

Efectos de la integración de la inteligencia artificial al Proceso de Selección y Priorización de Blancos en el sistema de combate de fuegos*

Jaider Ospina Navas^a ■ Diego Alejandro Esmeral Madrid^b

Recibido: 27/10/2026 **Aceptado:** 21/07/2026

Cómo citar: Ospina Navas, J., & Esmeral Madrid, D. A. (2026). Efectos de la integración de la inteligencia artificial al Proceso de Selección y Priorización de Blancos en el sistema de combate de fuegos. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, 21(1), 8268. <https://doi.org/10.18359/ries.8268>

Resumen: El artículo presenta una discusión sobre el actual empleo de la inteligencia artificial (IA) en sistemas de toma de decisiones y de defensa, así como ejemplos de países y organizaciones que ya integran la IA en sus operaciones, como es el caso de Estados Unidos, China, Israel y la Organización del Tratado del Atlántico Norte (OTAN); además, hace hincapié en que el liderazgo militar actual va más allá de la aceptación de tecnología y exige una consideración significativa del papel humano en la guerra algorítmica. De igual forma, examina los efectos que genera la integración de las nuevas tecnologías a los procesos de toma de decisiones, como es el caso de la integración de la IA al Proceso de Selección y Priorización de Blancos. Luego, se abordan los riesgos o las vulnerabilidades a las que podría enfrentarse el Ejército, derivados de esta integración. Finalmente, se propone un modelo estructural para realizar la integración de la IA al proceso, el cual debe ser estudiado en profundidad para posibilitar su optimización y entrada en vigor, acompañado de unas medidas de seguridad y control para mitigar riesgos cibernéticos.

Palabras clave: inteligencia artificial; targeting militar; ciberseguridad; toma de decisiones automatizada; control humano significativo; sistemas de armas autónomos.

* Artículo de investigación.

- a** Candidato a doctor en Sistemas de Información, Universidad de las Américas y el Caribe (Colima, México). Magister en Ciencias de la Información y las Comunicaciones, Universidad Distrital Francisco José de Caldas (Bogotá, Colombia). Correo electrónico: jaider.ospina@esdeg.edu.co; ORCID: <https://orcid.org/0000-0002-3251-3017>
- b** Magister en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra (Colombia). Correo electrónico: artillero208@gmail.com; ORCID: <https://orcid.org/0009-0000-5147-9734>

Effects of Integrating Artificial Intelligence into the Target Selection and Prioritization Process in the Fires Combat System

Abstract: This article presents a discussion on the current use of artificial intelligence (AI) in decision-making and defense systems, along with examples of countries and organizations that already integrate AI into their operations, such as the United States, China, Israel, and the North Atlantic Treaty Organization (NATO). It also emphasizes that current military leadership goes beyond the mere acceptance of technology and demands significant consideration of the human role in algorithmic warfare. Likewise, it examines the effects generated by the integration of new technologies into decision-making processes, such as the integration of AI into the Target Selection and Prioritization Process. It then addresses the risks or vulnerabilities the Army could face as a result of this integration. Finally, it proposes a structural model for integrating AI into the process, which must be studied in depth to enable its optimization and implementation, accompanied by security and control measures to mitigate cyber risks.

Keywords: artificial intelligence; military targeting; cybersecurity; automated decision-making; meaningful human control; autonomous weapons systems.

Efeitos da integração da inteligência artificial no Processo de Seleção e Priorização de Alvos no sistema de combate de fogos

Resumo: O artigo apresenta uma discussão sobre o atual emprego da inteligência artificial (IA) em sistemas de tomada de decisão e de defesa, bem como exemplos de países e organizações que já integram a IA em suas operações, como é o caso dos Estados Unidos, China, Israel e da Organização do Tratado do Atlântico Norte (OTAN); além disso, destaca que a liderança militar atual vai além da aceitação de tecnologia e exige uma consideração significativa do papel humano na guerra algorítmica. Da mesma forma, examina os efeitos gerados pela integração das novas tecnologias nos processos de tomada de decisão, como é o caso da integração da IA ao Processo de Seleção e Priorização de Alvos. Em seguida, são abordados os riscos ou as vulnerabilidades que o Exército poderia enfrentar, derivados dessa integração. Por fim, propõe-se um modelo estrutural para realizar a integração da IA ao processo, o qual deve ser estudado em profundidade para possibilitar sua otimização e entrada em vigor, acompanhado de medidas de segurança e controle para mitigar riscos cibernéticos.

Palavras-chave: inteligência artificial; targeting militar; cibersegurança; tomada de decisão automatizada; controle humano significativo; sistemas de armas autônomos.

El hombre necesita la máquina y la organización, pero tiene que dominarlas y humanizarlas en vez de resignarse a ser mecanizado y deshumanizado por ellas. El verdadero peligro para el hombre no está en los riesgos que corre la seguridad material, sino en el oscurecimiento del hombre mismo en su propio mundo humano.

Rabindranath Tagore (1861-1941)

Introducción

El crecimiento y desarrollo actual de la inteligencia artificial (IA) están sometiendo a una transformación radical la concepción de los conflictos y la forma de hacer la guerra. En comparación con la Antigüedad, cuando el eje central de la guerra era el enfrentamiento frontal como única dimensión, los conflictos actuales obligan la integración de otros dominios. Hoy se habla de la batalla multidominio, la cual además incluye el espacio, el ciberespacio, el espectro electromagnético e incluso competencias específicas como la robótica. La dinámica que caracteriza los conflictos de la actualidad sobrepasa las capacidades de percepción y reacción del ser humano, por lo cual se exige que estas capacidades sean optimizadas mediante el empleo de tecnologías disruptivas que permitan mejorar los procesos militares con herramientas de toma de decisiones como la IA, la cual tiene capacidad de operar con velocidad, alta precisión y autonomía en la incertidumbre operativa (Corvalán, 2018, p. 295).

Los ámbitos en los que el empleo militar de la IA se ha expandido en este nuevo paradigma son tres: los sistemas autónomos letales, los mecanismos de ciberdefensa automatizada y el planeamiento estratégico operacional. Cada uno de ellos reconfigura los tiempos, las escalas y las responsabilidades de la conducción militar, y facilita la aplicabilidad de sistemas que aprenden, deciden y ejecutan acciones sin la intervención humana directa (Gómez de Ágreda, 2024). Esta transformación no solo modifica la estructura de los poderes relativos de los Estados, sino que, a su vez, plantea serios desafíos éticos, legales y doctrinales (Bosio-Ballesteros, 2023).

La IA ha demostrado un gran potencial para redefinir los procesos de las operaciones militares revolucionando el nivel operacional. Esta facilita el análisis de *big data* en tiempo real, optimiza la asignación de recursos y aumenta la conciencia situacional de los comandantes, al tiempo que amplía su visión del panorama operacional. Como ejemplo, la integración de la IA en plataformas como DeepCOM ha reducido la carga cognitiva de los analistas e impulsado la generación de inteligencia procesable (Nitzl et al., 2024). En el nivel táctico, los algoritmos de IA se están entrenando para reconocer patrones de amenaza y contribuir a los procesos de selección y priorización de objetivos, lo que posibilita una integración progresiva en sistemas de armas automatizados, siempre con el principio de control humano significativo (Díaz Valenzuela et al., 2024).

En la actualidad, existen países que ya se encuentran bien posicionados en este ámbito. Estados Unidos, por ejemplo, ha impulsado proyectos como Project Maven o la Third Offset Strategy, los cuales apuntan a la conservación de su hegemonía tecnológica; por otra parte, China ha hecho pruebas de despliegue de “enjambres de drones autónomos” como punta de lanza de su doctrina de guerra algorítmica (Congressional Research Service, 2020). Israel, desde hace ya un tiempo, ha incorporado la IA en sus sistemas de defensa como el Iron Dome y recientemente en la búsqueda y selección automatizada de blancos como Where’s Daddy y Lavender (Abraham, 2024). La OTAN, por su parte, ya ha promulgado marcos normativos como la *NATO AI Strategy*, que buscan el empleo ético y seguro de estas tecnologías en el ámbito de la defensa (Cuartero Lorenzo, 2023).

Con este panorama, es comprensible que surjan diversos interrogantes en los ámbitos de la ciberseguridad y la ciberdefensa en el contexto estratégico colombiano. En consecuencia, la presente investigación formula la pregunta ¿cuál es el modelo estructural que permite integrar la IA en el Proceso de Selección y Priorización de Blancos (PSPB) del Ejército Nacional de Colombia, garantizando las medidas de ciberseguridad necesarias para el proceso?

Para responder a este interrogante, se establece como objetivo general analizar y demostrar la viabilidad de la integración de la IA en el PSPB, mediante el diseño de una estructura operativa respaldada por medidas y controles de ciberseguridad.

La investigación se organiza en cuatro objetivos específicos: 1) identificar en qué etapas del PSPB es posible integrar herramientas de IA para optimizar el PSPB, 2) determinar las vulnerabilidades que podrían surgir en dicho proceso a partir de la incorporación de la IA, 3) diseñar un modelo estructural de integración de la IA en el PSPB y 4) proponer medidas de seguridad y control orientadas a mitigar los riesgos cibernéticos asociados a esta integración.

Marco teórico-conceptual

Para garantizar la rigurosidad del análisis, la investigación se sustenta en las contribuciones de teóricos clásicos de la estrategia militar. Por ejemplo, Carl von Clausewitz (1832/1999), quien introdujo conceptos fundamentales como el de los centros de gravedad (CoG), entendidos como los puntos de concentración de las fuerzas enemigas cuya neutralización podría provocar su colapso; la fricción, concebida como los obstáculos inherentes a la conducción de las operaciones, y la niebla de la guerra, es decir, la incertidumbre derivada de la falta o ambigüedad de la información sobre el adversario. En esta misma línea, Jomini (1992) destacó la relevancia de los puntos decisivos y la necesidad de concentrar las fuerzas en torno a las líneas de operaciones, aportes que enriquecen el marco teórico de la presente investigación.

