procesos analíticos y la coordinación interagencial.

Doctrinas emergentes, como la Doctrina Damasco del Ejército Nacional de Colombia, reconocen la importancia de la inteligencia estratégica para el planeamiento operacional y la gestión del entorno, promoviendo un enfoque holístico que articula capacidades tecnológicas, humanas y doctrinales (Bastos Martínez, 2019; Cancelado, 2019).

La transición hacia una inteligencia estratégica basada en datos requiere el fortalecimiento de capacidades analíticas avanzadas, plataformas interoperables y marcos doctrinales dinámicos que integren la transformación digital con la misión institucional. En este contexto, la incorporación de algoritmos predictivos y técnicas de analítica avanzada no solo optimiza el proceso de inteligencia, sino que potencia su función anticipativa,

facilitando respuestas estratégicas eficaces y oportunas ante amenazas complejas (Gnodle & Verran, 2021; Probasco et al., 2025).

Algoritmos predictivos

La inteligencia artificial (IA) es un campo de la informática orientado al diseño de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de patrones, el razonamiento lógico, la planificación, el aprendizaje y la toma de decisiones. Esta disciplina ha evolucionado significativamente desde sus orígenes, integrando múltiples subcampos que permiten a las máquinas simular procesos cognitivos complejos y adaptarse a entornos cambiantes mediante el análisis de datos (Russell & Norvig, 2021). Entre las principales ramas y técnicas de la IA, se destacan:

- Lógica simbólica y sistemas expertos, que buscan representar conocimiento mediante reglas y ontologías.
- Procesamiento de lenguaje natural, orientado a la comprensión y generación de lenguaje humano.
- Robótica e inteligencia perceptiva, encargadas de la interacción física con el entorno.
- Visión por computador, utilizada para interpretar imágenes y videos.
- Aprendizaje automático (Machine Learning, ML), que permite a los sistemas aprender a partir de datos.
- Aprendizaje profundo (Deep Learning), una subrama del ML basada en redes neuronales artificiales de múltiples capas.

Los algoritmos predictivos son una subcategoría clave dentro del aprendizaje automático, y son ampliamente utilizados para identificar patrones ocultos, establecer correlaciones complejas y anticipar eventos futuros. Estas herramientas son especialmente relevantes en contextos donde la toma de decisiones debe ser rápida, basada en grandes volúmenes de datos y adaptada a condiciones de incertidumbre (Kelleher et al., s.f.; Probasco et al., 2025).

Los algoritmos predictivos son modelos computacionales que permiten inferir comportamientos o eventos futuros a partir del análisis de patrones en datos históricos o en

tiempo real. Se fundamentan en técnicas estadísticas, de aprendizaje automático y minería de datos, que transforman grandes volúmenes de datos en conocimiento útil para la toma de decisiones (Kelleher et al., s.f.; Goodfellow et al., 2016).

Entre los tipos de algoritmos predictivos más relevantes en el ámbito de la inteligencia estratégica se encuentran:

- Modelos supervisados, como la regresión logística, los árboles de decisión, las máquinas de soporte vectorial y las redes neuronales artificiales (ANN), que se entrenan con datos etiquetados para realizar clasificaciones o predicciones.
- Modelos no supervisados, como el clustering y la detección de anomalías, que descubren estructuras ocultas en los datos sin necesidad de etiquetado previo.
- Modelos basados en series temporales, como ARIMA o Prophet, especialmente útiles para predecir eventos futuros a partir de secuencias cronológicas (Bello et al., 2024; Marr, 2016).
- Modelos de aprendizaje profundo, como las redes neuronales recurrentes (RNN) o las redes convolucionales (CNN), aplicados a contextos complejos como reconocimiento de imágenes satelitales o análisis de video vigilancia en tiempo real (Goodfellow et al., 2016).

La aplicación de algoritmos predictivos comprende varias fases: recolección y preprocesamiento de datos, selección del modelo, entrenamiento y validación, y la interpretación de los resultados. Los algoritmos predictivos, también se articulan con otras tecnologías emergentes, como el Big Data y la computación en la nube, que posibilitan el procesamiento en tiempo real de información masiva, ampliando su utilidad operativa y estratégica.

En escenarios militares, su implementación permite identificar patrones de comportamiento hostil, anticipar rutas de desplazamiento de actores ilegales, o predecir amenazas cibernéticas mediante análisis multifuente (Hilton-Shomron, 2024; Sánchez, 2025). Su incorporación a plataformas C4ISR fortalece la capacidad de las FF.MM. para actuar proactivamente en entornos caracterizados por alta incertidumbre, velocidad y complejidad (He et al., 2020; Preece et al., 2019; NUVU, 2024).

Modelos teóricos relevantes

Teoría de Sistemas Adaptativos Complejos

Los sistemas adaptativos complejos, son estructuras dinámicas compuestas por elementos interdependientes, que interactúan entre sí y su entorno, generando comportamientos emergentes. En el contexto de defensa, esta teoría permite analizar la inteligencia estratégica como un sistema donde la información, la tecnología, la doctrina y los actores humanos coexisten en constante adaptación (Liwång et al., 2023).

Según Autio et Al. (2020), los ecosistemas digitales funcionan como sistemas interconectados cuya resiliencia y capacidad de adaptación dependen de la calidad de las relaciones entre sus nodos. En este sentido, la incorporación de algoritmos predictivos en entornos de defensa puede reforzar la capacidad del sistema para responder a estímulos externos y generar adaptaciones en tiempo real.

Teoría del Conocimiento Organizacional en Inteligencia

La generación de conocimiento dentro de las organizaciones militares no es un proceso automático, sino que depende de estructuras, normas y prácticas que permiten transformar datos en información y convertirla en conocimiento útil. En este sentido, la inteligencia estratégica requiere no solo herramientas tecnológicas, sino también procesos epistemológicos institucionalizados para facilitar la apropiación del conocimiento. El análisis bibliométrico de estrategias de conocimiento en estructuras de inteligencia destaca los vacíos en la investigación entre gestión del conocimiento y estructuras de inteligencia institucional (Budeanu, 2023).

Los algoritmos predictivos deben entenderse como herramientas entre la información y la acción estratégica. Su utilidad aumenta cuando se integran en procesos organizacionales de aprendizaje, análisis colaborativo y gestión del conocimiento. Existen estudios previos sobre inteligencia y epistemología, como el trabajo de Pili (2019), los análisis bibliométricos sobre la aplicación de aprendizaje automático en entornos militares son cada vez más relevantes, resaltando la necesidad de una inteligencia artificial

explicable, integrada con estructuras organizacionales (Galán et al., 2024; Cortés González, 2019).

Enfoques de Big Data y Analítica Predictiva

El paradigma del Big Data ha transformado la forma en que las instituciones de defensa procesan la información. Caracterizada por el manejo de grandes volúmenes de datos (volumen), rápida generación (velocidad), variedad de formatos (variedad), necesidad de veracidad y valor estratégico (5Vs) (Davenport, 2014). La analítica predictiva, por su parte, permite derivar conclusiones anticipadas mediante el uso de modelos matemáticos y estadísticos, orientando decisiones con base en evidencia (Han et al., 2012).

En las FF.MM. de Colombia, el uso de enfoques de Big Data y analítica predictiva se evidencia en la implementación progresiva de sistemas C4ISR, donde se consolidan fuentes multiescalares y se integran modelos que priorizan alertas y optimizan decisiones estratégicas (Alcántara-Suárez, 2023; NUVU, 2024).

