

Capítulo 2

La inteligencia artificial en las operaciones militares: un enfoque en los dominios aéreo, espacial y ciberespacial*

DOI: <https://doi.org/10.25062/9786287818507.02>

Fabio Baquero Valdés

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente capítulo es el resultado de un proceso de investigación basado en la revisión y el análisis documental, y ofrece una reflexión sobre la aplicación de la inteligencia artificial (IA) en las operaciones militares. Se describe el estado actual de la IA en este contexto y se analizan los desafíos más complejos y multifacéticos que surgen al aplicarla en ambientes denominados multidominio. Además, se examinan las operaciones militares en los ámbitos aéreo, espacial y ciberespacial con el uso de IA. Finalmente, se presentan los principales hallazgos derivados de la investigación.

Palabras clave: Desafío, dominio aéreo, dominio espacial, dominio ciberespacial, inteligencia artificial, operaciones militares.

* Capítulo resultado del proyecto de investigación *Desafíos futuros en los dominios aéreo, ciberespacial y espacial por la aplicación de la inteligencia artificial en la transición de la revolución industrial (5.0)*, desarrollado por el grupo de investigación Masa Crítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Este grupo está categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación y registrado bajo el código COL0123247. Los puntos de vista y los resultados presentados son responsabilidad de los autores y no necesariamente reflejan la posición de las instituciones participantes.

Fabio Baquero Valdés

Coronel (R) de la Fuerza Aeroespacial Colombiana. Magister en Educación, Universidad Santo Tomás de Aquino, Colombia. Especialista en Seguridad y Defensa Nacional y en Comando y Estado Mayor, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Administrador aeronáutico. Docente ocasional asociado, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Investigador junior reconocido por el Ministerio de Ciencia, Tecnología e Innovación. <https://orcid.org/0000-0002-5509-322X>
Contacto: fabio.baquero@esdeg.edu.co

Citación APA: Baquero Valdés, F. (2026). La inteligencia artificial en las operaciones militares: un enfoque en los dominios aéreo, espacial y ciberespacial. En F. Baquero-Valdés. (Ed.). *Desafíos futuros en los dominios aéreo, espacial y ciberespacial: IA y Revolución Industrial (5.0)* (pp. 43-70). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818507.02>

DESAFÍOS FUTUROS EN LOS DOMINIOS AÉREO, ESPACIAL Y CIBERESPACIAL: IA Y REVOLUCIÓN INDUSTRIAL (5.0)

ISBN impreso: 978-628-7818-49-1

ISBN digital: 978-628-7818-50-7

DOI: <https://doi.org/10.25062/9786287818507>

Colección Estrategia, Geopolítica y Cultura

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2026



Introducción

En las últimas décadas, la integración de la IA en las operaciones militares ha experimentado un crecimiento exponencial. La convergencia de avances tecnológicos, la creciente disponibilidad de grandes volúmenes de datos y el aumento de la capacidad de procesamiento han impulsado el desarrollo y la aplicación de sistemas de IA en diversos contextos militares.

La evolución de las operaciones militares ha llevado a la integración de los dominios, aéreo, espacial y ciberespacial. La incorporación de la IA en estos dominios ha transformado significativamente tanto las estrategias como las tácticas militares. Las operaciones realizadas en ambientes multidominio requieren la coordinación de diferentes frentes de batalla, especialmente en los ámbitos aéreo, espacial y ciberespacial. En este contexto, la IA desempeña un papel crucial al optimizar las capacidades de análisis de datos, la toma de decisiones y la ejecución de misiones.

La integración de la IA en entornos multidominio plantea desafíos que se agrupan en tres categorías: técnicos, éticos y legales, las cuales generan la necesidad crítica de mantener el control humano en las operaciones militares impulsadas por la IA (Raska, 2025, p. 1). En el plano técnico destacan la interoperabilidad de los sistemas, la robustez y la fiabilidad de los algoritmos, así como la gestión de grandes volúmenes de datos en tiempo real. Los desafíos éticos y legales se relacionan principalmente con la protección de la privacidad y el respeto a los derechos humanos. En particular, la autonomía de los sistemas de IA plantea importantes interrogantes éticos sobre la atribución de responsabilidades en caso de errores o fallos.

La IA se ha consolidado como una tecnología transformadora que mejora significativamente la capacidad operativa y estratégica en estos ámbitos, al facilitar el análisis de datos, apoyar la toma de decisiones y la ejecución de misiones. No obstante, con la integración de la IA, los dominios aéreo, espacial y Ciberespacial

ha desempeñado un papel central en la transformación de las estrategias y las tácticas militares.

Actualidad de la IA en las operaciones militares

El estado actual de la IA en las operaciones militares permite identificar su impacto en los dominios aéreo, espacial y ciberespacial. En el dominio aéreo, la IA es fundamental para el desarrollo de nuevos servicios ATM/U-space, dada la creciente demanda y complejidad del espacio aéreo. Entendido ATM/U-space como la convergencia fundamental entre la aviación tradicional y el futuro del espacio aéreo, marcando la transición de un modelo centrado en el humano hacia un ecosistema altamente automatizado y nativamente digital (Starburst, 2026). Así también lo relaciona (Vásquez Ruiz, 2024) cuando menciona que la IA ha dejado de ser una simple tecnología de apoyo para convertirse en el tejido conectivo de las operaciones militares multidominio, impactando de forma directa e interconectada en los dominios aéreo, espacial y ciberespacial.

En este sentido, "la IA desempeña un papel relevante en el ciberespacio gracias a su capacidad para procesar ingentes cantidades de datos y obtener resultados que fortalezcan la seguridad. Sin embargo, también puede ser utilizada para lanzar ataques" (Montes, 2023, p. 4). Asimismo, en el espacio ultraterrestre, la IA no solo está ganando relevancia como un ámbito operativo, sino también debido a las vulnerabilidades inherentes.