A pesar de la importancia de estos aportes teóricos clásicos, es innegable que el entorno operacional contemporáneo dista de las necesidades que analizaron en su tiempo Clausewitz (1832/1999) y Jomini (1992). En la actualidad, los comandantes presentan otras demandas y su análisis requiere perspectivas teóricas que coadyuven a evaluar los centros de gravedad y puntos decisivos en el momento de la toma de decisiones o priorización de blancos. En este caso, la teoría de Revolución en Asuntos Militares (RAM), desarrollada por Colom-Piella (2014), facilita la comprensión de los

cambios significativos de paradigma en los entornos operacionales bélicos a lo largo de la historia. De esta manera, los autores sostienen que “la llamada Revolución en los Asuntos Militares (RAM) representa una modificación radical en los estilos de combate, derivada de la incorporación de tecnologías emergentes, innovaciones doctrinales y nuevos esquemas organizativos” (p. 28). Esta revolución militar no solo transforma las formas de operar, sino que otorga una ventaja táctica y estratégica al actor que logre adaptarse primero a dichos cambios estructurales. Por su parte, King (2024) introduce el concepto de *targeting digital*, argumenta que “las fuerzas armadas han aprovechado principalmente la IA para acelerar y mejorar la selección de objetivos militares” (p. 1), y establece que la verdadera revolución militar contemporánea no radica en sistemas autónomos letales, sino en la capacidad de procesar datos masivos para el *targeting* inteligente. King (2024) enfatiza que “la IA ha sido empleada para el procesamiento de datos, de manera que los comandantes tengan mejor comprensión del espacio de batalla y puedan realizar *targeting* más efectivo” (p. 3). Esta perspectiva complementa la RAM tradicional al demostrar cómo la integración de IA en procesos de selección de blancos constituye el núcleo de la transformación militar actual.

Asimismo, Gómez de Ágreda (2024) sostiene que, pese a las bondades de esta nueva tecnología, se requiere una revisión crítica del nivel de autonomía que se le asigna, en términos militares, a una IA; advierte además que la supervisión humana no debe ser reemplazada. Sin embargo, según la Secretaría General Técnica del Ceseden (2020), el proceso de toma de decisiones en el nivel operacional debe estar cada vez más asistido por sistemas de IA que potencien, sin sustituir, el juicio del comandante. Dicha inteligencia simplifica y enriquece la información disponible, por lo cual es necesario emplear modelos de decisión híbridos sin condicionar la decisión final.

Estas perspectivas son útiles porque permiten dimensionar cómo la transformación del paradigma del uso de la IA como herramienta en el PSPB puede traer importantes ventajas, al tiempo que aumenta los desafíos en su operación. Esta

comprensión sustenta la propuesta del modelo estructural que posibilite la integración de la IA a dicho proceso en el Ejército Nacional de Colombia, al no resaltar únicamente sus beneficios, sino sus desafíos.

En este orden de ideas, la teoría respalda el objetivo de brindarle al comandante una herramienta que le facilite explotar al máximo sus capacidades, entender la guerra no solo como una interacción física, sino como un proceso fluctuante que requiere revisión constante, el cual con la asistencia de la IA transforma radicalmente los modos, medios y fines de la acción militar.

Metodología

Esta investigación desarrolla un estudio exploratorio-descriptivo, con componentes explicativos mediante la exploración y el análisis documental, así como el estudio de casos doctrinales en el marco militar. El enfoque metodológico se fundamenta en el método de revisión documental y el análisis de contenido, por medio de los cuales se examinaron de manera sistemática fuentes académicas, doctrinales y documentos estratégicos relacionados con la implementación de IA en procesos de toma de decisiones militares.

El desarrollo investigativo se estructuró alrededor del ciclo D3A (*decide, detect, deliver, assess*) en el PSPB, para identificar cómo podría configurarse un modelo estructural de integración de la IA que resulte pertinente y adaptable a este proceso. Para el desarrollo de este trabajo se seleccionaron fuentes con alto contenido académico, incluida literatura especializada en seguridad y defensa del Instituto Español de Estudios Estratégicos y publicaciones previas de la Escuela Superior de Guerra de Colombia sobre tendencias en implementación de la IA.

La estrategia metodológica incorporó el análisis de estudios de caso documentados, como los sistemas Lavender y Where's Daddy, empleados por Israel en Gaza, así como el Project Maven del Departamento de Defensa de Estados Unidos, para ilustrar tanto las prácticas actuales como los riesgos asociados a la implementación de estas tecnologías. El análisis contrasta sistemáticamente la

doctrina nacional con los desarrollos de referencia internacional, en particular la estrategia implementada por la OTAN en materia de automatización del *targeting*.

Para garantizar la pertinencia y calidad de la información analizada, se establecieron criterios específicos de inclusión y exclusión. Los contenidos incluidos se circunscribieron a empleos de la IA en procesos militares de toma de decisiones, literatura sobre selección de objetivos y armas o sistemas de defensa de respuesta automática, documentación sobre integración tecnológica en el ciclo D3A, fuentes con alto contenido académico en seguridad y defensa, así como casos de estudio documentados de implementación de IA militar. Se excluyeron aplicaciones de IA no relacionadas directamente con el PSPB y sistemas de armas autónomas letales del todo independientes, manteniendo el foco en el contexto operacional del Ejército Nacional de Colombia.

En cuanto a la transparencia metodológica, el análisis de contenido se estructuró en tres categorías principales: 1) empleo de IA en ciclos de *targeting* y D3A; 2) vulnerabilidades técnicas, operacionales y éticas asociadas a la automatización de la selección de blancos y 3) medidas de ciberseguridad y control humano significativo en sistemas militares de apoyo a la decisión. Cada documento fue codificado según estas categorías, registrando de forma sistemática los casos de uso, tipos de algoritmos empleados, riesgos identificados y controles propuestos, lo que permitió construir la matriz que sirve de base al modelo estructural en cinco fases. Esta matriz permitió contrastar de manera sistemática la doctrina nacional con los casos internacionales examinados y, al mismo tiempo, identificar patrones comunes útiles para el diseño del modelo estructural. De esta manera, la propuesta no surge solo de una revisión narrativa de literatura, sino de una organización analítica que vincula hallazgos empíricos documentados, categorías doctrinales y requerimientos de ciberseguridad aplicables al PSPB.

No obstante, se reconoce como limitación que el modelo aún no ha sido validado de manera empírica mediante entrevistas a oficiales de la célula de fuegos, analistas de inteligencia o ingenieros de

ciberseguridad del Ejército Nacional de Colombia. Esta ausencia de contrastación con la experiencia local obliga a considerar el modelo como una propuesta inicial, susceptible de ser ajustada una vez se incorporen fases futuras de validación cualitativa y pruebas piloto en unidades específicas.

Integración de la inteligencia artificial al Proceso de Selección y Priorización de Blancos

Para comenzar el análisis es pertinente realizar una contextualización sobre el PSPB que se encuentra definido y descrito en el *Manual de técnicas del Ejército Nacional (MTE) 3-60*; este proceso es garantía no solo de legalidad, sino de la calidad de los apoyos que se prestan al sistema de fuegos (Ejército Nacional de Colombia, 2019a). Uno de sus propósitos es buscar identificar capacidades enemigas, cuya neutralización contribuya de manera directa al cumplimiento de la intención del comandante.

Durante su ejecución, el PSPB se encuentra con varias restricciones operacionales que reducen su capacidad. Una de ellas es el hecho de que, en ocasiones, se cuenta con poco tiempo para recolectar y procesar información crítica del ambiente operacional y menos tiempo aún para validar blancos y coordinar acciones letales y no letales (Ejército Nacional de Colombia, 2016).

La metodología de desarrollo del PSPB se centra básicamente en el seguimiento de un ciclo de cuatro pasos que son: decidir, detectar, entregar y evaluar (D3A). Este proceso se descompone en una secuencia lógica de acciones, desarrolladas por la metodología D3A, cuyo objetivo es identificar, validar y neutralizar blancos, según una serie de prioridades y criterios operacionales y legales. Esta a su vez establece que, para cumplir con los estándares operacionales y legales, se requiere una integración eficaz de las funciones de mando, inteligencia y sistemas de adquisición de blancos (Ejército Nacional de Colombia, 2019a, p. 2-1).

En cada fase existe una tarea fundamental para cumplir: en la etapa de decisión lo principal es el direccionamiento de esfuerzos con arreglo a la intención del comandante; la detección es la

búsqueda y el seguimiento de blancos con prioridad de alto valor o alta retribución; la entrega es la aplicación de efectos deseados en los blancos que han sido listados y validados, mediante el empleo de las armas a disposición; y como último tenemos la evaluación, que no es otra cosa que la verificación de los efectos logrados sobre los blancos tratados y la amenaza residual. Esta evaluación incluye la decisión de cesar el ataque o recomendar un segundo ataque.

En este contexto, la introducción de herramientas de IA representa una oportunidad estratégica para mejorar la eficiencia del PSPB, que permite capacidades extendidas de asistencia por su capacidad de asistir a la célula de fuegos y al oficial de inteligencia de apoyo para recopilar, analizar y fusionar datos de los sensores (ISR E, UAV E, SIGINT, HUMINT E), acelerar la toma de decisiones y la priorización de blancos de alto valor (HVT) y los de alta retribución (HPT). Además, la IA podría elaborar de manera eficiente la Matriz Guía de Ataque (AGM), lo que garantiza la verificación, la actualidad y la confiabilidad de la información de cada uno de los blancos, además de la asignación prioritaria de estos blancos a los sistemas de fuego más adecuados, en razón a su disponibilidad, capacidad, alcance, localización, tipo de blanco y su permanencia. Además, podría generar alertas tempranas sobre comportamientos atípicos de los blancos o apoyar la administración de riesgos para reducir daños colaterales y evitar el uso excesivo de la fuerza (Ejército Nacional de Colombia, 2016, pp. 3-18 a 3-21).

Una visión prospectiva en torno a esta tecnología la ha desarrollado el mayor Jorge Iván García Torres (2024), quien asegura que la IA perfecciona la capacidad de los centros de combate y de defensa, el tratamiento inmediato de gran cantidad de información para una visión completa de la situación de los territorios, y funciona como una base para prever cambios y peligros. Esta visión respalda la posibilidad de integrarlas en doctrinas inteligentes al proceso de *targeting* de un país.