Clasificación de los tipos de algoritmos predictivos aplicados en sistemas de inteligencia estratégica, destacando su utilidad en la toma de decisiones a nivel estratégico

La incorporación de sistemas de IA, específicamente algoritmos predictivos en los sistemas de inteligencia estratégica de las FF.MM., permite evolucionar el proceso de gestión y análisis de datos, interpretación de escenarios operacionales y toma de decisiones críticas en contextos de alta complejidad. Esta transformación, ha sido posible gracias al avance de tecnologías tales como el aprendizaje automático (machine learning), el análisis de grandes volúmenes de datos (big-data), el modelado estadístico, entre otros. Los sistemas de algoritmos predictivos permiten procesar grandes volúmenes de información de múltiples fuentes, tales como SIGINT, IMINT, HUMINT y OSINT, para generar información de valor de forma oportuna, permitiendo anticipar riesgos emergentes y generar conocimiento como apoyo al proceso de toma de decisiones.

Esta sección presenta una clasificación de algoritmos predictivos potencialmente aplicables en el ámbito militar, particularmente en el campo de la inteligencia estratégica. Esta clasificación examina su funcionalidad técnica, además del enfoque de la Toma de Decisiones Basada en Datos (DDDM), evalúa su capacidad para transformar grandes volúmenes de datos en información accionable, fortaleciendo así el proceso de anticipación de amenazas y decisiones estratégicas. Así mismo, el análisis considera la viabilidad operativa y las implicaciones derivadas de su integración en los sistemas de inteligencia estratégica.

Clasificación general de algoritmos predictivos

En términos generales, los algoritmos predictivos se agrupan en cinco categorías principales, las cuales se describen a continuación.

Algoritmos supervisados

Estos algoritmos utilizan datos etiquetados para entrenar los modelos de predicción. Son útiles en la inteligencia estratégica para la clasificación de riesgos en zonas geográficas, predicción de eventos hostiles a partir de patrones históricos, priorización de objetivos en entornos complejos. Entre los modelos más aplicados están:

- *Árboles de decisión (Decision Trees):* permiten la creación de estructuras de escenarios, propuestas en función de las variables de entrada. Son útiles para para decisiones rápidas a escala táctica.
- *Regresión logística:* se utilizan para determinar la probabilidad de aparición de amenazas en eventos específicos.
- *Redes neuronales artificiales (ANN):* son modelos que permiten encontrar patrones no lineales complejos dentro de grandes volúmenes de datos.

Estos modelos de algoritmos han sido ampliamente utilizados en sistemas militares para clasificar eventos, identificar amenazas y categorizar situaciones de riesgo. Un ejemplo de su aplicación es el proyecto *Maven* del Departamento de Defensa de los EE.UU., este proyecto identifica blancos militares mediante el procesamiento de imágenes obtenidas por drones, Este sistema ha permitido la automatización de tareas que antes

requerían la participación de cientos de analistas, mejorando la velocidad de reacción y precisión al seleccionar los blancos (Allen, 2017).

Este tipo de modelos también ha sido aplicado en el análisis de imágenes satelitales, para detectar bases militares e infraestructuras críticas en áreas hostiles, con niveles de precisión superiores al 90 % (Surma, 2024), aunque su uso implica la necesidad de disponer de grandes volúmenes de datos etiquetados, existe el riesgo de sesgos o la baja explicabilidad de los resultados; factores que afectan la confianza de los operadores humanos (Goodfellow et al., 2016).

Algoritmos no supervisados

Se utilizan para la detección de patrones ocultos en datos sin etiquetas. Tienen un papel clave en aquellos casos donde la información es parcial, ambigua o no está estructurada:

- *Clustering (K-Means, DBSCAN):* agrupan datos por similitudes, permiten detectar células logísticas o redes de actores.
- *Análisis de componentes principales (PCA):* reducción de dimensionalidad a partir de información, permiten visualizar comportamientos anómalos.
- *Detección de anomalías:* permiten detectar desviaciones en comportamientos esperados, tal como tráfico inusual de comunicaciones o movimientos logísticos sospechosos.

Los modelos no supervisados, como los modelos K-means o Density Based Spatial Clustering of Applications with Noise (DBSCAN) y la detección de anomalías, son ampliamente utilizados en la vigilancia electrónica y en defensa cibernética. En el contexto de la iniciativa Anomaly Detection at Multiple Scales (ADAMS) de Defense Advanced Research Projects Agency (DARPA), se hace uso de estos algoritmos para detectar amenazas internas en redes militares, permitiendo descubrir patrones de comportamiento anómalo en el uso de sistemas de información (Imran, 2025).

Este tipo de modelos, son efectivos para detectar estructuras ocultas o identificar actividades sospechosas en entornos no etiquetados, o priorizar los eventos a utilizar en el análisis. Sin embargo, presentan limitaciones tales como: elevados falsos positivos, dificultad de interpretación de los clústeres o la sensibilidad a los parámetros de configuración, lo cual puede disminuir la eficiencia y efectividad operativa. Su mayor

potencial, está en su utilización como filtros de alerta temprana en los sistemas SIGINT, OSINT y en vigilancia de redes (He et al., 2020; Preece et al., 2019).

Algoritmos semi-supervisados

Los algoritmos semi-supervisados combinan propiedades de los enfoques supervisados y no supervisados, aprovechando las fortalezas del entrenamiento a partir de un número pequeño de datos etiquetados y un amplio conjunto de datos no etiquetados. Esta característica, es especialmente relevante en contextos de inteligencia estratégica, donde la obtención de etiquetas fiables puede ser costosa en términos de tiempo, recursos y seguridad, sensible debido al riesgo de comprometer fuentes, capacidades operativas y a la naturaleza de la información.

En arquitecturas como C4ISR, los algoritmos semi-supervisados ofrecen una oportunidad estratégica al reducir los costos asociados al etiquetado manual, optimizando el uso de datos etiquetados junto con grandes volúmenes de datos no etiquetados, aumentando la capacidad de detección de patrones y la previsión de riesgos, robusteciendo los sistemas de alerta temprana y toma de decisiones estratégicas en situaciones de alta incertidumbre (Williams & Qian, 2025; Rizve et al., 2021; Shu et al., 2022).

Dentro de los retos para su implementación se destaca la dependencia de la selección de ejemplos de referencia y la dependencia de la calidad, dado que, si un conjunto de etiquetas está sesgado o incorrecto, puede propagar errores a través del modelo. Sin embargo, esta metodología sigue siendo una oportunidad estratégica para minimizar costos de etiquetado, acelerar el desarrollo de sistemas adaptativos y reducir la dependencia de la supervisión humana en entornos de inteligencia estratégica (Shu et al., 2022).

Modelos de series temporales

Estos modelos permiten proyectar tendencias y eventos futuros basándose en datos cronológicos. Los modelos más empleados se encuentran:

- *ARIMA y Prophet:* útiles para anticipar ataques recurrentes o desplazamientos de grupos armados.
- *Redes Neuronales Recurrentes:* su aplicación se encuentra ligada a la vigilancia ISR, analizando patrones temporales complejos (Hilton-Shomron, 2024).

Estos modelos, permiten la simulación de escenarios prospectivos, apoyando la generación de alertas tempranas y la planificación anticipada. Esta es una importante herramienta en la inteligencia estratégica, dado que permite analizar datos con una secuencia temporal, identificando tendencias, patrones recurrentes y ciclos, con el fin de generar simulaciones confiables sobre posibles eventos futuros, permitiendo anticipar incidentes cibernéticos, aumento de actividades hostiles o desplazamientos adversos, lo que mejora la planeación preventiva y distribución oportuna de recursos militares (Landauer et al., 2025; Baboş et al., 2022).

Modelos como ARIMA, Prophet y RNN, han sido aplicados exitosamente en la predicción de patrones operacionales y de gasto militar, alcanzando precisión y minimizando la incertidumbre en la toma de decisiones (Sharma & Phulli, 2020). En contextos de seguridad fronteriza, estos modelos permiten anticipar desplazamientos de actores armados ilegales, picos de violencia o cambios en las rutas del narcotráfico, mediante el análisis de eventos históricos (Bello et al., 2024).