La obra *Artificial Intelligence and National Security*, de Greg Allen y Taniel Chan, destaca cómo la IA ha transformado a las fuerzas armadas, señalando que no solo ha revolucionado la recopilación de la información, sino también la toma de decisiones estratégicas (Allen, Greg & Chan, 2017). Este cambio se refleja en la adopción de sistemas autónomos y en la mejora de las capacidades de análisis de datos, lo que permite una toma de decisiones más rápida y precisa.

En su análisis *Artificial Intelligence and a Reconfiguration of Military Power*, (Annett et al., 2026) resaltan la importancia de la IA en la planificación y ejecución de las operaciones militares, subrayando que su integración progresiva trasciende la mera evolución tecnológica o automatización, toda vez que reconfigura la toma de decisiones, la aplicación de la fuerza y el juicio estratégico, operando como un pilar central en las políticas de defensa.

En el ámbito aéreo, la obra *Air Superiority 2030 Flight Plan*, del Departamento de la Fuerza Aérea de los Estados Unidos, ofrece una visión integral sobre la

incorporación de la IA en la superioridad aérea, abordando aspectos como la interoperabilidad de sistemas autónomos y la toma de decisiones asistida por la IA (United States Air Force, 2016).

En su informe *AI and International Stability*, (Horowitz & Scharre, 2021) exploran las implicaciones de la IA en las fuerzas militares, destacando cómo los sistemas autónomos aceleran el ritmo del combate transformando la dinámica en el campo de batalla, y abordan las consideraciones éticas, normativas y de control humano asociadas con estas tecnologías.

En cuanto al ámbito espacial, el informe *Autonomous Systems in the Battlespace: An Assessment of China's Evolving Military Doctrine*, de Elsa B. Kania (2018), resalta la creciente importancia de la IA en las estrategias espaciales, destacando cómo China está incorporando sistemas autónomos en sus doctrinas militares.

En relación con el ámbito de la ciberseguridad, (Huskaj, 2026) en el artículo *AI-Enabled Cyberspace Operations*, analiza cómo la IA es una herramienta eficaz para mitigar amenazas cibernéticas a 'velocidad de máquina', destacando la relevancia de los microservicios automatizados que ingieren telemetría de los sistemas de detección de intrusiones, correlacionan alertas y orquestan secuencias de respuesta rápida ante incidentes.

El estado actual de la IA en las operaciones militares refleja una transición significativa hacia la integración de sistemas autónomos y tecnologías avanzadas de análisis de datos. La literatura revisada destaca tanto las oportunidades como los desafíos asociados con este cambio, enfatizando la necesidad de considerar aspectos éticos, legales y estratégicos en el desarrollo y la aplicación de la IA en el ámbito militar.

La IA y las operaciones militares en el dominio aéreo

La aplicación de la IA en las operaciones militares realizadas en el dominio aéreo ha revolucionado la forma en que las fuerzas armadas planifican y ejecutan sus misiones. La integración de sistemas autónomos, algoritmos de aprendizaje automático y herramientas de análisis de datos ha permitido mejoras significativas en la superioridad aérea y la capacidad de respuesta estratégica.

En el dominio aéreo, la IA está transformando la ejecución de las operaciones militares. Los sistemas de IA integrados en aeronaves no tripuladas mejoran las capacidades de reconocimiento y vigilancia, lo que permite una toma de decisiones más rápida y precisa. Por ejemplo, los drones equipados con IA pueden

identificar objetivos enemigos y evaluar amenazas potenciales en tiempo real, proporcionando información valiosa a los comandantes militares.

En su obra *Algorithmic Warfare*, Layton (2018) sostiene que la conciencia situacional es la condición *sine qua non* de la victoria para los aviadores militares, la integración de máquinas inteligentes permitirá a las fuerzas 'sentir y percibir los patrones del campo de batalla de manera más fácil y rápida', facilitando decisiones de combate oportunas y aumentando significativamente la eficacia de las operaciones tácticas.

Según el informe *Air Superiority 2030 Flight Plan* de la United States Air Force (2016), del Departamento de la Fuerza Aérea de los Estados Unidos, en la próxima década, la IA desempeñará un papel fundamental en el mantenimiento y mejora de la superioridad aérea. El informe destaca la importancia de los sistemas autónomos en la vigilancia, la detección temprana de amenazas y la toma de decisiones rápida y precisa. Además, la implementación de tecnologías de aprendizaje automático se considera esencial para adaptarse a entornos cambiantes y amenazas imprevisibles (United States Air Force, 2016).

En su informe *Battlefield Singularity*, Kania (2017) profundiza en cómo la IA no se limita a la automatización de plataformas, sino que demuestra un tremendo potencial en el mando operativo, la planificación y el apoyo a las decisiones, allí mismo analiza el rápido avance de China en la incorporación de sistemas autónomos en sus operaciones. Este enfoque comprende el desarrollo de múltiples plataformas de vehículos aéreos no tripulados (VANT) y la *inteligentización* de sistemas de armas, dotándolos de la capacidad para percibir, analizar datos, tomar decisiones autónomas y adaptarse dinámicamente en tiempo real a situaciones complejas durante el vuelo.

La aplicación de la IA en el dominio aéreo también abarca la capacitación y simulación. Los sistemas de simulación avanzados, impulsados por algoritmos de aprendizaje automático, permiten entrenar a pilotos y tripulaciones de manera más efectiva, replicando escenarios realistas y ajustándose a las habilidades individuales (Allen, Greg & Chan, 2017).

Sin embargo, el uso de la IA en operaciones aéreas no está exento de desafíos. Aspectos éticos y legales, como la toma de decisiones autónoma y la responsabilidad de las acciones, plantean interrogantes que requieren una atención cuidadosa. Además, la interoperabilidad entre sistemas autónomos y tripulados es un área en desarrollo que debe abordarse para optimizar la efectividad de las operaciones aéreas integradas.