Por otra parte, pese a que el MTE 3-60 no menciona el empleo de IA específicamente, sus descripciones sobre la necesidad de tecnología, la interoperabilidad entre agencias y el empleo de

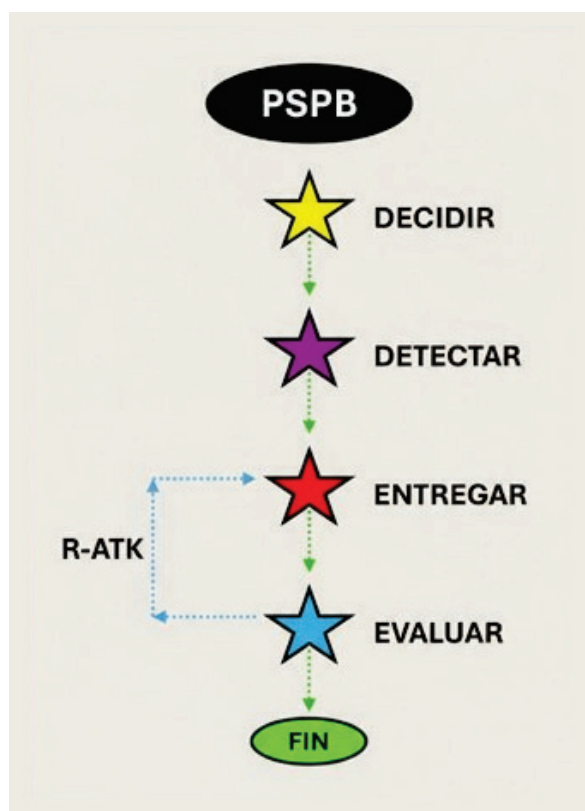
medios de recolección inexorablemente abren un espacio claro para desarrollar esta integración (Ejército Nacional de Colombia, 2019b). Esta debe hacerse con políticas institucionales, reglas de enfrentamiento y controles éticos, para asegurar que el juicio humano predomina en las decisiones críticas, como la legalidad del blanco y la proporcionalidad del ataque.

En el contexto colombiano, la integración propuesta debe armonizarse con las capacidades reales de mando y control, comunicaciones y sensores actualmente disponibles en las unidades de fuego y de inteligencia. A diferencia de los casos de estudio de potencias como Estados Unidos o Israel, el Ejército Nacional de Colombia enfrenta limitaciones de conectividad en áreas rurales, dependencia de plataformas aéreas de ala rotatoria envejecidas (como la flota UH-1N y Huey II) y procesos de modernización gradual hacia helicópteros y sistemas ISR más avanzados. Estas condiciones obligan

a que las fases del modelo de IA se implementen de manera escalonada, priorizando inicialmente la analítica de datos en centros de inteligencia y la fusión multisensor básica, para luego incorporar capacidades más complejas de *targeting* digital conforme se renuevan las plataformas y se fortalecen las redes tácticas.

No menos importante es entender el hecho de que la integración propuesta no puede plantearse como una simple transferencia de experiencias internacionales, sino como una adaptación doctrinal y tecnológica al marco funcional del MTE 3-60 y a las capacidades reales del Ejército Nacional de Colombia. Si bien dicho manual no formula un capítulo específico sobre IA, su arquitectura operativa sí prevé la articulación entre mando, inteligencia, adquisición de blancos y sistemas de fuego, lo que ofrece una base doctrinal suficiente para incorporar herramientas algorítmicas como medios de apoyo a la decisión. La figura 1 ilustra el PSPB.

Figura 1. Proceso de Selección y Priorización de Blancos



Fuente: elaboración propia con base en la información del *Manual PSPB MTE 3-60*.

Identificar en qué etapas del PSPB se pueden integrar herramientas de IA para optimizar la selección y priorización de blancos

En el contexto de la guerra, en el cual la precisión al atacar un blanco y la disminución del daño colateral son fundamentales, la implementación de la IA en el PSPB permite consolidar el entendimiento de la situación y la asignación efectiva de los recursos de fuego. Esto posibilita al comandante una toma de decisiones más acertada, una mejor administración de los recursos, la minimización de los riesgos de daño colateral y el aseguramiento de la proporcionalidad en el uso de la fuerza. En el panorama actual, en el que la tecnología ha evolucionado con sistemas que simulan la inteligencia humana, capaces de analizar y sistematizar grandes cantidades de información, el PSPB + IA constituiría una herramienta crucial para desarrollar situaciones en las que la precisión desempeña un

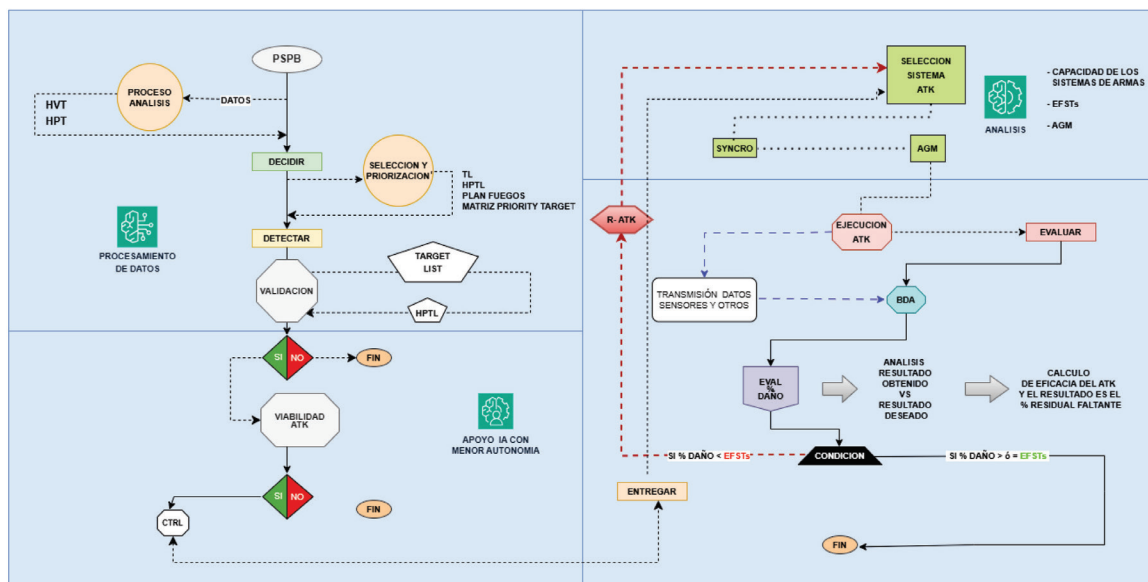
papel tan importante que podrían asegurar el éxito o decretar el fracaso de una operación.

Como se describe en el *Manual de técnicas del Ejército MTE 3-60*, el empleo de una metodología ayuda a determinar qué tareas y propósitos se deben ejecutar para cumplir con los objetivos planteados, qué unidades tienen la capacidad de ejecutarlo y qué sistemas de fuegos se deben emplear en articulación con las maniobras y los otros medios de ataque disponibles (Ejército Nacional de Colombia, 2016, pp. 1-11).

Por su parte, García Torres (2024) asegura que la IA tiene el potencial para mejorar la toma de decisiones tácticas y estratégicas, aprovechar los recursos disponibles y recortar errores en operaciones de alto riesgo (p. 8), lo que indica que se debe modernizar el PSPB con tecnologías emergentes.

Para materializar la integración se analizaron los pasos del proceso de selección y priorización de blancos, y posteriormente se establecen las etapas en las que este proceso podría automatizarse mediante IA; estos se denominan *procesos candidatos*. Para entender mejor lo anterior, la figura 2 ilustra, de manera detallada, la integración propuesta de la IA en el PSPB.

Figura 2. Integración de la IA en priorización de blancos



Fuente: elaboración propia con base en la información del *Manual PSPB MTE 3-60*.

Básicamente existen cuatro subetapas del proceso en las cuales esta integración genera una optimización del proceso. La primera es durante el proceso de análisis, previo a la etapa de Decisión, en la que se recibe una gran cantidad de información, en ocasiones inexacta; la IA puede ayudar a elaborar un análisis rápido y oportuno de toda la información, enfrentándose con los requerimientos del mando superior, para lograr una mayor celeridad en el procesamiento de datos.

Luego de analizar todos los elementos en la etapa de Detección, en la cual se tienen determinadas las listas de blancos (HVT-HPT), es preciso que estas sean verificadas para su validación y para establecer la viabilidad de ataque de estos. La validación y viabilidad son fundamentales para dar legitimidad al proceso y garantizar que no existan “sesgos de máquina” en la toma de decisiones y que exista el control del factor humano en cada decisión.

Una vez las listas tengan la validación y viabilidad necesarias para proceder a la Entrega, la IA puede optimizar esta etapa mediante el procesamiento de datos como la selección del sistema de ATK, su sincronización con las maniobras en curso y, finalmente, generar la Matriz Guía de Ataque AGM (Attack Guide Matrix). Este punto más que una toma de decisión es un proceso matemático, ya que acá se requiere análisis y procesamiento de datos que ya existen, y las decisiones en este punto solo obedecen a resultados matemáticamente más rentables. Para finalizar, la etapa de Evaluación requiere cálculos para establecer el porcentaje residual de la amenaza respecto del requerimiento inicial del comando.

En este punto se puede inferir que existen cuatro etapas en las cuales se puede integrar la IA para potenciar el proceso, y se logra determinar que en una de estas la integración se debe hacer de manera limitada y con mayor supervisión del elemento humano, por la sensibilidad e importancia que reviste la información tratada en este punto.