La aplicabilidad de estos modelos se ha extendido también al campo de la ciberdefensa, anticipando ataques distribuidos de denegación de servicio (DDoS) y análisis de registros de eventos en tiempo real, permitiendo detectar señales de preparación del ataque y ganar tiempo defensivo ante amenazas masivas (Neira et al., 2023). Así mismo, investigaciones como las de Alfatemi et al. (2024) han mostrado que el uso de redes neuronales profundas (ResNets), combinadas con técnicas de sobremuestreo como SMOTE, pueden alcanzar tasas de precisión superiores al 99 % en la detección temprana de este tipo de ataques.

El principal reto de esta categoría es la dependencia de datos consistentes y actualizados, además de la dificultad para identificar eventos disruptivos o emergentes, ya que los patrones de análisis evolucionan constantemente (Becerra-Suárez et al., 2024). De igual forma, existen modelos que alcanzan un rendimiento limitado generado por la calidad del conjunto de datos disponibles (Surma, 2024).

Aprendizaje por refuerzo

Esta categoría es emergente en entornos estratégicos. Se basa en la retroalimentación constante para mejorar el entrenamiento y obtener mejores resultados en la toma de

decisiones: se aplica en simulaciones de escenarios de combate y entrenamiento autónomo de sistemas de defensa inteligentes; aporta mayor adaptabilidad en ambientes de incertidumbre, reforzando decisiones basadas en contexto y experiencia acumulada (Galán et al., 2024).

El aprendizaje por refuerzo (RL) y su evolución, el aprendizaje profundo por refuerzo (Deep RL), ha revolucionado la forma de adquisición de experiencia y toma de decisiones en sistemas militares autónomos. Como es el caso de los entornos simulados de combate aéreo, que usan algoritmos tales como la "optimización de políticas por proximales" y "ActorCrítico Suave", los cuales han sido entrenados para maniobras ofensivas y evasivas, superando en varios escenarios a pilotos humanos (Zhu et al., 2023).

En contextos de vigilancia con enjambres de drones, el RL emerge como una técnica estratégica para el control autónomo. El aprendizaje multiagente (MARL), ha permitido coordinar misiones de seguimiento y cobertura territorial, optimizando el consumo energético y la eficiencia operativa (Arranz et al., 2025), las arquitecturas basadas en este modelo, han permitido comportamientos de enjambre robustos con características de adaptabilidad dinámica, resiliencia operativa, coordinación descentralizada y escalabilidad redundancia, en tiempo real y adaptación en entornos cambiantes (Batra et al., 2022; Arranz et al., 2025).

Pese a sus logros, este tipo de modelos presenta retos importantes, tales como: explicabilidad limitada, dificultad de auditoría, detección de errores o sesgos, el entrenamiento con alto costo computacional, y existe el riesgo de comportamiento no deseado en misiones críticas si no se cuenta con mecanismos de seguridad robustos (Yue et al., 2023).

Aplicabilidad estratégica en sistemas de inteligencia

La aplicabilidad estratégica de los algoritmos predictivos ha demostrado un uso potencial en las FF.MM., especialmente en sistemas de C4ISR. Estos sistemas facilitan la integración de capacidades predictivas mediante el uso de algoritmos supervisados, no supervisados, modelos de series temporales y aprendizaje por refuerzo, permitiendo:

- acelerar el procesamiento de datos multifuente (SIGINT, HUMINT, OSINT),

- reducir la carga cognitiva de los analistas humanos,
- detectar patrones y amenazas de forma temprana,
- generar productos de inteligencia oportunos, precisos, confiables y con valor anticipativo para la toma de decisiones.

Una posibilidad de uso reside, en la capacidad de aprendizaje, para hacer ajustes de forma automática a nuevas situaciones operativas, y anticipación ante amenazas cibernéticas. De este modo, incrementa la capacidad de respuesta de los sistemas de inteligencia estratégica, integrando grandes volúmenes de datos estructurados y no estructurados desde dominios como OSINT, SIGINT y vigilancia cibernética, permitiendo la asignación de recursos y mejora la eficacia operacional en escenarios complejos. En este sentido, como lo señalan Gnodle y Verran (2021), plantea la combinación de algoritmos supervisados y no supervisados en ecosistemas digitales adaptativos, para una gestión integral de amenazas híbridas, caracterizadas por su dinamismo, distribución y ambigüedad.

Ahora bien, el éxito de la presente aplicación estratégica depende de la existencia de factores críticos como: infraestructura tecnológica interoperable, doctrina actualizada, formación del talento humano y regulación ética del uso de IA como soporte para la toma de decisiones de seguridad. Las oportunidades de incorporación de algoritmos predictivos no solo están en su rendimiento técnico, sino en su articulación efectiva en los sistemas de información y las estructuras de toma de decisiones para C4ISR de las FF.MM. (He et al., 2020; Preece et al., 2019; Mindefensa, 2024).

Tendencias emergentes y nuevas evidencias científicas

Recientemente se ha evidenciado una evolución en la aplicación de algoritmos predictivos dentro del dominio de la inteligencia estratégica. Wilner & Atkinson (2025), analizan la aplicación que han tenido estos algoritmos dentro del sector defensa en Canada y 5 paises principales , evidenciando el potencial que tienen los sistemas de IA adaptativa y modelos híbridos, para transformar la capacidad anticipativa de eventos futuros. Dicha transformación permite realizar procesos complejos de toma de decisiones estratégicas en contexto militar en tiempo real, mejorando la eficiencia en misiones de defensa.

Estudios como los de Zhu et al. (2023) y el de Arranz et al. (2025), han enfatizado el alcance de la aplicabilidad del Deep-RL en simulaciones de combate o en rutas de vigilancia terrestre a través del uso de enjambres de UAVs o sistemas autónomos de seguimiento. Al integrar estas capacidades, se ha desarrollado el mejoramiento en la eficacia operativa, maximizando el resultado de las misiones, como también ha minimizado los tiempos de respuesta y aumenta la capacidad de adaptación ante diferentes escenarios, incrementando la resiliencia institucional (Monzón-Baeza et al., 2025).

Sin embargo, su adopción demanda desafíos significativos que van más allá de la dimensión tecnológica. Algunos de los retos en este sentido son la explicabilidad de las decisiones resultantes (Gunning & Aha, 2019), reducir la tecnodependencia, dependencia de proveedores extranjeros, capacitación del personal, asegurar la integración con las doctrinas, y establecer mecanismos sólidos de gobernanza ética que regulen el uso de la IA en el ámbito de la seguridad nacional (Yue et al., 2023).

Clasificación de los algoritmos predictivos aplicables en inteligencia estratégica

La tabla 1, presenta una comparación basada en el análisis bibliométrico de los diferentes modelos de algoritmos predictivos, presenta cómo cada categoría se ajusta a diferentes objetivos estratégicos en inteligencia militar, planteando un análisis mediante ejemplos, la aplicación en la inteligencia estratégica, la utilidad estratégica y los retos o consideraciones especiales para tener en cuenta para su aplicación.

Tabla 1. Clasificación de algoritmos predictivos y sus retos para su implementación.