En resumen, la aplicación de la IA en las operaciones militares del dominio aéreo ha marcado un hito significativo en la evolución de las fuerzas armadas. Desde la mejora de la superioridad aérea hasta la planificación estratégica avanzada, la IA ha demostrado su capacidad para transformar la manera en que se llevan a cabo las operaciones aéreas. A pesar de los desafíos, el potencial para lograr una mayor eficiencia y capacidad operativa sugiere que la IA seguirá desempeñando un papel fundamental en el futuro del dominio aéreo militar.

La IA y las operaciones militares en el dominio espacial

Al integrarla a las operaciones militares del dominio espacial, la IA se ha convertido en un componente estratégico esencial para numerosas naciones. En este entorno crítico, la convergencia de la tecnología espacial con la IA ha impulsado avances significativos en la vigilancia, el control y la capacidad de respuesta.

En el dominio espacial, la IA se emplea para mejorar la navegación, la comunicación y la vigilancia satelital. Los sistemas de IA tienen la capacidad de analizar grandes volúmenes de datos recopilados por satélites, proporcionando información procesable que respalda las operaciones militares en tierra, mar y aire. Además, la IA desempeña un papel crucial en el desarrollo de tecnologías para la detección de objetos espaciales y la prevención de colisiones en órbita.

En su análisis *AI on the Edge of Space*, Huynh (2025) señala que la inteligencia artificial está transformando el dominio espacial, destacando que su integración —tanto en los sistemas terrestres como a bordo de los propios satélites— es esencial para acelerar la toma de decisiones, mejorar la eficiencia y supervivencia de las plataformas, y mantener el conocimiento del dominio en un entorno cada vez más disputado. En su obra *Autonomous Systems in the Battlespace: An Assessment of China's Evolving Military Doctrine*, Kania (2017) destaca la creciente importancia de la IA en las estrategias espaciales. China, en particular, ha logrado un avance significativo al integrar sistemas autónomos en sus operaciones espaciales, destacándose la implementación de satélites autónomos y sistemas de control. Estos avances podrían transformar las capacidades militares en el espacio, abarcando desde la recolección de información hasta la respuesta a amenazas.

En el dominio espacial, la interoperabilidad y adaptabilidad de los sistemas autónomos son factores esenciales. En este contexto, la obra *Air Superiority 2030 Flight Plan*, la United States Air Force (2016) del Departamento de la Fuerza Aérea de los Estados Unidos, destaca el papel de la IA en la protección de activos espaciales críticos mediante la gestión eficiente de constelaciones de satélites y la

toma de decisiones en tiempo real. La capacidad de anticipar y responder a amenazas en el espacio depende cada vez más de la IA.

En el ámbito de la conciencia situacional espacial, los análisis recientes de la industria destacan que la identificación de objetos, la predicción de trayectorias y la evasión de colisiones se benefician enormemente de los algoritmos de aprendizaje profundo y automático (Huynh, 2025).

Al examinar la seguridad en el dominio espacial, Enayati (2025) destaca la importancia de la cooperación internacional frente a la creciente competitividad y militarización de la órbita terrestre. La investigación subraya que emular e implementar marcos diplomáticos entre naciones es una medida clave para mitigar los riesgos derivados de las tecnologías espaciales de uso dual, reducir malentendidos y garantizar la rendición de cuentas y la seguridad en el espacio.

No obstante, la militarización del espacio y la aplicación de sistemas avanzados en este dominio también plantean desafíos significativos. En su obra sobre *astropolítica* y la escalada armamentística espacial, Enayati (2025) enfatiza la urgencia de implementar marcos diplomáticos y de control para mitigar los riesgos inherentes a las tecnologías de uso dual, reducir los malentendidos y garantizar tanto la certidumbre como la rendición de cuentas en las operaciones espaciales.

En resumen, la aplicación de la IA en las operaciones militares del dominio espacial está transformando la manera en que se desarrollan las actividades en el espacio. Desde la vigilancia hasta la gestión de activos, la IA ofrece una ventaja estratégica crucial. Sin embargo, la comunidad internacional debe abordar, de manera proactiva, los desafíos éticos y legales asociados, a fin de garantizar un desarrollo responsable y sostenible en este ámbito estratégico.

La IA y las operaciones militares en el dominio ciberespacial

En el dominio ciberespacial, la IA desempeña un papel fundamental en la defensa contra amenazas cibernéticas. Los sistemas de IA son capaces de detectar y mitigar ataques cibernéticos de manera proactiva, identificando patrones anómalos y respondiendo en tiempo real, a fin de proteger las redes militares y los sistemas de información.

Al respecto, Huskaj (2026) argumenta que la IA proporciona una ventaja decisiva en el ciberespacio al acelerar el ritmo operativo y expandir significativamente el alcance de las misiones defensivas. Frente a una interconexión global crítica, la implementación de sistemas de aprendizaje por refuerzo permite a los defensores operar a «velocidad de máquina» para fortalecer las redes, pre calcular secuencias

de mitigación, contener anomalías y adaptarse rápidamente a las tácticas del atacante, transformando la manera en que se salvaguardan las infraestructuras.

En su informe *Artificial Intelligence and National Security*, Allen y Chan (2017) destacan la capacidad de la IA para detectar y mitigar amenazas cibernéticas. A través de algoritmos de aprendizaje automático integrados en la defensa de redes, los sistemas logran analizar grandes flujos de información para detectar desviaciones de la actividad normal e identificar comportamientos anómalos, permitiendo responder automáticamente ante ataques previamente desconocidos en un entorno en constante evolución (Allen, Gregory C. et al., 2018).

La autonomía de los sistemas de defensa cibernética se ha vuelto esencial para responder de manera inmediata a los ataques. En su obra *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Brundage et al. (2018) destacan la importancia de los sistemas autónomos capaces de adaptarse y contraatacar en tiempo real, lo que reduce la ventana de exposición a las amenazas cibernéticas.