Esta integración no es novedosa en el ámbito militar, como se señaló previamente. Esta tecnología ya ha demostrado su utilidad en diversas fuerzas armadas del mundo como parte de la Revolución en los Asuntos Militares. De hecho, las potencias que buscan mantener su posición

estratégica en el orden internacional ya la han incorporado a sus capacidades. Un ejemplo de ello es Project Maven, desarrollado por el Departamento de Defensa de Estados Unidos, que emplea IA para el procesamiento de videos de vigilancia y el análisis de imágenes satelitales. Su implementación ha mejorado significativamente la etapa de Decidir, al reducir la carga cognitiva asociada con la interpretación de grandes volúmenes de información visual. En este sentido, el *Bulletin of the Atomic Scientists* justifica su utilización al afirmar que

[...] aviones y satélites estadounidenses recopilan más datos brutos de los que el Departamento de Defensa podría analizar incluso si dedicara toda su fuerza de trabajo a ello. Lamentablemente, el análisis de imágenes suele ser una tarea tediosa —implica mirar pantallas para contar automóviles, personas o actividades... la mayoría de los datos de los sensores simplemente desaparecen y nunca se observan—, a pesar de que el Departamento ha contratado a la mayor cantidad posible de analistas durante años. (González, 2023, p. 90)

Este proyecto comenzó su implementación en el 2017 y, durante sus primeras etapas operativas, etiquetó aproximadamente 150 000 imágenes para el entrenamiento del algoritmo. En relación con esta dinámica, el coronel de la Infantería de Marina de Estados Unidos, Drew Cukor, afirmó: “Estamos en una carrera armamentista de inteligencia artificial. Está ocurriendo en la industria y las cinco grandes empresas de Internet están dedicando todos sus recursos a desarrollar esta tecnología” (González, 2023, p. 91).

La evidencia empírica reciente respalda estos avances. Por un lado, Baxter (2024) demuestra que “los sistemas impulsados por IA pueden procesar datos de múltiples fuentes, como sensores, vehículos aéreos no tripulados (UAV) y satélites, proporcionando a los comandantes información actualizada e inteligencias clave para decisiones más informadas y oportunas” (p. 3). Asimismo, investigaciones de Collins Aerospace destacan que las herramientas de IA “mejoraron la precisión del reconocimiento de objetivos, asistiendo rápidamente a los operadores humanos y optimizando la efectividad durante los enfrentamientos” (p. 2).

Por otro lado, estudios de la RAND Corporation señalan que estos sistemas pueden “analizar vastas cantidades de datos y detectar, analizar y responder a ataques más rápida y efectivamente que los operadores humanos” (p. 3). En el ámbito táctico, este desempeño se traduce en reducciones de hasta el 70 % en los tiempos de procesamiento dentro del ciclo sensor-disparador.

Implementaciones contemporáneas: el caso NATO MSS

La implementación práctica de IA en *targeting* militar ha evolucionado significativamente en 2024-2025. La OTAN completó la adquisición del Maven Smart System NATO (MSS) de Palantir, un sistema habilitado por IA para operaciones de combate que mejora la fusión de inteligencia, la selección de objetivos (*targeting*) y la aceleración de la toma de decisiones (NATO Communications and Information Agency, 2025). Este sistema representa la primera implementación operacional a gran escala de IA para la selección colaborativa de objetivos entre múltiples aliados y ha demostrado capacidades para integrar en tiempo real datos de inteligencia procedentes de múltiples sensores, proporcionando a los comandantes una imagen operacional común enriquecida mediante algoritmos de aprendizaje automático (Defense Update, 2025).

King (2024) analiza casos similares como el Security Assistance Group-Ukraine, en el cual “el XVIII Cuerpo Aerotransportado también asistió al militar ucraniano en identificar objetivos rusos mediante el uso de datos procesados por IA. Muchos de esos objetivos fueron posteriormente atacados con fuego de artillería o cohetes” (p. 4). Este caso demuestra que “la dataficación del *targeting*, evidente en Liverpool y por el Security Assistance Group-Ukraine, probablemente tendrá efectos profundos en las fuerzas armadas, relaciones internacionales y competencia entre grandes potencias en el futuro cercano” (p. 4).

Determinar las vulnerabilidades que puede enfrentar el PSPB con la integración de herramientas de IA

El PSPB, como función crítica dentro del sistema de combate de fuegos, enfrenta diversos riesgos, tanto operacionales como legales y éticos, que son inherentes a su estructura y ejecución. Tal vez uno de los riesgos más importantes al que se enfrenta es la dependencia del juicio humano, en especial en situaciones de estrés o bajo presión de tiempo, lo cual puede derivar en errores de apreciación, clasificación indebida de objetivos o fallos en la proporcionalidad del ataque. Además, existe la posibilidad de la presencia de sesgos cognitivos o de información durante la fase de evaluación de los blancos y la asignación de los efectos deseados sobre estos, lo que podría, indiscutiblemente, comprometer la legalidad y legitimidad del uso de la fuerza.

Asimismo, la integración de tecnologías en procesos y sistemas militares implica riesgos significativos si no se establecen mecanismos robustos de validación y supervisión humana. La ausencia de estos controles podría derivar en decisiones erróneas, cuya magnitud se vería incrementada por la velocidad del procesamiento automatizado y por la opacidad algorítmica, lo que genera escenarios en los que la detección de fallas ocurra demasiado tarde para implementar medidas correctivas eficaces.

Para Gómez de Ágreda (2024), la verdadera clave radica en la autonomía de los comandantes para la toma de decisiones, lo que exige preservar la agencia humana como garantía de control y responsabilidad en el proceso.

La integración de las herramientas de IA en este proceso va a potencializar indiscutiblemente la eficiencia del proceso; sin embargo, también debemos ser conscientes de que esta mejora trae consigo riesgos y vulnerabilidades que deben ser tenidos en cuenta para tomar acciones respectivas. En el presente estudio se han identificado básicamente tres grupos generales de vulnerabilidades que se describirán a continuación.

Grupo de vulnerabilidades en la protección de datos

En este grupo se puede presentar manipulación de datos de tipo SQL Injection o MITM, mediante los cuales un adversario puede extraer, inyectar o modificar los datos que se estén manejando en el proceso, con el fin de orientar un error en el proceso y ocasionar una desinformación en los sistemas, incluso yendo más allá, al impulsar la creación de datos falsos para que, en lugar de atacar los objetivos enemigos, el ataque se oriente hacia instalaciones protegidas, población civil o incluso las propias tropas. Otra posible acción puede ser generar estos ataques directamente a los sistemas de detección, para modificar los algoritmos para que los radares no logren identificar las amenazas. Según un informe presentado por el Congressional Research Service (2020), los sistemas de IA militares, al igual que los sistemas digitales, son altamente susceptibles a formas únicas de manipulación (p. 2).

Grupo de vulnerabilidades en la precisión de la inteligencia artificial

Como todo sistema computacional, la IA actúa en función de algoritmos que ejecutan criterios, parámetros y reglas de decisión predefinidas. Si bien la efectividad de la IA radica en su capacidad para procesar volúmenes masivos de datos en tiempo real, dicha capacidad operacional depende directamente de la calidad, integridad y exactitud de los insumos de información con los que se alimenta.

En consecuencia, la alteración o el envenenamiento de los datos desde la fuente (*data poisoning*) provoca respuestas inexactas o desviadas por parte del sistema, lo que desencadena fenómenos de sesgo algorítmico o de máquina. En el PSPB, esta vulnerabilidad resulta crítica, ya que compromete la confiabilidad de procesos sensibles como la identificación, clasificación y evaluación de blancos.

La IA podría clasificar erróneamente objetivos militares o civiles, y generar fallos críticos en operaciones. En su informe, el Congressional Research Service (2020) menciona que el desarrollo de la IA puede aumentar la necesidad de contar con altos estándares de seguridad, y más adelante, en

este mismo informe, desarrolla un análisis acerca de la forma en la que los algoritmos de IA se vuelven vulnerables a sesgos, robos y manipulaciones, en particular si el conjunto de datos de entrenamiento no está adecuadamente seleccionado o protegido (p. 13).

Grupo de vulnerabilidades en la supervisión humana

Sumado a las vulnerabilidades asociadas a la integridad de los datos, emerge el riesgo de la sobredependencia tecnológica (*automation bias*). Este fenómeno se manifiesta cuando el personal militar confía excesivamente en los algoritmos, omitiendo las verificaciones de inteligencia humana (HUMINT) debido a un historial previo de aciertos del sistema, lo que conduce a una delegación tácita de la responsabilidad operacional. Al respecto, el informe del Comité Internacional de la Cruz Roja sobre IA y tecnologías relacionadas en la toma de decisiones militares (Greipl et al., 2024) advierte que “los riesgos e ineficiencias de los sistemas de IA en apoyo al *targeting* militar incluyen la opacidad algorítmica, sesgos en los datos de entrenamiento y la erosión del control humano significativo” (p. 15).

En este escenario, Baxter (2024) establece una distinción operacional determinante entre los esquemas de interacción hombre-máquina: por un lado, el modelo *human-in-the-loop*, en el cual “los humanos permanecen activamente comprometidos e influyen de forma directa en la toma de decisiones asistida por IA”; por otro lado, el enfoque *human-on-the-loop*, referente a “una supervisión de mayor nivel donde los humanos monitorean y gestionan el desempeño del sistema, interviniendo únicamente cuando se requiere” (p. 6).

Esta degradación del criterio operacional suele gestarse de manera gradual debido a falencias en la capacitación del personal para interpretar las recomendaciones de los algoritmos. Por ello, resulta imperativo implementar protocolos de control que exijan la validación humana obligatoria antes de transmitir cualquier orden de ataque. Como enfatiza Baxter (2024), “encontrar el equilibrio adecuado entre estos dos modos de operación es crucial para optimizar las capacidades de los sistemas de

IA, garantizando al mismo tiempo un despliegue responsable y confiable” (p. 6). Gómez de Ágreda (2024) concluye que la aplicación de la IA afecta a las capacidades distintivas del ser humano y que hay que entender la IA como una herramienta para facilitar el ejercicio de los rasgos humanos, no como un sustituto de estos (p. 10). Esta perspectiva se refuerza con la advertencia de que “la colaboración no se vea meramente como integración de tecnologías, sino como una asociación sinérgica donde el juicio humano e *insights* de IA se complementen mutuamente” (Baxter, 2024, p. 6).