Tipo de Algoritmo	Ejemplos de Modelos	Aplicaciones en Inteligencia Estratégica	Utilidad Estratégica	Retos / Consideraciones
Supervisados	Redes Neuronales (ANN, CNN), Regresión Logística, Árboles de Decisión	- Identificación automática de blancos (ej. Project Maven) - Clasificación de amenazas - Análisis de imágenes satelitales	- Aumenta precisión en decisiones operacionales - Automatiza tareas complejas	Requieren grandes volúmenes de datos etiquetados Riesgo de sesgo y baja explicabilidad
No Supervisados	K-means, DBSCAN, PCA	- Detección de amenazas internas (ej. DARPA ADAMS) - Análisis SIGINT/OSINT - Vigilancia cibernética	- Descubrimiento de patrones ocultos - Alertas tempranas	Alta tasa de falsos positivos Dificultad para interpretar conjuntos de datos
Semi-Supervisados	Graph-based SSL, Semi-supervised SVM	- Clasificación de amenazas con pocos datos etiquetados - Monitoreo en redes de defensa	- Aumenta precisión donde hay escasez de etiquetas - Mejora la eficiencia en tiempo real	Necesita equilibrio adecuado entre datos etiquetados y no etiquetados Complejidad algorítmica
Series Temporales	ARIMA, Prophet, LSTM	- Predicción de picos de violencia - Anticipación de ataques DDoS - Vigilancia de rutas de narcotráfico	- Soporte para decisiones anticipativas - Optimización de despliegue de recursos	Dependencia de datos históricos precisos Dificultad con eventos disruptivos
Aprendizaje por Refuerzo	Q-Learning, PPO, Deep Q-Network, MARL	- Maniobras autónomas de drones - Simulaciones de combate aéreo - Coordinación de enjambres de drones	- Mejora la adaptabilidad táctica - Optimiza misiones dinámicas en tiempo real	Bajo nivel de explicabilidad Costos computacionales elevados Riesgo de comportamientos no deseados

Fuente: elaboración propia con base en los datos recolectados.

Caracterización de las capacidades institucionales y los factores organizacionales que condicionan la integración de algoritmos predictivos en el sistema de inteligencia estratégica de las Fuerzas Militares de Colombia

A continuación, se caracteriza la integración de los algoritmos predictivo a los sistemas de inteligencia estratégica bajo el enfoque de la Teoría General de Sistemas (TGS),

concibiendo la inteligencia estratégica como un ecosistema de subsistemas interdependientes (tecnológico, humano, doctrinal, normativo, etc.), cuyo funcionamiento armónico es necesario para producir conocimiento útil (Bertalanffy, 1968; Liwång et al., 2023). Desde esta óptica sistémica, cualquier falla en uno de los componentes puede degradar el rendimiento global del sistema de inteligencia.

El enfoque de Toma de Decisiones Basada en Datos (DDDM), proporciona un marco metodológico para estructurar el flujo de datos desde su recolección, análisis y uso en la toma de decisiones con base en evidencia objetiva y actualizada (Provost & Fawcett, 2013; Davenport, 2014). En el contexto militar, DDDM establece procesos sólidos de gestión de datos, preprocesamiento, almacenamiento seguro, análisis predictivo y la retroalimentación, de forma que las decisiones estratégicas se deriven de información confiable y pertinente. Bajo estos lineamientos, a continuación, se analiza la situación desde las perspectivas de TGS y DDDM, para luego evaluar las capacidades institucionales de las FF.MM. de Colombia en torno a la incorporación de algoritmos predictivos.

Análisis desde la perspectiva de la Teoría General de Sistemas

Desde esta teoría, la inteligencia estratégica militar puede entenderse como un sistema complejo de múltiples subsistemas interrelacionados: infraestructura tecnológica, talento humano, doctrina operativa, cultura organizacional, marco normativo, entre otros. La incorporación de algoritmos predictivos en este sistema exige que todos los subsistemas estén alineados y fortalecidos: por ejemplo, que los datos generados en campo (sensores, informes de inteligencia humana, fuentes abiertas), puedan ser transmitidos, procesados eficientemente por análisis predictivo, interpretados correctamente por analistas capacitados, e incorporados en la planificación estratégica según doctrinas y protocolos establecidos (He et al., 2020; Preece et al., 2019; Liwång et al., 2023). Una deficiencia en cualquiera de estos eslabones sea tecnológica o humana, puede comprometer la efectividad global del sistema de inteligencia estratégica.

Estudios recientes sugieren que los sistemas de defensa modernos funcionan como ecosistemas digitales interdependientes, donde la adaptabilidad depende de la coordinación entre sus nodos tecnológicos y humanos (Bertalanffy, 1968; Autio et Al., 2020; Márquez-

Díaz, 2024). En consecuencia, bajo la TGS, la integración de algoritmos predictivos debe abordarse mediante un rediseño sistémico coordinado, no basta con adquirir una herramienta de IA, además se requiere actualizar la infraestructura, capacitar al personal, adaptar la doctrina y ajustar la normativa en forma conjunta para aprovechar las capacidades predictivas (Liwång et al., 2023; Meerveld & Lindelauf, 2024).

Análisis desde la perspectiva de la Toma de Decisiones basada en Datos

Desde esta perspectiva, los algoritmos predictivos se basan en el análisis de datos, subrayando tres requisitos fundamentales: disponibilidad de datos confiables, integrados y actualizados; existencia de procesos analíticos robustos (almacenamiento, limpieza, análisis, visualización) para extraer conocimiento de esos datos; capacidad institucional para traducir las salidas de los modelos predictivos en decisiones y acciones concretas (Provost & Fawcett, 2013; Gnodle & Verran, 2021).

DDDM requiere una cultura organizacional que valore la evidencia empírica por encima de la intuición, soportada por infraestructuras de datos que permitan flujos de información rápidos y seguros hacia los tomadores de decisión (Davenport, 2014; Meerveld & Lindelauf, 2024). En el ámbito de la defensa, adoptar DDDM implica mejorar la interoperabilidad de los sistemas C4ISR, de modo que la información recolectada sea accesible en tiempo real para su análisis (Hilton-Shomron, 2024). Así mismo, se requiere optimizar los canales de transmisión, implementando estándares de QoS y automatizar tareas de filtrado y agregación de información (Han et al., 2012).

Un aspecto crucial del DDDM es la retroalimentación, asegurando mejora continua y adaptación dinámica al entorno cambiante. En el contexto colombiano, este enfoque requiere cerrar brechas tecnológicas tales como integrar bases de datos entre fuerzas, actualizar plataformas de analítica avanzada, y formar talento humano para soporte e interpretación de resultados (Ghasemaghaei & Calic, 2019; Zambrano González, 2025). Las FF.MM. están entrando en la era de las DDDM, donde la ventaja estratégica dependerá de la capacidad en big-data y analítica en tiempo real (Meerveld & Lindelauf, 2024; Probasco et al., 2025). Por tanto, es necesario fortalecer la infraestructura de datos como los

procesos decisionales, asegurando que cada decisión estratégica esté sustentada en el análisis de la información, en lugar de depender de criterios subjetivos o históricos.

Dimensiones clave de las capacidades institucionales y factores organizacionales

Derivado del análisis teórico, se identifican cinco dimensiones críticas para evaluar la viabilidad de integrar algoritmos predictivos en la inteligencia estratégica de las FF.MM. de Colombia (Ardila-Castro & Jiménez, 2020; He et al., 2020; Preece et al., 2019). Estas dimensiones abarcan tanto capacidades institucionales internas, como factores del entorno organizacional que pueden facilitar o limitar dicha integración:

Capacidades tecnológicas e infraestructura

Corresponde al estado de las plataformas tecnológicas de C4ISR, así como las redes de datos y capacidades de almacenamiento. En Colombia, existen esfuerzos de modernización tecnológica en marcha como la actualización de sistemas de vigilancia multifuente y la adopción de arquitecturas de big-data en el sector defensa (NUVU, 2024; Ministerio de Defensa Nacional, 2024), representando una oportunidad para insertar herramientas de IA en nuevos desarrollos. Sin embargo, persisten desafíos como la fragmentación tecnológica, baja interoperabilidad entre sistemas de las fuerzas, dependencia de proveedores externos y riesgos en ciberseguridad.