La colaboración entre los sectores público y privado es crucial para combatir las amenazas cibernéticas. En su informe *Artificial Intelligence and National Security*, Allen, Greg & Chan (2017) destacan que conciliar los intereses comerciales y de seguridad nacional es un gran desafío, pero subrayan que la cooperación histórica y actual con la industria tecnológica es la que permite al gobierno mantener su liderazgo en ciberseguridad, recomendando destinar mayores recursos a promover la colaboración directa entre la comunidad de defensa y la industria comercial de IA.

La aplicación de la IA en la seguridad nacional y la ciberdefensa no se limita únicamente a las grandes potencias mundiales. En su análisis *Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados*, (Romero, 2020) destaca que, aunque el camino es largo, países latinoamericanos como Brasil, Argentina, Perú y Colombia están buscando incorporar tecnologías basadas en IA para desarrollar estrategias competitivas clave dentro de un ambiente digital y militar dominado por sistemas computacionales.

Sin embargo, el desarrollo y la implementación de la IA en operaciones ciberespaciales también generan profundas preocupaciones éticas y legales. De acuerdo con Pouw & Pijpers (2025) la velocidad y la escala tecnológica amenazan con difuminar el control humano, por lo que la transparencia frente a la capacidad de los sistemas (la "caja negra") y la clara atribución de responsabilidades en la toma de decisiones autónomas son aspectos críticos que deben ser abordados cuidadosamente bajo el derecho internacional.

La constante evolución de las amenazas cibernéticas hace que la adaptabilidad de los sistemas de IA sea crucial. En su investigación Huskaj (2026) destaca que la inteligencia artificial impulsará una 'carrera co-evolutiva' donde la ofensiva y la defensa se adaptarán continuamente a las innovaciones del oponente, lo que exige que los sistemas de defensa se actualicen constantemente para contrarrestar nuevas tácticas, haciendo que las inversiones en adaptabilidad y capacidad de aprendizaje sean más decisivas que los saltos tecnológicos aislados

En resumen, la IA desempeña un papel central en la protección y el fortalecimiento de las operaciones militares llevadas a cabo en el ciberespacio. Desde la detección temprana de amenazas hasta la respuesta automática, su implementación ha demostrado ser esencial para abordar las complejidades del ciberespacio. Sin embargo, es imperativo abordar las cuestiones éticas y legales para garantizar un uso responsable y efectivo de estas tecnologías en las operaciones militares ciberespaciales.

Cuadros comparativos: aplicaciones clave de la IA, desafíos éticos y legales, y colaboración internacional

La implementación de la IA en las operaciones militares de los dominios aéreo, espacial y ciberespacial presenta tanto similitudes como diferencias significativas. A continuación, se presentan tablas comparativas que permiten visualizar estos aspectos clave, destacando las convergencias y divergencias en la aplicación de la IA en cada uno de estos dominios.

Tabla 1. Comparación 1: Aplicaciones clave de la IA

Dominio	Aplicación de la IA
Aéreo	<ul style="list-style-type: none">• Sistemas autónomos para la vigilancia y detección temprana.• Mejora de la toma de decisiones estratégicas.• Simulación y entrenamiento avanzado de pilotos.
Espacial	<ul style="list-style-type: none">• Satélites autónomos para la recolección de datos.• Gestión eficiente de las constelaciones de satélites.• Predicción y prevención de colisiones en el espacio.
Ciberespacial	<ul style="list-style-type: none">• Detección y mitigación de amenazas cibernéticas.• Respuesta automática y en tiempo real a ataques.• Colaboración público-privada en defensa cibernética.

Fuente. Elaboración propia.

El cuadro detalla las aplicaciones clave de la IA en cada dominio. En el ámbito aéreo, se destaca la vigilancia y la toma de decisiones estratégicas, mientras que,

en el dominio espacial, se resalta la gestión de satélites autónomos y la prevención de colisiones. En el ciberespacio, la detección y respuesta automática a amenazas cibernéticas son fundamentales.

Tabla 2. Comparación 2: Desafíos éticos y legales asociados

Dominio	Desafíos
Aéreo	<ul style="list-style-type: none"> • Responsabilidad en la toma de decisiones autónomas. • Ética en el uso de drones y sistemas autónomos. • Privacidad en la vigilancia aérea.
Espacial	<ul style="list-style-type: none"> • Normas éticas en el uso de sistemas autónomos. • Colaboración internacional para la ciberseguridad en el espacio. • Protección de la privacidad en la observación espacial.
Ciberespacial	<ul style="list-style-type: none"> • Transparencia en las operaciones cibernéticas. • Protección de datos y privacidad en la defensa cibernética. • Responsabilidad ante ataques cibernéticos automatizados.

Fuente. Elaboración propia.

Este cuadro destaca los desafíos éticos y legales comunes en los dominios aéreo, espacial y ciberespacial. La responsabilidad en la toma de decisiones autónomas, la ética en el uso de tecnologías y la protección de la privacidad son preocupaciones compartidas.

Tabla 3. Comparación 3: Colaboración internacional

Dominio	Colaboración internacional en la IA militar
Aéreo	<ul style="list-style-type: none"> • Intercambio de tecnologías entre naciones aliadas. • Establecimiento de normas para el uso ético de la IA. • Desarrollo conjunto de sistemas interoperables.
Espacial	<ul style="list-style-type: none"> • Colaboración en la gestión de las constelaciones satelitales. • Acuerdos para prevenir la militarización del espacio. • Desarrollo conjunto de sistemas autónomos espaciales.
Ciberespacial	<ul style="list-style-type: none"> • Compartir información sobre amenazas cibernéticas. • Establecimiento de normas internacionales para la ciberseguridad. • Cooperación internacional en la respuesta a ataques cibernéticos.

Fuente. Elaboración propia.