Además, existen desafíos en términos de responsabilidad ética y legal en caso de errores derivados de decisiones autónomas por parte de la IA. Un ejemplo de la importancia del *human-in-the-loop* es lo ocurrido en 1983 con un oficial soviético, Stanislav Petrov, quien mientras se encontraba en su puesto de comando empezó a recibir alarmas del sistema indicando una alarma de cinco misiles estadounidenses entrando en espacio aéreo ruso; este, gracias a su experiencia de más de diez años en la fuerza aérea soviética, en lugar de confirmar el lanzamiento de respuesta, cuestionó la validez de la información, analizando con cabeza fría cada uno de los elementos que tenía a su disposición que le permitieron determinar que se trataba de una falsa alarma, lo que finalmente evitó un posible desastre nuclear (Barba-Kay, 2024).

Esta es la forma en la que pueden evitarse errores, siempre que se cuente con personal altamente capacitado y con el amplio criterio para cuestionar una decisión generada por IA.

Entre los riesgos más recurrentes asociados al empleo de IA en el ámbito militar destacan aquellos vinculados a la eventual vulneración de marcos éticos y legales. Diversos autores advierten que la delegación de la selección y neutralización de blancos críticos en sistemas algorítmicos profundiza la deshumanización del conflicto, al tiempo que erosiona principios fundamentales del derecho internacional humanitario, como la distinción entre combatientes y población civil, y diluye la imputabilidad y responsabilidad del mando en la cadena de orden (Gómez de Ágreda, 2024; Moliner, 2017). Otros aseguran que se agudiza el riesgo porque, lejos de garantizar la precisión, la

automatización puede resultar en imprevisibilidad y en la difuminación de la diplomacia o las leyes que pretenden evitar conflictos al reducirse el número de bajas propias y crear un impulso para la extensión de las guerras y la proliferación de armas (Boulanin et al., 2020).

La IA no es un desafío solo técnico, sino también un desafío para la ética directamente al negar la intervención humana en las decisiones sobre la vida de otro ser humano, como se observa en el caso de Lavender: medios y organizaciones de derechos humanos han señalado que se ejecutaron ataques sobre objetivos mal identificados, al haber sido clasificados como combatientes únicamente por su número de teléfono, sin verificación humana suficiente. Esto ilustra el riesgo de clasificación errónea por sesgo de datos.

Para concluir el desarrollo del segundo objetivo y la caracterización de los tres grupos de vulnerabilidades, se infieren tres premisas operacionales fundamentales:

1. Protección e integridad de datos: es imprescindible implementar medidas redundantes de ciberseguridad que garanticen la autenticidad, trazabilidad e inalterabilidad de los insumos de información (*data integrity*).
2. Actualización algorítmica continua: se requiere revisar y actualizar periódicamente los parámetros, criterios y algoritmos que rigen el comportamiento de los sistemas de IA empleados.
3. Preservación del control humano (*human-in-the-loop*): es imperativo asegurar la supervisión e intervención humana directa en la cadena de decisión, para garantizar que el mando militar mantenga el control efectivo y la responsabilidad ética y legal sobre las decisiones de carácter crítico.

Desarrollar un modelo estructural de integración de herramientas de inteligencia artificial en el PSPB

Una vez analizados todos los aspectos referentes a la integración de la IA al PSPB, se propone un modelo estructural en cinco fases que garantice

la integración eficaz de esta inteligencia en dicho proceso, manteniendo como principio rector el control humano significativo y medidas de ciberseguridad como pilares fundamentales.

Fase 1: Captura y procesamiento de datos

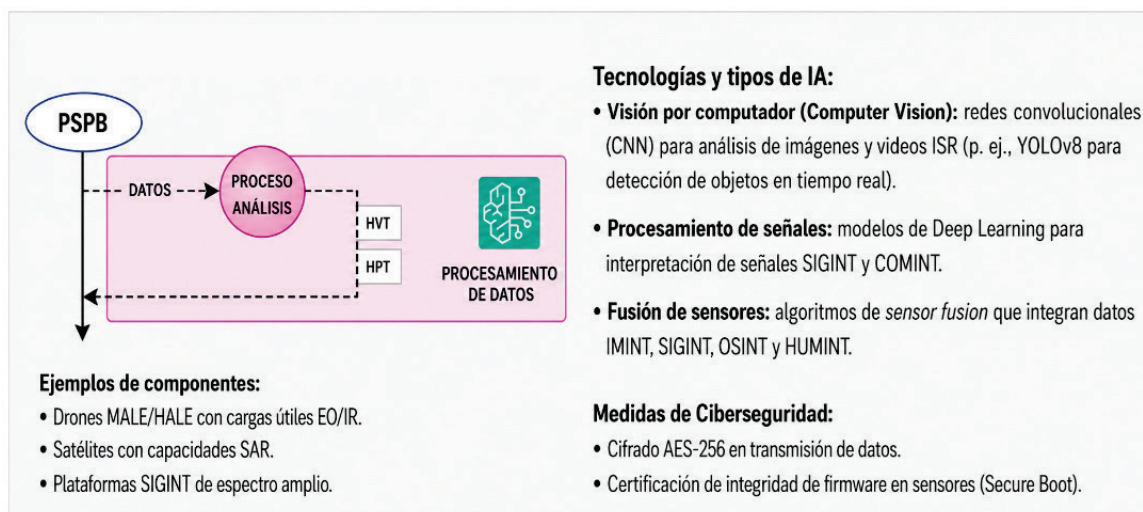
El objetivo de esta fase es la obtención y el procesamiento de la información multisensorial del campo de batalla, y la preparación de esta para su análisis avanzado. Para ello se requiere la implementación de sensores ISR y análisis automatizado

con IA, al igual que el uso de visión artificial y *machine learning* para identificar objetivos (figura 3).

En el caso colombiano, esta fase se apalanca inicialmente en los medios de vigilancia descritos en el MTE 3-60 (sensores terrestres, aeronaves de observación, SIGINT y HUMINT) y en nodos de procesamiento ubicados en centros de inteligencia, para evitar depender de enlaces permanentes de alta capacidad que aún no son generalizados en todas las unidades de maniobra.

En este punto se integran sensores ISR, visión por computador y fusión de datos para alimentar la base de información HVT/HPT.

Figura 3. Fase 1: Captura y procesamiento de datos



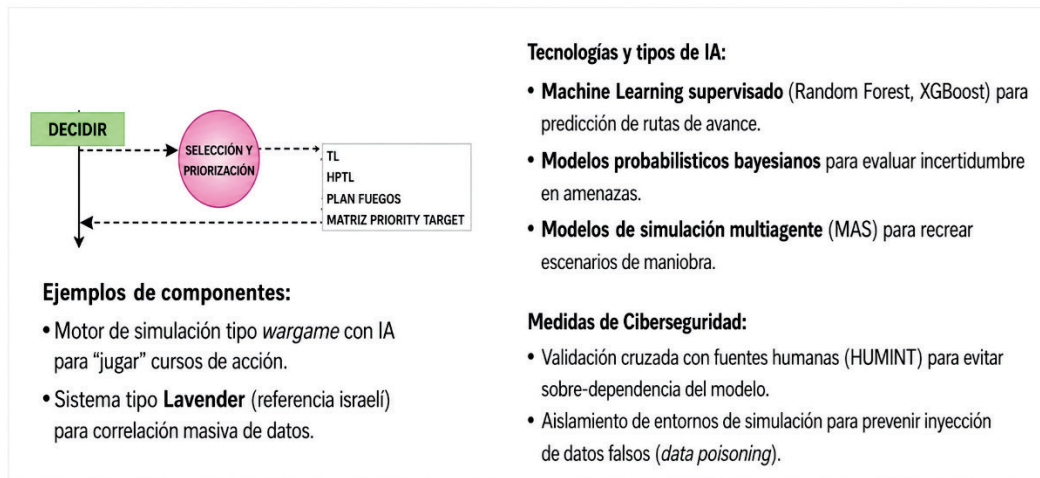
Fuente: elaboración propia con base en la información del *Manual PSPB MTE 3-60*.

Fase 2: Análisis predictivo y modelado de amenazas

El objetivo de esta fase es la anticipación de movimientos y patrones del enemigo para poder

priorizar las acciones por ejecutar. Para esta fase se requiere el empleo de una IA aplicada a la identificación de tendencias de movimientos del enemigo y la implementación de modelos probabilísticos para evaluar riesgos operacionales (figura 4).

Figura 4. Fase 2: Análisis predictivo y modelado de amenazas



Fuente: elaboración propia con base en la información del *Manual PSPB MTE 3-60*.

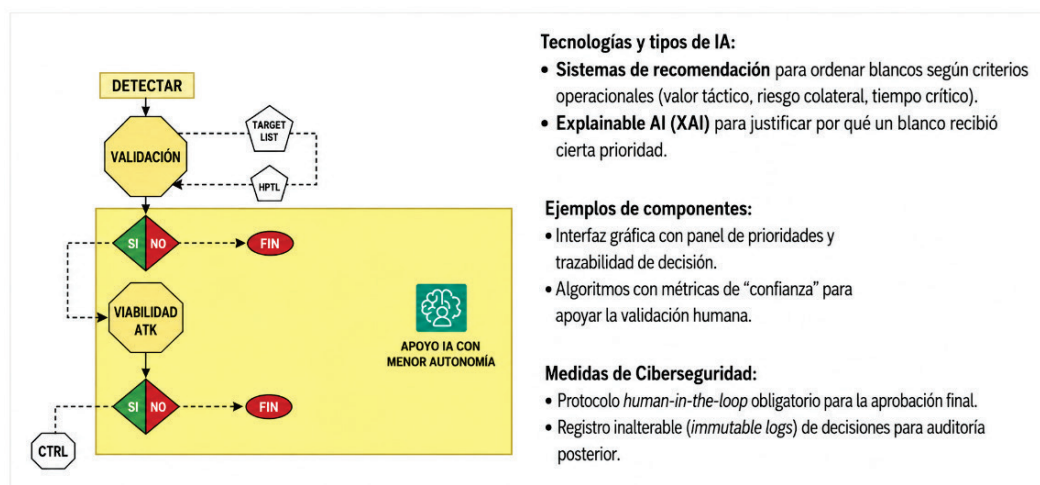
Aquí entran los algoritmos predictivos a estimar movimientos y riesgos antes de decidir la prioridad de blancos.