Talento humano y capacidades analíticas

Se refiere al recurso humano especializado disponible, tales como analistas de inteligencia con formación en ciencia de datos, ingenieros de datos, expertos en ciberseguridad, entre otros, y a los programas de capacitación existentes. Actualmente, el personal con competencias avanzadas en analítica de datos e IA en las FF.MM. es reducido, y existe riesgo de fuga de talento hacia el sector privado (Zambrano González, 2025). No obstante, existen oportunidades para fortalecer el talento mediante convenios académicos, creación de unidades especializadas en análisis avanzado, e iniciativas de formación continua en temas de big-data e inteligencia artificial orientada a defensa (Barbosa, 2021; Camacho et

al., 2024). El desafío principal es desarrollar una estrategia integral de talento humano, que abarque reclutamiento, formación, continuidad y retención de perfiles técnicos, a la vez que se sensibiliza al personal operativo y de comando sobre la toma de decisiones basada en el análisis de datos.

Doctrina y adaptación operativa

Esta dimensión contempla la incorporación de la analítica predictiva en la doctrina militar, las directrices estratégicas y los procedimientos operativos. En Colombia, doctrinas recientes como la Doctrina Damasco del Ejército Nacional han comenzado a reconocer la importancia de la transformación digital y el uso de herramientas de análisis de datos en operaciones militares (Cancelado, 2019; Bastos Martínez, 2019). Esta actualización doctrinal ofrece una oportunidad para integrar el empleo de algoritmos predictivos en funciones de inteligencia, planeamiento y logística. Sin embargo, persisten desafíos de adopción: la doctrina vigente aún carece de protocolos estandarizados para el uso de IA en operaciones críticas, no define claramente roles y responsabilidades para sistemas autónomos, y en general la innovación tecnológica suele avanzar más rápido que su incorporación doctrinal (Bastos Martínez, 2019). Superar este reto requerirá actualizar manuales tácticos, reglamentos y cursos de estado mayor para incluir escenarios con herramientas predictivas, y fomentar ejercicios de simulación donde se validen estos conceptos (Márquez-Díaz, 2024; Zhu et al., 2023).

Marco normativo y consideraciones éticas

Comprende el conjunto de leyes, políticas públicas, reglamentos internos y principios éticos que rigen el uso de IA en el ámbito de defensa. Colombia ha dado pasos importantes, como la Política Nacional de Inteligencia Artificial 2023–2030, que promueve el uso ético de IA en el sector público, y el Marco jurídico de inteligencia (Ley 1621 de 2013) que establece lineamientos para la actividad de inteligencia y contrainteligencia (CONPES, 2020; Jaramillo, 2024). Si bien constituyen marcos generales, no abordan de forma específica el empleo en el ámbito militar de algoritmos predictivos ni los desafíos particulares que esto implica, como la explicabilidad de los modelos, la gestión de sesgos algorítmicos, la

responsabilidad ante decisiones autónomas o la protección de datos sensibles (Taddeo et al., 2021; Gunning & Aha, 2019).

Igualmente, surgen dilemas éticos como: equilibrar la eficacia de un modelo predictivo con el respeto a los derechos fundamentales (privacidad, presunción de inocencia), o asegurar que un algoritmo no reproduzca sesgos discriminatorios en la identificación de amenazas. Abordar estos temas requerirá actualizar el marco normativo, elaborar directrices éticas claras y establecer mecanismos de auditoría y supervisión (Jaramillo, 2024; Khan et al., 2021).

Cultura organizacional y cambio institucional

Esta dimensión engloba las actitudes, valores y prácticas respecto al uso de datos, tecnología y toma de decisiones. Tradicionalmente, la cultura militar colombiana ha privilegiado la experiencia del comandante y la observancia de la cadena de mando por encima del análisis cuantitativo. Esto puede generar resistencia a adoptar modelos automatizados de apoyo a la decisión, por temor a que reemplacen el "criterio militar" o por falta de confianza en sistemas "caja negra". No obstante, también se observan señales positivas de apertura a la innovación: se han creado laboratorios de innovación en defensa, existen colaboraciones con universidades y empresas en proyectos de IA (Budeanu, 2023). El desafío cultural para la incorporación de algoritmos predictivos requiere difundir casos de éxito, promover una cultura de toma de decisiones basada en evidencia en todos los niveles, e involucrar a los líderes clave como patrocinadores del cambio (Scharre & Horowitz, 2019); además, la cooperación inter agencial e internacional (Kiss et al., 2023; Baboș et al., 2022).

Clasificación de las oportunidades, desafíos, algoritmos predictivos viables y resultados esperados

La tabla 2 presenta las oportunidades y desafíos identificadas, junto con los tipos de algoritmos predictivos más adecuados para cada ámbito y los resultados esperados de su implementación en los sistemas de inteligencia estratégica de las FF.MM. de Colombia.

Tabla 2. Clasificación de las oportunidades, desafíos, algoritmos predictivos viables y resultados esperados.

Dimensión	Oportunidades	Desafíos	Algoritmos Predictivos Viables	Resultados Esperados
Tecnológica / Infraestructura (C4ISR)	Modernización progresiva de sistemas de mando y control; integración de *big data* y análisis multifuente en tiempo real (NUVU, 2024).	Fragmentación tecnológica, baja interoperabilidad entre plataformas, dependencia de proveedores externos; vulnerabilidades cibernéticas heredadas.	Modelos de series de tiempo (ARIMA, Prophet, *RNN*) para vigilancia y alerta temprana en ISR; aprendizaje supervisado (árboles de decisión, redes neuronales), para clasificación y priorización de amenazas (Bello et al., 2024; Marr, 2016).	Detección anticipada de amenazas emergentes (p.ej. movimientos anómalos en fronteras); generación de alertas tempranas confiables; asignación óptima de recursos de vigilancia en tiempo real según pronósticos de riesgo.
Talento Humano / Capacidades Analíticas	Formación creciente en IA y ciencia de datos en el sector defensa; posibilidad de crear unidades especializadas de analítica e inteligencia	Escasez de personal con competencias avanzadas en datos e IA; fuga de talento calificado al sector privado; resistencia de analistas tradicionales a la	Algoritmos semi-supervisados que aprovechan conjuntos de datos limitados (p.ej. *self-training*, *label propagation*); técnicas de *clustering* (K-means, DBSCAN) para descubrir patrones	Análisis de inteligencia más eficiente y profundo con el mismo personal, aumenta la productividad analítica; descubrimiento de nuevas tendencias o amenazas ocultas que podrían pasar

	artificial dentro de las Fuerzas.	automatización de tareas.	ocultos en datos no etiquetados (Chapelle et al., 2010; Rizve et al., 2021).	inadvertidas manualmente; desarrollo gradual de capacidades internas de ciencia de datos en las fuerzas reduciendo la dependencia externa.
Doctrina / Adaptación Operativa	Inclusión de objetivos de transformación digital en doctrinas recientes, por ejemplo, la Doctrina Damasco; oportunidad para integrar directrices sobre uso de IA en procesos operativos y de planificación estratégica.	Rigidez doctrinal y burocrática; falta de protocolos tácticos específicos para empleo de IA en combate o en apoyo a decisiones de alto nivel; posibles vacíos legales o de responsabilidad en operaciones autónomas.	Aprendizaje por refuerzo (incluyendo *Deep Reinforcement Learning*) para simulaciones de combate y entrenamiento autónomo de sistemas; modelos supervisados, como regresión logística y SVM, para evaluación de riesgos y apoyo a decisiones en juegos de guerra (Zhu et al., 2023; Arranz et al., 2025).	Mayores capacidades de simulación y ensayo de escenarios (*wargaming* avanzado) para entrenamiento de comandantes; decisiones operativas más ágiles y adaptativas basadas en evaluación objetiva de riesgos; doctrina más flexible que incorpora mejores prácticas derivadas del análisis de datos.
Marco Normativo / Ético	Marco legal general existente (Ley 1621/2013, Política de IA 2023–2030) que puede adaptarse al ámbito militar; discusión incipiente sobre ética de IA en seguridad nacional a nivel gubernamental.	Ausencia de normativa específica para IA militar; riesgos de sesgo y decisiones opacas (*black-box*) que generen responsabilidad difusa; necesidad de compatibilizar el uso de IA con derechos humanos y el DIH.	Modelos supervisados explicables tales como árboles de decisión interpretables, o métodos SHAP/LIME, para asegurar transparencia y trazabilidad en el análisis automatizado (Gunning & Aha, 2019; Herman et al., 2022).	Mayor confianza institucional y pública en el uso de IA militar al proveer explicaciones claras de las predicciones; cumplimiento de estándares éticos y legales, reduciendo riesgos de violaciones; capacidad de auditoría y control humano sobre los algoritmos evitando la "caja negra.