El cuadro destaca la importancia de la colaboración internacional en la implementación de la IA en las operaciones militares. Esta colaboración, que abarca desde el intercambio tecnológico hasta la respuesta coordinada a amenazas, se revela indispensable en los tres dominios. En resumen, estos cuadros comparativos proporcionan una visión general de las similitudes y diferencias clave en la

aplicación de la IA en las operaciones militares de los dominios aéreo, espacial y ciberespacial. Cabe destacar que los desafíos éticos y la necesidad de colaboración internacional son temas recurrentes en estos ámbitos estratégicos.

Desafíos en ambientes multidominio por la aplicación de la IA

La creciente aplicación de la IA en los ámbitos militar, espacial y ciberespacial ha dado lugar a una serie de desafíos complejos y multifacéticos. En este acápite, se analizan los retos derivados de la integración de la IA en entornos multidominio, presentando una clasificación clara de estos mediante cuadros comparativos.

Los desafíos técnicos son aquellos aspectos relacionados con el desarrollo, la implementación y la operación de sistemas de IA en ambientes multidominio. Estos incluyen la interoperabilidad de los sistemas, la robustez y fiabilidad de los algoritmos de IA, así como la gestión de grandes volúmenes de datos en tiempo real (Horowitz & Scharre, 2021, p. 7). Además, la falta de estándares comunes y la rápida evolución de la tecnología pueden dificultar la integración efectiva de la IA en entornos multidominio.

Los desafíos éticos y legales emergen de las implicaciones de la IA en áreas críticas como la privacidad, los derechos humanos y la asignación de responsabilidades. La autonomía de los sistemas de IA plantea interrogantes éticos sobre quién debe asumir la responsabilidad en caso de errores o malentendidos. Además, la recopilación masiva de datos para el entrenamiento de los algoritmos de IA suscita inquietudes sobre la privacidad y la protección de los datos personales (Raska, 2025).

Los desafíos de seguridad y ciberseguridad son críticos en entornos multidominio, donde los sistemas de IA se vuelven susceptibles a ciberataques y manipulación (Annett et al., 2026). La protección de la integridad y confidencialidad de los datos, así como la prevención de ataques dirigidos contra los sistemas de IA, son aspectos clave que deben ser considerados. Además, los desafíos de coordinación y cooperación destacan la necesidad de establecer mecanismos efectivos de colaboración entre diferentes actores y naciones. La falta de una coordinación adecuada puede dificultar la interoperabilidad de los sistemas y la respuesta conjunta a amenazas comunes.

Para analizar los desafíos que plantea la aplicación de la IA en ambientes multidominio, es útil clasificarlos en distintas categorías. A continuación, se propone una clasificación, seguida de un análisis detallado.

Desafíos técnicos

Los desafíos técnicos en la aplicación de la IA en ambientes multidominio son significativos y abarcan diversos aspectos, que van desde la interoperabilidad de los sistemas hasta la gestión de grandes volúmenes de datos.

La interoperabilidad entre sistemas de IA pertenecientes a diferentes dominios y fabricados por distintos proveedores es fundamental para garantizar la efectividad de las operaciones conjuntas. Sin embargo, este aspecto representa un desafío debido a la heterogeneidad de tecnologías y los estándares empleados en diversos contextos militares. La interoperabilidad entre sistemas impulsados por IA sigue siendo un desafío crítico. Frente a la necesidad de integrar tecnologías de distintos fabricantes, la *Estrategia de Inteligencia Artificial* para el Secretary of War (2026) exige la adopción obligatoria de Arquitecturas de Sistemas Abiertos Modulares (MOSA) y el cumplimiento de decretos de datos estandarizados, con el fin de exponer interfaces comunes que permitan la integración ágil de componentes de terceros sin depender de un único contratista principal.

A partir de Zhang et al. (2022) quien destaca que la protección de la propia inteligencia artificial es un área de investigación altamente activa, la robustez y fiabilidad de los algoritmos de IA son aspectos críticos, especialmente en entornos militares, donde la vida y la seguridad de las personas pueden depender de las decisiones tomadas por estos sistemas. La capacidad de los algoritmos para adaptarse a condiciones cambiantes y operar de manera confiable en entornos adversos es fundamental para garantizar su utilidad y efectividad en aplicaciones militares.

En entornos multidominio, la gestión de grandes volúmenes de datos representa otro desafío técnico importante. La recopilación y el procesamiento de datos heterogéneos exigen sistemas sofisticados de almacenamiento y análisis. Además, la calidad y relevancia de los datos son aspectos críticos que deben ser abordados para garantizar la precisión y la eficacia de los sistemas de IA. En el contexto de las operaciones multidominio, Barragan (2019) señala que la gestión de grandes volúmenes de datos exige enfoques innovadores, como el diseño de procesos de extracción, transformación y carga (ETL) integrados en una «nube de combate» (*Combat Cloud*). Este enfoque estructural es fundamental para recopilar, almacenar y hacer fluir la información masiva desde los múltiples sensores hasta los sistemas de explotación, garantizando que el procesamiento se realice de manera eficiente, segura e interoperable.

Tabla 4. *Desafíos técnicos*

Desafíos	Descripción
Interoperabilidad	Dificultad para integrar sistemas de IA provenientes de diferentes dominios y fabricados por distintos proveedores.
Robustez y confiabilidad	Garantizar que los algoritmos de IA funcionen de manera confiable en entornos adversos.
Gestión de datos	Problemas para gestionar grandes volúmenes de datos y garantizar su calidad y relevancia.

Fuente. Elaboración propia.