Fase 3: Priorización y validación de blancos

El objetivo de esta fase es asignar niveles de prioridad a cada uno de los blancos y posteriormente

validarlos con la supervisión humana. Para esta fase se requieren algoritmos de IA con capacidad de análisis y comparación de criterios que después permitan asignar niveles de prioridad a los blancos identificados; una vez desarrollado esto, es necesario pasar por el filtro de validación manual de los blancos antes de aprobar su selección (figura 5).

Figura 5. Fase 3: Priorización y validación de blancos



Fuente: elaboración propia con base en la información del *Manual PSPB MTE 3-60*.

En esta parte del proceso, como se menciona en la figura 5, opera la IA con menor autonomía, proponiendo prioridades y validando criterios, pero con verificación humana.

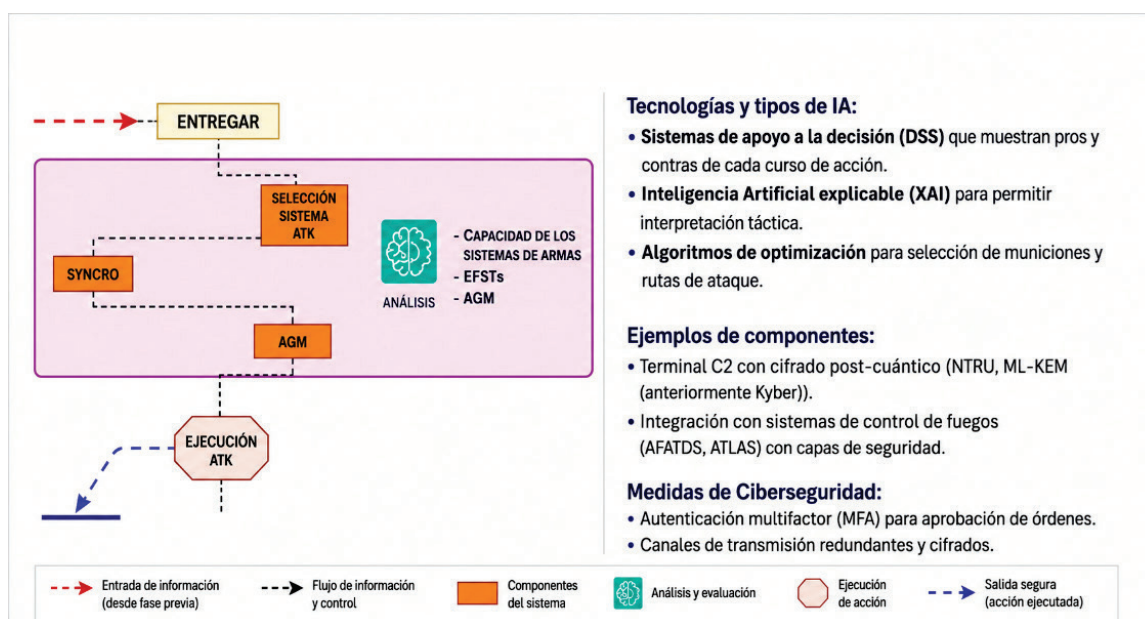
En términos doctrinales, esta fase se integra de forma directa con los procedimientos de validación y control de legalidad que ya establece el *MTE 360*, de modo que los algoritmos de IA se conviertan en apoyo analítico a la construcción de la Matriz Guía de Ataque y de las listas HVT/HPT, sin reemplazar los pasos de revisión jurídica y operacional prescritos para el PSPB.

Fase 4: Toma de decisiones y ejecución segura

El objetivo de esta fase es garantizar que la ejecución o el tratamiento de blancos se haga de una manera controlada, segura y estable. Para esta fase se requiere el envío de órdenes cifradas y supervisión humana en la ejecución de ataques, al igual que la implementación de IA explicable (XAI) para que las decisiones sean fácilmente interpretables.

En este punto la IA optimiza la selección del sistema de armas y las rutas, pero siempre bajo control humano y cifrado seguro (figura 6).

Figura 6. Fase 4: Toma de decisiones y ejecución segura



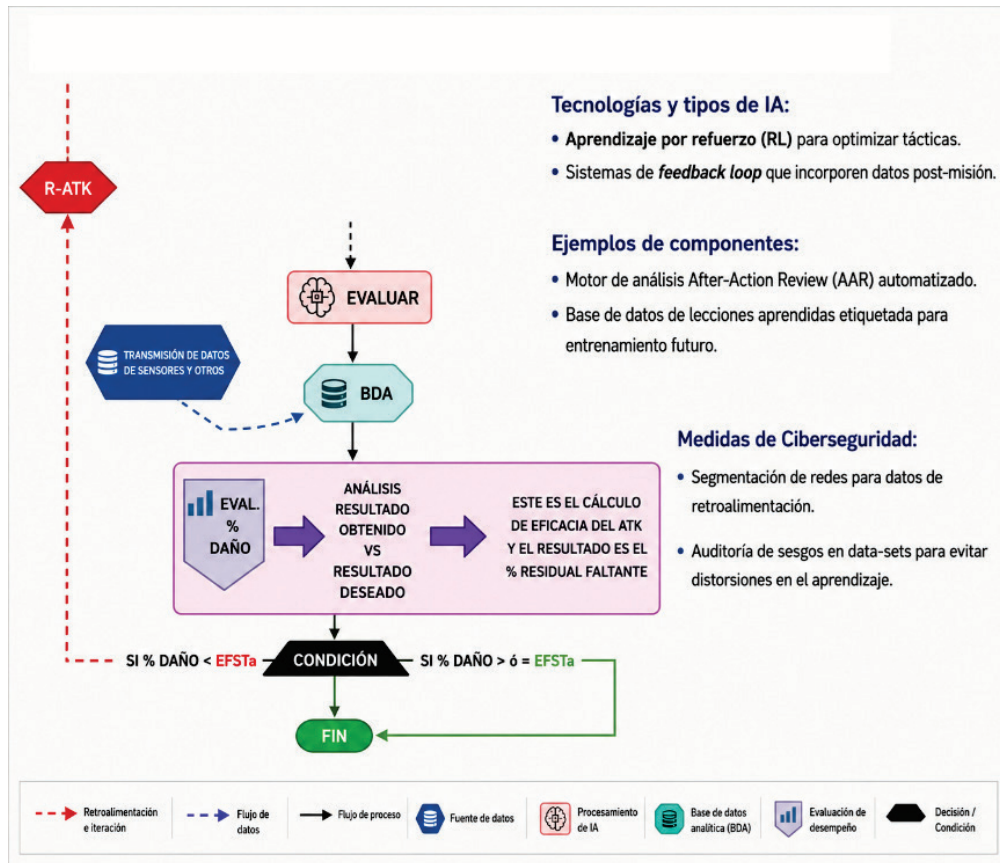
Fuente: elaboración propia con base en la información del *Manual PSPB MTE 3-60*.

Fase 5: Evaluación y aprendizaje automático

El objetivo de esta fase es mejorar continuamente el sistema con base en resultados reales y lecciones

aprendidas. Para esta fase se requiere un mecanismo de retroalimentación de datos para mejorar el rendimiento de la IA y crear un sistema de aprendizaje continuo con base en experiencias previas (figura 7).

Figura 7. Fase 5: Evaluación y aprendizaje automático



Fuente: elaboración propia con base en la información del *Manual PSPB MTE 3-60*.

Aquí la IA analiza el porcentaje de daño y lo compara con el resultado esperado, alimentando un sistema de aprendizaje continuo, y recomienda un segundo ataque si es necesario para cumplir con los objetivos planteados por el comandante en su estado final deseado, y posteriormente el elemento humano valida si se da o no el R-ATK.

La implementación práctica en Colombia requiere, en el corto plazo, concentrar las funciones de IA en los centros de fuegos y puestos de mando de brigada/división, donde existen mejores condiciones de conectividad y seguridad de la información; mientras que las unidades desplegadas en el terreno continúan ejecutando la entrega de fuegos y la evaluación de daños (BDA, Battle Damage Assessment) con sistemas de comunicación tácticos convencionales conectados de forma segura a estos nodos centrales.

Medidas de seguridad y control para mitigar los riesgos cibernéticos

La integración de la IA al PSPB, como se observó, implica varios riesgos, y el Ejército como institución es consciente de las medidas que se deben tomar en estos casos; así “la sección de guerra electrónica coordina, integra y evalúa ataques físicos, ataques electrónicos, ataques a redes informáticas y explotación de redes informáticas, para operar [...] degradar, destruir y neutralizar capacidades del enemigo” (Ejército Nacional de Colombia, 2016, pp. 3-4).

De esta manera, la gestión de la información operacional constituye un reto integral para el personal involucrado en el proceso. Este desafío no solo radica en la responsabilidad de

determinar qué objetivo debe ser tratado y en qué momento puede considerarse neutralizado, sino también en garantizar la conservación y protección de la información frente a un posible acceso del adversario.

En este sentido, si bien la implementación de protocolos de seguridad redundantes no garantiza la invulnerabilidad absoluta de los sistemas, sí reduce de forma significativa su superficie de ataque y nivel de exposición. Con el fin de fortalecer estas salvaguardas, se proponen las siguientes medidas:

Medidas de seguridad en la recolección y procesamiento de datos

- Arquitectura de datos federada: implementación de sistemas de análisis continuo multidominio que integren tierra, mar, aire, ciberespacio y espacio, siguiendo el modelo descrito por King (2024), en el cual “el objetivo es crear un sistema de *targeting* multidominio único que una los esfuerzos de todos los cinco dominios” (p. 5).
- Cifrado avanzado en almacenamiento y transmisión de información.
- Redes militares cerradas (*air-gapped*) para evitar filtraciones de datos a sistemas externos.
- Análisis forense de datos para detectar intentos de manipulación o falsificación de información.