Cultura Organizacional / Cambio	Apertura gradual a la innovación tecnológica; creciente *mindset* digital en mandos jóvenes; oportunidades de cooperación inter agencial e internacional.	Cultura jerárquica con preferencia por la experiencia y el método tradicional sobre el análisis de datos; posible temor a que la automatización reemplace el criterio humano; inercia al cambio e incertidumbre sobre nuevas tecnologías.	Aprendizaje no supervisado para la detección de anomalías mediante *outlier detection*, *clustering* adaptativo, implementado como *herramienta de apoyo* no intrusiva para analistas; modelos híbridos combinando técnicas supervisadas y no supervisadas, introducidos paulatinamente para resolver problemas concretos (Peng et al., 2022).	Adopción incremental de la IA con bajo rechazo, al demostrarse como apoyo que complementa, no sustituye, la experiencia del personal; mejora de la confianza en sistemas analíticos al integrarlos en flujos de trabajo existentes; una cultura organizacional más orientada a datos, dispuesta a innovar y cooperar en el uso de nuevas tecnologías.

Fuente: Elaboración propia con base en los datos recolectados y autores.

Síntesis final

Las oportunidades para incorporar algoritmos predictivos en la inteligencia estratégica de las FF.MM. de Colombia se concentran en varios aspectos positivos: infraestructura de sistemas C4ISR en proceso de modernización, políticas nacionales de IA que promueve la innovación tecnológica, experiencia acumulada en el uso de inteligencia multifuente. Además, doctrinas recientes muestran voluntad de adaptarse a los cambios digitales, y hay indicios de apertura cultural hacia metodologías basadas en datos.

Sin embargo, los desafíos son significativos, destacan la fragmentación tecnológica y baja interoperabilidad, la falta de talento humano especializado en analítica avanzada, la rigidez doctrinal que dificulta cambios rápidos, la ausencia de regulación detallada para el uso de IA en el campo militar, y resistencias culturales a la automatización y a la toma de decisiones asistida por máquinas. En síntesis, el panorama actual muestra un potencial considerable pero que podrá materializarse si se abordan proactivamente estas brechas.

Desde la TGS, integrar algoritmos predictivos con éxito requerirá una aproximación holística: es necesario alinear y fortalecer todos los componentes del sistema institucional de inteligencia para que se refuercen mutuamente (Bertalanffy, 1968; Autio et Al., 2020), de poco sirve adquirir herramientas sofisticadas de IA si no se dispone de datos de calidad o si el personal no confía en sus resultados. Así mismo, desde el enfoque DDDM, se debe consolidar un ciclo completo de gestión de datos donde la información clara, relevante y accesible alimente modelos predictivos, cuyos resultados se integren en la toma de decisiones estratégicas (Provost & Fawcett, 2013; Meerveld & Lindelauf, 2024).

Esto implica adoptar prácticas de gobierno de datos, indicadores de desempeño para las decisiones basadas en IA, y mecanismos de retroalimentación para mejorar continuamente tanto los datos como los algoritmos. El sector defensa debe entrar en una etapa de toma de decisiones sustentadas en datos, factor diferencial en la superioridad estratégica (Kiss et al., 2023; Meerveld & Lindelauf, 2024).

Conclusiones

La presente investigación identifica oportunidades y desafíos para la incorporación de algoritmos predictivos en los sistemas de inteligencia estratégica de las FF.MM. de Colombia. Los hallazgos más relevantes muestran que dichas tecnologías ofrecen un potencial para transformar la inteligencia estratégica, generando herramientas que permiten el procesamiento de altos volúmenes de datos, anticipación de amenazas, optimizar la asignación de recursos y fortalecer la toma de decisiones en escenarios complejos y dinámicos.

Los algoritmos supervisados, no supervisados, semi-supervisados, basados en series temporales y de aprendizaje por refuerzo, tienen aplicaciones diferenciadas, cuya sinergia puede aumentar la eficacia de los sistemas C4ISR y robustecer el ciclo de inteligencia. No obstante, para su implementación existen desafíos tales como la calidad del dato, plataformas interoperables, formación de talento humano especializado, y marcos éticos y normativos (Arranz et al., 2025; Williams & Qian, 2025).

Esta investigación consolida un marco teórico actualizado sobre el uso de algoritmos predictivos en inteligencia estratégica, articulando los enfoques de la TGS y la

DDDM. El análisis bibliométrico realizado evidencia tendencias globales y vacíos en la producción científica nacional, requiriendo generar nuevo conocimiento aplicable a las ciencias militares, en particular a la construcción de doctrinas adaptativas que integren tecnologías emergentes con estructuras de mando y control (He et al., 2020; Preece et al., 2019; Provost & Fawcett, 2013).

La integración de algoritmos predictivos no solo implica una innovación tecnológica, sino una transformación institucional hacia una inteligencia estratégica soportada en herramientas tecnológicas, capaz de anticipar amenazas híbridas y de operar en ecosistemas digitales interdependientes. Ello demanda fortalecer las capacidades técnicas, doctrinales y culturales de las FF.MM. para garantizar un uso ético, seguro y efectivo de estas herramientas en la seguridad nacional (Jaramillo, 2024; Autio et Al., 2020).

Como trabajos futuros, se propone evaluar la eficacia de algoritmos específicos en escenarios simulados y operaciones reales, en ámbitos como la ciberdefensa, la vigilancia fronteriza y la predicción de desplazamientos de actores armados. Así mismo, profundizar en líneas de investigación tales como la explicabilidad de los modelos de IA, y diseño de una metodología para la integración de algoritmos predictivos en los sistemas de inteligencia estratégica. Estos enfoques permitirán consolidar un conocimiento que complemente la revisión teórica con evidencia práctica, facilitando la transición de las FF.MM. hacia una inteligencia estratégica proactiva, adaptativa y sustentada en herramientas de analítica de datos en tiempo real.

Referencias

Alcántara-Suárez, E. J. (2023). Análisis de la aplicación de machine learning en sistemas de defensa [Universidad Abierta de Cataluña]. https://tinyurl.com/nvjc377v

Alfatemi, A., Rahouti, M., Amin, R., AlJamal, S., Xiong, K., & Xin, Y. (2024). Advancing DDoS attack detection: A synergistic approach using deep residual neural networks and synthetic oversampling. arXiv. https://doi.org/10.48550/arXiv.2401.03116

Allen, G. C. (2017, 21 de diciembre). Project Maven brings AI to the fight against ISIS. https://tinyurl.com/mu8td5w3

Ardila-Castro, C. A., & Jiménez-Reina, J. (2020). *Aportes teóricos a la construcción del concepto de inteligencia estratégica*. Planeta. https://tinyurl.com/2ckc5eap

Arranz, R., Carramiñana, D., de Miguel, G., Besada, J. A., & Bernardos, A. M. (2025). Application of deep reinforcement learning to UAV swarming for ground surveillance. arXiv. https://doi.org/10.48550/arXiv.2501.08655