Desafíos éticos y legales

La aplicación de la IA en ambientes multidominio plantea una serie de desafíos éticos y legales que deben abordarse para garantizar su uso responsable. Entre estos, destacan la responsabilidad, la privacidad y la protección de los datos. En particular, la atribución de responsabilidades adquiere especial relevancia en el contexto de los sistemas autónomos de IA. Determinar quién debe responder en caso de errores o malentendidos representa un reto ético y legal de gran complejidad. En el caso de los sistemas autónomos de IA, la atribución de responsabilidad plantea importantes preguntas éticas y legales que aún no han sido completamente resueltas. Advierte sobre el riesgo de impunidad y la enorme dificultad para determinar la responsabilidad criminal individual ante comportamientos autónomos perjudiciales, planteando que la solución jurídica a estos vacíos normativos podría requerir la implementación de esquemas de responsabilidad internacional objetiva (o estricta) a los Estados que despliegan dicha tecnología.

La privacidad y la protección de datos son aspectos fundamentales en la aplicación de la IA en ambientes multidominio. La recopilación y el procesamiento de grandes volúmenes de datos pueden generar preocupaciones sobre la privacidad y la seguridad de la información personal. Es esencial garantizar que los datos utilizados por los sistemas de IA sean gestionados de manera ética y conforme a las leyes y regulaciones de protección de datos.

La privacidad y la protección de datos son consideraciones críticas en el diseño e implementación de sistemas de IA. De acuerdo con Gomez de Agreda (2019) desde la misma concepción y diseño de las aplicaciones deben considerarse salvaguardas éticas y jurídicas; resulta fundamental establecer de manera integral el respeto por la privacidad de los datos, la preservación de la autonomía y el respeto a la dignidad humana para no vulnerar los derechos de las personas.

Tabla 5. *Desafíos éticos y legales*

Desafíos	Descripción
Responsabilidad	¿Quién asume la responsabilidad en caso de errores o malentendidos causados por sistemas de IA autónomos?
Privacidad y protección de datos	¿Cómo se protegen los datos personales empleados por los sistemas de IA en ambientes multidominio?

Fuente. Elaboración propia.

Desafíos de seguridad y ciberseguridad

La implementación de la IA en ambientes multidominio conlleva riesgos significativos para la seguridad y la ciberseguridad, ya que los sistemas de IA son susceptibles a ciberataques y manipulación.

La protección de la integridad y la confidencialidad de los datos es fundamental para garantizar la seguridad de los sistemas de IA y prevenir la manipulación de la información. Por lo tanto, es crucial implementar medidas de seguridad robustas para salvaguardarlos de las intrusiones y los ciberataques.

La protección de datos es una prioridad ineludible en la aplicación de la IA en entornos operacionales. Al respecto, Quiñones Sigala (2023) destaca que los sistemas de ciberdefensa apoyados por IA requieren y facilitan enfoques netamente proactivos; estas tecnologías mejoran sustancialmente la capacidad de proteger programas, datos y redes reservadas al analizar grandes volúmenes de información para identificar vulnerabilidades y reconocer comportamientos sospechosos mucho antes de que las amenazas logren comprometer la integridad del sistema.

La prevención de ataques cibernéticos es un aspecto crucial para garantizar la seguridad de los ambientes multidominio. Los sistemas de IA son susceptibles a diversas amenazas, que van desde intrusiones en redes hasta la manipulación de datos y sabotaje. Por lo tanto, es esencial implementar medidas de seguridad avanzadas para protegerlos de las amenazas cibernéticas.

Al respecto, Quiñones Sigala (2023) subraya que, para mitigar los riesgos frente a ataques maliciosos, las capacidades de ciberdefensa asistidas por IA deben actuar de forma «sinérgica y coordinada» con el resto de las organizaciones del Estado.

Tabla 6. *Desafíos de seguridad y ciberseguridad*

Desafíos	Descripción
Protección de datos	Garantizar la integridad y la confidencialidad de los datos utilizados por los sistemas de IA
Prevención de ataques	Proteger los sistemas de IA contra los ataques cibernéticos y la manipulación por parte de adversarios.

Fuente. Elaboración propia.

Desafíos de coordinación y cooperación

La coordinación y la cooperación son pilares fundamentales para el despliegue exitoso de la IA en ambientes multidominio, donde múltiples actores realizan operaciones conjuntas. La interoperabilidad es esencial, permite que los distintos sistemas de plataformas se comuniquen y compartan información de manera eficiente.

La interoperabilidad entre actores es un requisito clave para la efectividad de las operaciones conjuntas en ambientes multidominio. Requiere de una estandarización y coordinación efectiva de tecnologías y procesos. Las operaciones multidominio exigen una sincronización sin fisuras. “Las fuerzas del futuro deben operar vinculadas por una red unificada, coordinándose libremente y dejando atrás las rivalidades o barreras de comunicación tradicionales entre los servicios militares” (Cozad et al. 2023).

La colaboración internacional es otro aspecto clave en la aplicación de la IA en entornos multidominio. La cooperación entre países no solo facilita el intercambio de información y tecnología, sino que también favorece la coordinación de esfuerzos.

Tabla 7. Desafíos de coordinación y cooperación

Desafíos	Descripción
Interoperabilidad entre actores	Coordinación entre diversos actores, como fuerzas armadas, agencias gubernamentales y aliados internacionales.
Colaboración internacional	Cooperación entre países para abordar desafíos comunes en ambientes multidominio.

Fuente. Elaboración propia.

Aplicación de la IA en operaciones militares multidominio (aéreo, espacial y ciberespacial)

En la era moderna, la evolución de la guerra ha transformado las operaciones militares, pasando de un entorno tradicional a un ambiente Multidominio. Este cambio demanda la integración y coordinación de diferentes poderes en el campo de batalla, como el aéreo, el espacial y el ciberespacial.

La IA emerge como una tecnología transformadora, potenciando significativamente la capacidad operativa y estratégica al proporcionar herramientas avanzadas para el análisis de datos, la toma de decisiones y la ejecución de misiones, entre otros aspectos. Paralelamente, los dominios aéreo, espacial y ciberespacial han cobrado una importancia crítica, desempeñando un papel central en la transformación de las estrategias y las tácticas militares.