Medidas de seguridad en la inteligencia artificial y algoritmos

- Desarrollo de IA explicable (XAI) para evitar decisiones de “caja negra”: desarrollo de sistemas que permitan “interpretación contextualmente apropiada de *insights* generados por IA”, como recomienda Baxter (2024, p. 6), al asegurar que “la colaboración no se vea meramente como integración de tecnologías, sino como una asociación sinérgica donde el juicio humano e *insights* de ia se complementen mutuamente” (p. 6).
- Validación cruzada de fuentes: implementación de protocolos que eviten el sesgo algorítmico, conocido como sesgo de automatización, mediante

verificación independiente de múltiples sistemas de IA, siguiendo las lecciones del caso Lavender en el cual se ejecutaron ataques contra objetivos identificados erróneamente mediante su clasificación basada únicamente en números telefónicos, sin una verificación humana suficiente.

- Mecanismos de validación humana en todas las decisiones críticas: la implementación de controles de supervisión humana constituye el elemento central de cualquier sistema de *targeting* asistido por IA, estableciendo múltiples niveles de verificación antes de autorizar acciones cinéticas. Estos mecanismos deben garantizar lo que el Australian Department of Defence (2020) define como “control humano significativo”, al requerir que “un operador humano tome una decisión informada y deliberada sobre el compromiso de cada objetivo específico” (p. 15).

El IEEE SA Research Group on Issues of Autonomy and AI in Defense Systems (2024) enfatiza que “un sistema no puede ser aceptable para uso a menos que comandantes y operadores tengan suficiente comprensión contextual de cómo funciona y qué puede y no puede hacer” (p. 19), y establece que el control humano debe mantenerse a través de todo el ciclo de vida del sistema. Los protocolos de validación incluyen: verificación de identidad de blancos mediante múltiples sensores independientes, confirmación de legalidad del objetivo bajo el derecho internacional humanitario, evaluación de proporcionalidad del daño colateral previsto versus ventaja militar esperada, y autorización escalonada por niveles de comando según la criticidad del objetivo.

El marco IEEE determina que los humanos deben mantener *in-the-loop* u *on-the-loop* control dependiendo del nivel de riesgo, en el que “ningún sistema autónomo debe tener la capacidad de seleccionar y atacar objetivos sin control humano apropiado y autorización explícita” (IEEE SA Research Group on Issues of Autonomy and AI in Defense Systems, 2024, p. 24), lo cual requiere que cada decisión letal mantenga supervisión humana activa durante todo el ciclo de *targeting*.

Simulaciones y pruebas de estrés periódicas para detectar sesgos y errores en el modelo

Medidas contra ciberataques y manipulación de datos

- Sistemas de detección de intrusiones (IDS) y prevención de ataques (IPS).
- Uso de IA adversarial para identificar intentos de engaño en los datos.
- Monitoreo en tiempo real de ciberamenazas y redes de defensa activa.

Medidas de seguridad en la ejecución operacional

- Validación múltiple de órdenes antes de la ejecución de ataques con ia.
- Autenticación multifactor (MFA) para operadores autorizados en el sistema.
- Desarrollo de auditorías posoperacionales para verificar el correcto uso de la IA en combate.

Al considerar estas salvaguardas, la integración de la IA en el PSPB cumple con el objetivo de evaluar la propuesta del modelo no solo desde sus ventajas y aportes operacionales, sino mediante la identificación de sus debilidades y la formulación de medidas de mitigación frente a los desafíos diagnosticados. En consonancia con el marco teórico de esta investigación, las transformaciones de paradigma en el ámbito militar no se limitan a la adaptación de “estructuras, procedimientos y tácticas militares, sino también la ideología y prácticas del colectivo castrense, que debe sustituir las viejas costumbres por nuevas técnicas, métodos y estilos de mando y control de las operaciones” (Colom-Piella, 2014, p. 29). En consecuencia, resulta imperativo diseñar estrategias institucionales que faciliten la adaptación doctrinaria y cultural ante este nuevo fenómeno tecnológico.

Análisis y discusión

Los hallazgos de esta investigación confirman que la integración de la IA al PSPB se inscribe de manera plena en la transición hacia el digital *targeting* descrito por King. En dicho enfoque, la verdadera revolución militar contemporánea no radica en la simple proliferación de sistemas autónomos letales, sino en la capacidad de procesar macrodatos (*big data*) para identificar y seleccionar objetivos con mayor celeridad y precisión. Al contrastar el esquema propuesto con desarrollos como el Project Maven (EE. UU.) y el Maven Smart System de la OTAN, se observa que las cinco fases diseñadas (captura, análisis predictivo, priorización, ejecución y evaluación) replican, de forma adaptada, los pilares de fusión multisensor, apoyo a la decisión y retroalimentación continua, bajo el imperativo doctrinal del Ejército Nacional de Colombia: preservar el control humano significativo en cada etapa.

No obstante, a diferencia de las capacidades desplegadas por las potencias tecnológicas, el contexto colombiano introduce tensiones estructurales entre la ambición técnica y las realidades presupuestales e infraestructurales. La formulación de técnicas avanzadas —como el cifrado poscuántico, la visión por computador de alta resolución o las simulaciones multiactor— exige reconocer que su adopción será progresiva y estará supeditada a la modernización de las redes de Mando y Control (C2), así como a la consolidación de una cultura institucional de ciberseguridad y ética operacional.

Como consecuencia, este trabajo no debe interpretarse como una hoja de ruta de implementación inmediata, sino como un marco de referencia estratégico destinado a orientar las decisiones de inversión, el desarrollo doctrinal y la capacitación de la fuerza.

En este sentido, la arquitectura de cinco fases evidencia una viabilidad diferenciada. Las etapas iniciales de captura, depuración y análisis de datos presentan las mayores probabilidades de adopción en el corto plazo, toda vez que pueden centralizarse

en los puestos de mando y nodos de inteligencia existentes. Por el contrario, la fusión multisensorial en tiempo real, la ejecución altamente automatizada y los mecanismos de aprendizaje continuo demandan requerimientos técnicos y financieros considerablemente más exigentes.

Por último, el análisis ratifica que el factor crítico no reside en el grado de automatización en sí mismo, sino en su gobernanza. La evidencia analizada y la lógica intrínseca del PSPB demuestran que la IA posee el potencial de potenciar la velocidad y la precisión operativa, pero también de amplificar errores si actúa sobre insumos alterados, sesgados o no verificados. Por lo tanto, cualquier proceso de integración debe erigirse sobre esquemas de validación humana, trazabilidad de las decisiones, auditoría posterior y salvaguardas cibernéticas robustas, que garanticen en todo momento la legitimidad operacional, ética y jurídica de la fuerza.

Conclusiones

Como producto de esta investigación, y en cumplimiento de los objetivos establecidos como hoja de ruta, se obtuvieron los siguientes resultados:

En cuanto al primer objetivo, orientado a identificar las etapas del PSPB susceptibles de integrar herramientas de IA, se demostró mediante esquemas los puntos clave en los cuales su uso optimiza la dinámica operativa. Los hallazgos confirman que esta modernización no reemplaza el control humano, sino que incrementa la eficiencia en el procesamiento de datos, la asignación de fuegos y la reducción de daños colaterales.

En consecuencia, el PSPB asistido por IA se consolida como una herramienta estratégica para la toma de decisiones militares en escenarios donde la rapidez, la proporcionalidad y la legitimidad de la fuerza determinan el éxito de la operación.

Respecto al segundo objetivo, centrado en determinar las vulnerabilidades asociadas a esta integración, se analizaron tres grupos principales de riesgos a partir de la revisión bibliográfica y de casos de estudio contemporáneos. Se reconoce que

el empleo de la IA en operaciones militares conlleva desafíos éticos y dilemas morales en ambientes de alta incertidumbre que superan las capacidades algorítmicas actuales. Asimismo, emergen riesgos operativos, como la eventual sobredependencia tecnológica, la cual podría degradar el criterio y las capacidades de decisión de los comandantes en el campo de combate.

Frente al tercer objetivo, enfocado en el diseño de un modelo estructural de integración de la IA en el PSPB, se identificaron cinco fases clave en las cuales su adopción genera mayor eficacia, en consonancia con las mejores prácticas de otras fuerzas armadas internacionales. No obstante, el modelo ratificó la conveniencia de preservar el factor humano (*human-in-the-loop*) en la toma de decisiones de alto impacto, manteniendo esquemas de supervisión directa en las fases críticas del proceso.

En relación con el cuarto objetivo, destinado a formular medidas de seguridad y control para mitigar los riesgos cibernéticos, se estructuraron cuatro ejes de acción derivados de las vulnerabilidades diagnosticadas. Al tratarse de una tecnología en constante evolución que revoluciona el arte militar, resulta imperativo adoptar modelos analíticos que no solo aprovechen sus ventajas operacionales, sino que contemplen salvaguardas estrictas en todos sus marcos de actuación, asegurando que la herramienta permanezca supeditada al juicio y control humano.

Como reflexión final, la investigación evidencia que la integración de la IA en el PSPB solo será sostenible si se alinea de manera realista con los ciclos de inversión, la renovación de medios y el desarrollo de la infraestructura crítica del país. Las propuestas avanzadas —tales como el cifrado de alto nivel, la fusión multisensor en tiempo real y la analítica distribuida— deben priorizarse bajo criterios de costo-efectividad, impacto operacional y sostenibilidad logística, y evitar esquemas que presupongan capacidades de conectividad, ancho de banda o plataformas que aún no se encuentran desplegadas de forma generalizada en el Ejército Nacional de Colombia.