Autio, E., Nambisan, S., Thomas, L. D. W., & Wright, M. (2020). *Digital ecosystems and their implications for competitive strategy*. *Journal of Organization Design*, 9(1), 12. https://doi.org/10.1186/s41469-020-00073-0

Ayub, M. Y., Mehdi, M. A., Tawaseem, S. G., Zukhraf, S. Z. N., & Zupash. (2022). Role of computational intelligence in cybersecurity. En M. Ouaissa, Z. Boulouard, M. Ouaissa, I. U. Khan, & M. Kaosar (Eds.), *Big data analytics and computational intelligence for cybersecurity* (pp. 125-144). Springer. https://doi.org/10.1007/978-3-031-05752-6_8

Baboş, A., Iacob, C.-G., & Ene, C. (2022). Use of forecasting systems in the military decision-making process. *Land Forces Academy Review, 27*(4), 316–322. https://doi.org/10.2478/raft-2022-0040

Barbosa Fontecha, J. L. (2021). Modelos predictivos para la rotación del talento humano. Tecnología, Investigación y Academia, *8*(1), 54—71. https://tinyurl.com/5bpeexyr

Bastos Martínez, L. (2019). Doctrina del Ejército Nacional: Componente de capacidad clave para afrontar los desafíos y amenazas de la nación en el siglo XXI. *Experticia Militar*, (7), 22–29. https://tinyurl.com/yvrd3bjs

Batra, S., Huang, Z., Petrenko, A., Kumar, T., Molchanov, A., & Sukhatme, G. S. (2022). Decentralized control of quadrotor swarms with end-to-end deep reinforcement learning. En *Proceedings of the 5th Conference on Robot Learning* (Vol. 164, pp. 576-586). Proceedings of Machine Learning Research. https://tinyurl.com/yr29k5z6

Becerra-Suárez, F. L., Fernández-Román, I., & Forero, M. G. (2024). Improvement of Distributed Denial of Service attack detection through machine learning and data processing. *Mathematics, 12*(9), 1294. https://doi.org/10.3390/math12091294

Bello, A. M., Iorliam, A., & Asilkan, O. (2024, 30 de octubre). Data science insights and the classification of terrorist attacks in Nigeria using machine learning techniques. *Global Journal of Computer Sciences: Theory and Research, 14*(2).

Bertalanffy, L. von. (1968). *General system theory: Foundations, development, applications*. George Braziller.

Budeanu, N. A. (2023). Bibliometric analysis regarding knowledge strategies in intelligence structures. *Proceedings of the International Conference on Business Excellence, 17*(1), 1179–1192. https://doi.org/10.2478/picbe-2023-0106

Camacho, A., Gómez, J., & Galindo, C. (2024). *Los desafíos éticos del uso de IA en la toma de decisiones [Trabajo de especialización, EAN]*. Repositorio Insitucional https://tinyurl.com/4yphzctd

Cancelado, H. (2019). Doctrina Damasco: La interacción de la vida nacional y el dominio terrestre. *Experticia Militar*, (7), 76–78. https://tinyurl.com/yvrd3bjs

CONPES. (2020). *Política Nacional para la Transformación Digital e Inteligente del Sector Defensa y Seguridad*. Departamento Nacional de Planeación. https://tinyurl.com/mpdt2d28

Cortés González, D. C. (2019). *Transformación de la inteligencia estratégica en Colombia: Hitos y retos en el escenario actual* [Tesis de maestría, Universidad Nacional de Colombia]. Repositorio UNAL. https://tinyurl.com/nhja6rdp

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Danish, M. (2024, 15 de julio). *Enhancing cyber security through predictive analytics: Real-time threat detection and response*. arXiv. https://doi.org/10.48550/arXiv.2407.10864

Davenport, T. (2014). *Big data at work: Dispelling the myths, uncovering the opportunities*. Harvard Business Review. https://tinyurl.com/bdzmebey

Galán, J. J., Carrasco, R. A., & LaTorre, A. (2024). *Military applications of machine learning: A bibliometric perspective*. arXiv. https://doi.org/10.48550/arXiv.2410.17272

Ghasemaghaei, M., & Calic, G. (2019). Can big data improve firm decision quality? The role of data quality and data diagnosticity. *Decision Support Systems*, (120), 38–49. https://doi.org/10.1016/j.dss.2019.03.008

Gnodle, M. A., & Verran, D. (2021). *Data-Enabled Decision-Making*. U.S. Army. https://tinyurl.com/4ekdjtff

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press. https://www.deeplearningbook.org/

Gunning, D., & Aha, D. W. (2019). DARPA's explainable artificial intelligence (XAI) program. *AI Magazine*, *40*(2), 44–58. https://doi.org/10.1609/aimag.v40i2.2850

Habeeb, M. S. (2024). Predictive analytics and cybersecurity. En *Intelligent Techniques for Predictive Data Analytics* (pp. 151–169). Wiley https://doi.org/10.1002/9781394227990.ch8

Han, J., Kamber, M., & Pei, J. (2012). *Data Mining: Concepts and Techniques* (3a ed.). Morgan Kaufmann. https://tinyurl.com/579aeajz

He, H. Y., Zhu, W. X., Li, R. Y., & Deng, Q. Y. (2020). *An executable modeling and analyzing approach to C4ISR architecture*. Journal of Systems Engineering and Electronics, 31(1), 109–117. https://doi.org/10.21629/JSEE.2020.01.12

Heuer, R. J. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence.

Hilton-Shomron, Y. D. (2024, febrero 23). Report: Revolutionizing Military Strategy: Integrating AI for Predictive Analytics and Real-Time Battle Planning. *LinkedIn*. https://www.linkedin.com/pulse/report-revolutionizing-military-strategy-integratinghilton-shomron-dy9re

Imran, I.I. (2025). Exploiting anomalies with data mining techniques to enhance cloud security. *Mathematical Modelling of Engineering Problems, 12*(2), 636646. https://doi.org/10.18280/mmep.120227

Jaramillo, J. (2024). *El marco jurídico para la regulación de la inteligencia artificial en Colombia: Retos y Perspectivas en la Creación de un Régimen Normativo* [Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/server/api/core/bitstreams/1f7766ea-aa98-4e91-b391-59ac4bdbc32b/content

Joint Chiefs of Staff. (2022). *Joint Intelligence (JP 2-0)*. U.S. Department of Defense. https://tinyurl.com/mw8fchd7

Kelleher, J. D., Mac Namee, B., & D'Arcy, A. (s. f.). *Fundamentals of Machine Learning for Predictive Data Analytics: Algorithms, Worked Examples, and Case Studies*. MIT Press. https://tinyurl.com/yfhfz3zd

Khan, A. A., Badshah, S., Liang, P., Waseem, M., Khan, B., Ahmad, A., Fahmideh, M., Niazi, M., & Akbar, M. A. (2021). *Ethics of AI: A systematic literature review of principles and challenges*. arXiv. https://doi.org/10.48550/arXiv.2109.07906

Kiss, J., Skraba, F., & De Oliveira, C. (2023). The future of intelligence: AI, big data and challenges for policymakers. *Journal of Defense Studies, 10*(3), 47–60.

Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cybersecurity analytics: From intrusion detection to attack prediction. *International Journal of Information Security, 24*(3). https://doi.org/10.1007/s10207-024-00921-0

Lappin, Y. (2023). Embracing big data and AI strategically: The digital transformation of the IDF. En *Leveraging Innovation and Artificial Intelligence* (Capítulo 7). The Air Power Journal, Third Edition. Begin-Sadat Center for Strategic Studies. https://theairpowerjournal.com/big-data-ai-digital-transformation-idf/

Liwång, H., Kent E, A., Bang, M., & Tärnholm, T. (2023). How can systemic perspectives on defence capability development be strengthened? *Defence Studies, 23*(3), 399–420. https://doi.org/10.1080/14702436.2023.2239722

Márquez-Díaz, J. E. (2024). *Benefits and challenges of military artificial intelligence in the field of defense*. *Computación y Sistemas*, 28(2), 309–323. https://doi.org/10.13053/cys-28-2-4684

Marr, B. (2016). *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results*. Wiley.