A continuación, se ofrece un análisis de estos conceptos y su interrelación, detallando cómo la IA aplicada a las operaciones multidominio mejora la flexibilidad, eficiencia y efectividad de las operaciones militares, además de su impacto en la superioridad aérea, la ciberseguridad y las operaciones espaciales.

Operaciones militares en ambientes multidominio

Las operaciones multidominio constituyen una estrategia integral que coordina y sincroniza esfuerzos en diversos dominios de combate, como el terrestre, marítimo, aéreo, espacial y ciberespacial. Esta sincronización táctica y estratégica permite, por ejemplo, que las defensas aéreas, las formaciones terrestres y los buques navales no necesiten una dirección vertical rígida, sino que puedan ingerir información del campo de batalla y coordinar una respuesta cruzada de forma mucho más ágil (Cozad et al., 2023). La inclusión de la IA en estos dominios facilita una toma de decisiones más rápida y precisa, optimizando los recursos y mejorando la capacidad de respuesta.

IA en el dominio aéreo

La superioridad aérea ha sido un objetivo crucial para las fuerzas militares y, la IA desempeña un papel fundamental en su consecución. La integración de sistemas autónomos y semiautónomos equipados con IA ha transformado la gestión del espacio aéreo, la logística y el mantenimiento de aeronaves, y la efectividad con la logística y el mantenimiento predictivo. Más allá de las misiones cinéticas, la IA transforma el soporte vital de las operaciones. En el mantenimiento de las aeronaves, se están implementando modelos de algoritmos de *Deep Learning* para realizar un mantenimiento predictivo sumamente preciso (Quiñones Sigala, 2023).

Dominio aéreo.

El dominio aéreo abarca las operaciones militares llevadas a cabo en el espacio aéreo, que involucran tanto aeronaves tripuladas como no tripuladas. En este contexto, la IA puede mejorar significativamente la eficiencia y efectividad de las operaciones mediante:

- Optimización de rutas: aplicación de algoritmos de aprendizaje automático para identificar las rutas de vuelo más seguras y eficientes.
- Mantenimiento predictivo: análisis de datos en tiempo real para predecir fallos en los equipos.
- Reconocimiento y vigilancia: uso de la IA para procesar grandes volúmenes de datos visuales y de radar, lo que facilita la detección de amenazas y objetivos.

Gestión del espacio aéreo.

La IA optimiza la gestión del espacio aéreo, crucial para las operaciones militares, mediante el análisis de datos del tráfico aéreo y condiciones meteorológicas con otros factores relevantes. Sus algoritmos previenen congestiones, redirigen vuelos para evitar colisiones y mejoran la eficiencia operativa.

Figura 1. Optimización de la gestión del espacio aéreo mediante la IA



Fuente. Yanuki (2017).

Detección y respuesta a amenazas.

La IA ha revolucionado la detección y la respuesta ante amenazas aéreas. Los sistemas basados en IA utilizan sensores avanzados y redes neuronales profundas para identificar y clasificar amenazas en tiempo real. Estos sistemas son capaces de diferenciar entre amenazas reales y falsas alarmas, lo que resulta en una respuesta más rápida y precisa.

Figura 2. Detección y clasificación de amenazas aéreas mediante IA



Nota. Imagen elaborada mediante *Imagined with IA*.

Apoyo logístico.

La IA también desempeña un papel crucial en el apoyo logístico, optimizando la eficiencia del mantenimiento y la gestión de recursos. Los sistemas de mantenimiento predictivo basados en IA analizan datos de sensores para predecir fallos en los equipos y planificar el mantenimiento preventivo, lo que reduce el tiempo de inactividad y aumenta la disponibilidad de las aeronaves.

IA en el dominio ciberespacial

Acorde con (Quiñones Sigala, 2023), el ciberespacio se entiende como el quinto dominio de las operaciones militares. La doctrina internacional ha superado la *concepción* de la seguridad ligada puramente a lo físico. La mayoría de las naciones del mundo ya cuentan con capacidades de ciberdefensa en el seno de sus Fuerzas Armadas, consolidando al ciberespacio como el quinto ámbito operativo junto a la tierra, el mar, el aire y el espacio.

Dominio ciberespacial.

El dominio ciberespacial, conformado por redes informáticas y sistemas de información, demanda la aplicación de la IA en las siguientes áreas:

- Detección de amenazas cibernéticas: Los algoritmos de la IA son capaces de identificar patrones anómalos y posibles ciberataques.
- Respuesta automatizada: Sistemas capaces de responder automáticamente a incidentes cibernéticos, mitigando su impacto.
- Análisis de inteligencia: procesamiento y análisis de grandes volúmenes de datos para extraer información relevante y oportuna.

Detección de amenazas.

En el ciberespacio, la IA es fundamental para la detección de amenazas. Los sistemas de IA, mediante el análisis de patrones de tráfico de red y el comportamiento de los usuarios, identifican actividades sospechosas. Los modelos de aprendizaje automático permiten la detección de ataques en tiempo real, facilitando una respuesta inmediata y eficaz.

Figura 3. Detección de amenazas cibernéticas mediante la IA



Nota. Imagen elaborada mediante *Imagined with IA*.

Respuesta a incidentes.

La rápida atención a los incidentes cibernéticos es vital para minimizar los daños. La IA automatiza los procesos de contención y mitigación, lo que garantiza una respuesta inmediata. Gracias a estas capacidades, los sistemas de la IA pueden aislar amenazas y desplegar contramedidas, reduciendo significativamente los tiempos de reacción.

Figura 4. Automatización de la respuesta a incidentes cibernéticos mediante IA



Nota. Imagen elaborada mediante *Imagined with IA*.

Resiliencia cibernética.