Referencias

- Abraham, Y. (2024, 23 de noviembre). Lavender: La máquina de IA que dirige los bombardeos de Israel en Gaza. *Cuadernos de Beauchef*, 8(1), 135-154. <https://revistasdex.uchile.cl/index.php/cdb/article/view/15231>
- Australian Department of Defence. (2020). *A method for ethical AI in defence*. Defence Science and Technology Group, DSTG-TR-3786. Aerospace Division.
- Avendaño-Parra, P. A. (2024). ¿Cómo los ciberdelincuentes usan tecnologías avanzadas en IA para crear Deepfakes y Deepvoices para suplantar las identidades y estafar? *El Tiempo*. <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-los-ciberdelincuentes-usan-tecnologias-avanzadas-en-ia-para-crear-deepfakes-y-deepvoices-para-suplantar-las-identidades-y-estafar-3393101>
- Barba-Kay, A. (2024). There is no ethical automation: Stanislav Petrov's ordeal by protocol. *Journal of Military Ethics*, 23(3-4), 277-288. <https://doi.org/10.1080/15027570.2024.2434352>
- Baxter, C. A. (2024, 1.º de marzo). Enhancing tactical level *targeting* with Artificial Intelligence. *Field Artillery Journal*, (1). <https://www.lineofdeparture.army.mil/Journals/Field-Artillery/FA-2024-Issue-1/Enhancing-Tactical-Level-Targeting/>
- Blanquicet, J. A. (2025). Nueve helicópteros UH1-N del Ejército salen de circulación: Quedan 99 aeronaves funcionales. *El Tiempo*. <https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/nueve-helicopteros-uh1-n-del-ejercito-salen-de-circulacion-quedan-99-aeronaves-funcionales-3422708>
- Bossio-Ballesteros, V. E. (2023). La inteligencia artificial en el ámbito militar: Una herramienta relevante y útil. *Revista Seguridad y Poder Terrestre*, 2(3), 53-61. <https://doi.org/10.56221/spt.v2i3.33>
- Boulanin, V., Davison, N., Goussac, N. & Peldán-Carlsson, M. (2020). *Limits on autonomy in weapon systems; Identifying practical elements of human control*. Stockholm International Peace Research Institute (Sipri) and International Committee of the Red Cross (ICRC). <https://www.sipri.org/publications/2020/other-publications/limits-autonomy-weapon-systems>
- Brito-Acuña, G. (2023). Aeronautic maturity cybersecurity: A framework. *DYNA*, 90(227), 24-34. <https://doi.org/10.15446/dyna.v90n227.107420>
- Clausewitz, C. von. (1999). *De la guerra* (M.ª J. Vilar, trad.). Ediciones Ejército. (Obra original publicada en 1832).
- Colom-Piella, G. (2014). El desarrollo conceptual de la revolución en los asuntos militares. *Revista Científica General José María Córdova*, 12(14), 19-34. <https://www.redalyc.org/pdf/4762/476247222002.pdf>
- Congressional Research Service. (2020). *Artificial Intelligence and national security* (Report number R45178). <https://crsreports.congress.gov/product/pdf/R/R45178>
- Corvalán, J. G. (2018). Inteligencia artificial: Retos, desafíos y oportunidades - Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la justicia. *Revista de Investigações Constitucionais*, 5(1), 295-316. <https://doi.org/10.5380/rinc.v5i1.55334>
- Cuartero-Lorenzo, F. (2023). Irrupción de la inteligencia artificial en el Ministerio de Defensa: Primeros casos de uso. En *Actividades investigadoras enmarcadas en los trabajos fin de máster 2023-2024* (pp. 35-46). Ministerio de Defensa de España. <https://publicaciones.defensa.gob.es/media/downloadable/files/links/a/c/actividades-investigadoras-enmarcadas-en-los-trabajos-fin-de-master-2023-2024.pdf>
- Defense Update. (2025, 18 de abril). *NATO AI modernization: Palantir's Maven Smart System*. https://defense-update.com/20250418_palantir-mss-nato.html
- Díaz-Figueroa, J. E., González-Villamil, É. E., Pérez-Oliva, J. A., Medina-Echavarría, R. A. & Rangel-Ospino, Á. H. (2020). Complemento al simulador de vuelo del helicóptero Bell 206, para las prácticas en la formación de pilotos de la ESAVI. *Revista EIA*, 17(34), 113-125. <https://doi.org/10.24050/reia.v17i34.1327>
- Echeverría, G. (2023). *Amenazas cibernéticas: Tipos, riesgos y estrategias de protección para empresas y usuarios*. <https://www.tecnologia-informatica.com/amenazas-ciberneticas/>
- Ejército Nacional de Colombia. (2016). *Manual de operaciones de inteligencia militar*. Jefatura de Educación y Doctrina, Comando de Educación y Doctrina.
- Ejército Nacional de Colombia. (2019a). *Manual de técnicas del Ejército MTE 3-60*. Ejército Nacional de Colombia.

- Ejército Nacional de Colombia. (2019b). *MTE 3-60: Proceso de selección y priorización de blancos* [manual restringido]. Ejército Nacional de Colombia.
- Fernández-Altamirano, A. E. & Vela-Meléndez, L. (2021). *Los paradigmas y las metodologías usadas en el proceso de investigación: Una breve revisión*. Universidad César Vallejo (Perú) y Universidad Nacional Pedro Ruiz Gallo (Perú). <https://rua.ua.es/dspace/handle/10045/119978>
- Fonseca-Ortiz, T. L. (2022). El ciberespacio: Nuevo dominio de la guerra y el crimen. *Revista Ciberespacio, Tecnología e Innovación*, 1(1), 1-3. <https://doi.org/10.25062/2955-0270.4792>
- García Torres, J. I. (2024). *Tendencias y perspectivas futuras de la IA en el ámbito militar* (capítulo de libro de Maestría en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra “General Rafael Reyes Prieto”).
- Gómez de Ágreda, Á. (2024). Más que robots asesinos. Inteligencia artificial en la toma de decisiones en la guerra. *Escenarios Actuales*, 29(2), 11-21. Centro de Estudios e Investigaciones Militares.
- González, R. J. (2023). La militarización de las grandes empresas tecnológicas. El auge de la industria de defensa de Silicon Valley. En Consejo Latinoamericano de Ciencias Sociales (Clacso) y Transnational Institute (TNI), *Poder digital. Estado del poder 2023* (pp. 77-106). <https://www.clacso.org/wp-content/uploads/2023/11/Estado-del-poder.pdf>
- Gray, C. H. (2025). *AI, sacred violence, and war—The case of Gaza*. Springer. <https://doi.org/10.1007/978-3-031-81501-0>
- Greipl, A., Davison, N. & Hinds, G. (2024). *Expert consultation report. Artificial Intelligence and related technologies in military decision-making on the use of force in armed conflicts*. International Committee of the Red Cross (ICRC) and Geneva Academy. <https://geneva-academy.ch/wp-content/uploads/2025/09/Artificial-Intelligence-And-Related-Technologies-In-Military-Decision-Making.pdf>
- IEEE SA Research Group on Issues of Autonomy and AI in Defense Systems. (2024). *A framework for human decision-making through the lifecycle of autonomous and intelligent systems in defense applications* [White paper]. IEEE Standards Association. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10707139>
- King, A. (2024). Digital targeting: Artificial Intelligence, data, and military intelligence. *Journal of Global Security Studies*, 9(2), ogae009. <https://doi.org/10.1093/jogss/ogae009>
- Jomini, A.-H. (1992). *The art of war* (J. W. Bell, Trad.). Greenhill Books. (Obra original publicada en 1838).
- Lombardo, O. M. (2024). *La renovación de Bell con soluciones eficientes y modernas: Bell 505, 412 EPI y 407 GXi/M*.
- Moliner, J. A. (2017). Desafíos éticos en el uso militar de la inteligencia artificial. En *La inteligencia artificial aplicada a la defensa* (pp. 127-149). Instituto Español de Estudios Estratégicos. <https://dialnet.unirioja.es/servlet/articulo?codigo=6896755>
- NATO Communications and Information Agency. (2025, 14 de abril). *NATO acquires AI-enabled warfighting system*. North Atlantic Treaty Organization (NATO). <https://www.ncia.nato.int/newsroom/news/nato-acquires-ai-enabled-warfighting-system>
- Nitzl, C., Cyran, D., Krstanovic, S. & Borghoff, U. (2024). *El impacto de la IA en el análisis de inteligencia militar*. SciSimple. <https://scisimple.com/es/articles/2025-04-17-el-impacto-de-la-ia-en-el-analisis-de-inteligencia-militar--a9v0255>
- Organización de Aviación Civil Internacional (OACI). (2020). *Webinario sobre la implementación de ciberseguridad de la aviación OACI/Canso/Airbus*.
- Pérez-Benítez, J. I. (2019). Ciberdefensa aeroespacial. *Revista Científica Seguridad, Ciencia & Defensa*, 5(5), 86-94. <http://revista.unade.edu.do/index.php/rscd/article/view/65/80>
- Rivas, S. (2025). El Ejército de Colombia y el reemplazo de sus UH-1N y Huey 2, una necesidad urgente. *Pucará Defensa*. <https://n9.cl/b3i62>
- Salamanca-Rodríguez, E. A., Cabrera-Ortiz, F. & Reith, S. (eds.). (2022). *Estrategia de Seguridad de la Infraestructura Crítica Nacional 2022-2032*. Escuela Superior de Guerra “General Rafael Reyes Prieto”. <https://esdeglibros.edu.co/index.php/editorial/catalog/view/163/160/2003>
- Secretaría General Técnica del Ceseden. (2020). *Memoria 2019*. Centro Superior de Estudios de la Defensa Nacional [informe]. Ministerio de Defensa.
- Sobrevilla, J. (2026, 3 de agosto). La inteligencia artificial en el campo de batalla. *Entre Semana*. <https://entresemana.mx/otredades-la-inteligencia-artificial-en-el-campo-de-batalla/>

- Tovar, G. A. & Figueroa, E. (2021). El helicóptero como factor decisivo para la movilidad táctica: El caso colombiano (1997-2012). *Revista Científica General José María Córdova*, 19(34). <https://doi.org/10.21830/19006586.750>
- Universidad Internacional de Valencia (viu). (2025). *TIC en Colombia: Cómo impulsan el futuro y desarrollo del país*. <https://www.universidadviu.com/co/actualidad/nuestros-expertos/tic-en-colombia-como-impulsan-el-futuro-y-desarrollo-del-pais>
- Zapata-Madrigal, G. D. & García-Sierra, R. (2021). CyberDrone: Una plataforma de ciberseguridad para detección de ataques a drones. *Ingeniería y Desarrollo*, 39(1). <https://doi.org/10.14482/inde.39.1.621.389>