McDowell, K., Novoseller, E., Madison, A., Goecks, V. G., & Kelshaw, C. (2024). *Re-Envisioning Command and Control*. arXiv. https://doi.org/10.48550/arXiv.2402.07946

Meerveld, H., & Lindelauf, R. (2024). *Data science in military decision-making: Foci and gaps*. *Global Society*, 39(2), 103–129. https://doi.org/10.1080/13600826.2024.2353657

Ministerio de Defensa Nacional [Mindefensa]. (2024). *Plan Estratégico del Sector Defensa y Seguridad: Guía de planeamiento estratégico del sector defensa 2022-2026*. Mindefensa. https://tinyurl.com/2em77pp7

Ministerio de Defensa Nacional [Mindefensa]. (2024). *Plan Nacional de Transformación Digital del Sector Defensa 2023–2030*. Mindefensa. https://tinyurl.com/55kcbddh

Ministry of Defence (UK). (2022). *Defence Artificial Intelligence Strategy*. Ministry of Defence. https://tinyurl.com/2s486shd

Monzón-Baeza, V., Parada, R., Concha Salor, L., & Monzó, C. (2025). *AI-driven tactical communications and networking for defense: A survey and emerging trends*. arXiv. https://doi.org/10.48550/arXiv.2504.05071

NATO. (2016). *AJP-2: Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* (Edition A, Version 2). North Atlantic Treaty Organization. https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf

Neira, A., Kantarci, B., & Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks, 222*(3), 109553. https://doi.org/10.1016/j.comnet.2022.109553

NUVU. (2024). Inteligencia Artificial: Revolucionando el sector de la defensa en Colombia. *NUVU*. https://tinyurl.com/547kv3kr

Pellerin, C. (2017, 21 de julio). Project Maven to deploy computer algorithms to war zone by year's end. *DoD News, Defense Media Activity*. https://tinyurl.com/evys32y2

Pherson, R., & Pherson, K. (2021). *Critical Thinking for Strategic Intelligence* (3rd ed.). CQ Press.

Phythian, M. (2021). Conclusion: The development of critical intelligence studies. *Intelligence and National Security, 36*(4), 615–620. https://doi.org/10.1080/02684527.2021.1912266

Pili, G. (2019). Intelligence and social epistemology: Toward a social epistemological theory of intelligence. *Social Epistemology, 33*(6), 574–592. https://doi.org/10.1080/02691728.2019.1658823

Preece, A., Braines, D., Cerutti, F., & Pham, T. (2019). *Explainable AI for Intelligence Augmentation in Multi-Domain Operations*. arXiv. https://doi.org/10.48550/arXiv.1910.07563

Probasco, E., Toner, H., Burtell, M., & Rudner, T. G. J. (2025, abril). AI for military decision-making. *CSET*. https://cset.georgetown.edu/wp-content/uploads/CSET-AI-for-Military-Decision-Making.pdf

Provost, F., & Fawcett, T. (2013). *Data Science for Business: What You Need to Know About Data Mining and Data-Analytic Thinking*. O'Reilly Media.

Quiñones-Sigala, J. (2023). Aplicaciones de la inteligencia artificial en contribución a la defensa nacional de Chile: Una oportunidad para la integración de la defensa, la

industria y la academia. *Revista Política y Estrategia*, (141), 155–185. https://doi.org/10.26797/rpye.vi141.1044

Rashid, J., Batool, A., Kim, J., Wasif Nisar, M., Hussain, A., Juneja, S., & Kushwaha, P. (2022). An augmented artificial intelligence approach for chronic diseases prediction. *Frontiers in Public Health*, *10*, 860396. https://doi.org/10.3389/fpubh.2022.860396

Rizve, M. N., Duarte, K., Rawat, Y. S., & Shah, M. (2021). *In defense of pseudo-labeling: An uncertainty-aware pseudo-label selection framework for semi-supervised learning*. arXiv. https://doi.org/10.48550/arXiv.2101.06329

Russell, S. J., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4a ed.). Pearson.

Sánchez, J. L. (2025, 4 de febrero). Inteligencia artificial en apoyo a la inteligencia militar. IEEE - Ministerio de Defensa de España. https://tinyurl.com/3j7yu9wb

Sarker, I. H., Janicke, H., Maglaras, L., & Camtepe, S. (2023). *Data-driven intelligence can revolutionize today's cybersecurity world: A position paper*. arXiv. https://doi.org/10.48550/arXiv.2308.05126

Scharre, P., & Horowitz, M. C. (2019). *A stable nuclear future? The impact of autonomous systems and artificial intelligence (ARYA Working Paper No. 1912.05291*). arXiv. https://doi.org/10.48550/arXiv.1912.05291

Shapira, I. (2020a). The limited influence of competitive intelligence over corporate strategy in Israel: Historical, organizational, conceptual, and cultural explanations. *Intelligence and National Security*, *36*(1), 95-115. https://doi.org/10.1080/02684527.2020.1796338

Shapira, I. (2020b). *The main challenges facing strategic intelligence*. *Strategic Assessment*, 23(1), 4–22. https://www.inss.org.il/wp-content/uploads/2022/12/Adkan23.1Eng_4.pdf

Sharma, D., & Phulli, K. (2020). *Forecasting and analyzing the military expenditure of India using Box-Jenkins ARIMA model*. arXiv. https://doi.org/10.48550/arXiv.2011.06060

Shu, R., Xia, T., Tu, H., Williams, L., & Menzies, T. (2022). *Reducing the cost of training security classifier via optimized semi-supervised learning*. arXiv. https://doi.org/10.48550/arXiv.2205.00665

Surma, J. (2024). *Deep learning in military applications: Threats and opportunities*. *Safety & Defense*, 10(1), 1–7. https://doi.org/10.37105/sd.214

Taddeo, M., McNeish, D., Blanchard, A., & Edgar, E. (2021). *Ethical principles for artificial intelligence in national defence*. *Philosophy & Technology*, 34, 1707–1729. https://doi.org/10.1007/s13347-021-00482-3

Van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Villamin, P., Lopez, V., Thapa, D. K., & Cleary, M. (2024). A worked example of qualitative descriptive design: A step-by-step guide for novice and early career researchers. *Journal of Advanced Nursing, 81*(8), 5181–5195. https://doi.org/10.1111/jan.16481

Williams, B., & Qian, L. (2025). Semi-supervised learning for intrusion detection in large computer networks. *Applied Sciences, 15*(11), 5930. https://doi.org/10.3390/app15115930

Wilner, A., & Atkinson, R. (2025, March 17). *Artificial intelligence and national defence: A strategic foresight analysis* (CIGI Paper No. 316). Centre for International Governance Innovation. https://www.cigionline.org/publications/artificial-intelligence-and-national-defence-a-strategic-foresight-analysis/

Yue, L., Yang, R., Zuo, J., & Zhang, Y. (2023). Research on reinforcement learning-based safe decision-making methodology for multiple unmanned aerial vehicles. *Frontiers in Neurorobotics, 16*, 1105480. https://doi.org/10.3389/fnbot.2022.1105480

Zambrano González, E. E. (2025). *Ética de la inteligencia artificial militar: análisis de principios, marcos normativos y desafíos futuros*. *Revista Ciberespacio, Tecnología e Innovación*, 4(7), 43–60. https://doi.org/10.25062/2955-0270.4943

Zhu, J., Kuang, M., Zhou, W., Shi, H., & Han, X. (2023). Mastering air combat game with deep reinforcement learning. *Defence Technology*, (34), 295—312. https://doi.org/10.1016/j.dt.2023.08.019