La resiliencia cibernética es fundamental para mantener la operatividad en el ciberespacio. La IA refuerza esta resiliencia mediante el desarrollo de estrategias adaptativas que permiten a los sistemas recuperarse rápidamente de los ataques y mantener su funcionalidad crítica.

Figura 5. Estrategias de resiliencia cibernética mejoradas mediante IA



Nota. Imagen elaborada mediante *Imagined with IA*.

IA en el dominio espacial

El espacio ultraterrestre plantea desafíos únicos; múltiples autores, entre ellos el sitio web (Maris Tech Ltd, 2024) estos desafíos dejan el espacio abierto a la IA de forma esencial para enfrentarlos. La posibilidad de procesar grandes volúmenes de datos en tiempo real y tomar decisiones autónomas es fundamental para mantener la superioridad espacial y proteger los activos orbitales de posibles amenazas.

Dominio espacial.

El dominio espacial comprende las operaciones que se desarrollan en el espacio exterior, desde la utilización de satélites hasta la gestión de otros sistemas orbitales. En este ámbito, la IA desempeña un papel clave, especialmente en los siguientes campos:

- Gestión del tráfico espacial: monitoreo y predicción orbital de satélites y escombros espaciales para la prevención de colisiones.
- Mantenimiento autónomo: uso de robots equipados con IA para realizar reparaciones y mantenimiento de satélites en órbita.
- Reconocimiento y vigilancia: procesamiento de datos de sensores espaciales para identificar amenazas y objetivos desde el espacio.

Vigilancia y reconocimiento.

La IA ha transformado las operaciones de vigilancia y reconocimiento en el espacio. Los satélites equipados con IA pueden analizar imágenes en tiempo real, identificando cambios y anomalías con gran precisión. Esto mejora significativamente la capacidad de monitoreo y respuesta.

Figura 6. Aplicación de la IA en operaciones de vigilancia y reconocimiento espacial



Nota. Imagen elaborada mediante *Imagined with IA*.

Gestión del tráfico espacial.

La proliferación de satélites y desechos en órbita exige una gestión eficiente del tráfico espacial. En este contexto, la IA se emplea para predecir trayectorias y evitar colisiones, contribuyendo así a la seguridad y la sostenibilidad de las operaciones ultraterrestres.

Figura 7. Optimización del tráfico espacial mediante IA



Nota. Imagen elaborada mediante *Imagined with IA*.

Defensa de activos espaciales.

La protección de los activos espaciales es crucial para mantener la superioridad estratégica. La IA permite el desarrollo de sistemas de defensa autónomos capaces de detectar y neutralizar amenazas, como satélites hostiles o armas antisatélites.

Figura 8. *Sistemas de defensa de activos espaciales potenciados por IA*



Nota. Imagen elaborada mediante *Imagined with IA*.

Integración de la IA en operaciones multidominio.

La integración de la IA en operaciones multidominio favorece una mayor sinergia y eficacia en la planificación y ejecución de misiones que involucran fuerzas terrestres, navales, aéreas, cibernéticas y espaciales. La IA es capaz de analizar grandes volúmenes de datos en tiempo real, proporcionar recomendaciones basadas en patrones y tendencias para automatizar tareas repetitivas, lo que permite a los comandantes tomar decisiones más informadas y precisas. Además, facilita la integración de sistemas y plataformas en distintos dominios, mejorando la interoperabilidad y la coordinación entre fuerzas.

La verdadera ventaja de la IA radica en su capacidad para integrar y coordinar las operaciones en estos dominios. Algunas de sus aplicaciones clave son las siguientes:

- Fusión de datos: combinación de datos de multisensor y multifuente para proporcionar una visión completa y coherente del campo de batalla.
- Toma de decisiones asistida por IA: sistemas que respaldan a los comandantes en la toma de decisiones estratégicas y tácticas mediante el análisis de datos en tiempo real y la simulación de escenarios.
- Operaciones autónomas y semiautónomas: drones y robots capaces de operar de manera independiente o con mínima supervisión humana, realizando tareas de reconocimiento, logística y combate.

Sin embargo, la IA plantea desafíos en términos de seguridad, privacidad y ética, por lo que es crucial desarrollar e implementar la IA de forma responsable y transparente, en las operaciones multidominio.

Conclusiones

La IA está transformando las operaciones militares realizadas en los dominios aéreo, espacial y ciberespacial, redefiniendo las estrategias y capacidades de defensa a nivel mundial. En esta investigación se han analizado las contribuciones de la IA en cada uno de estos dominios, destacando tanto las oportunidades como los desafíos que plantea este escenario en constante transformación.

En el dominio aéreo, la implementación de sistemas autónomos ha mejorado significativamente la vigilancia, la toma de decisiones y la eficiencia operativa. Además, la simulación y el entrenamiento avanzado han tenido un impacto positivo en la preparación de los pilotos. Sin embargo, persisten desafíos éticos relacionados con la atribución de responsabilidades y la protección de la privacidad. Estos desafíos demandan una atención cuidadosa, a fin de lograr un equilibrio entre el uso efectivo de la IA y las consideraciones éticas y legales.

En el dominio espacial, la IA ha impulsado la gestión eficiente de constelaciones de satélites, la predicción de colisiones y la recolección de datos mediante satélites autónomos. Sin embargo, la creciente militarización del espacio plantea desafíos significativos, por lo que la colaboración internacional se vuelve esencial para establecer normas éticas y garantizar la seguridad en este entorno.

En el ciberespacio, la IA ha transformado la manera en que se abordan las amenazas cibernéticas, permitiendo la detección temprana y la respuesta automática ante ataques. Si bien la cooperación público-privada es esencial para la defensa cibernética, los desafíos relacionados con la transparencia y la responsabilidad exigen una gestión cuidadosa.

En todos estos dominios, la colaboración internacional se destaca como un factor clave para enfrentar desafíos comunes y garantizar un uso ético y eficiente de la IA en las operaciones militares. El intercambio de tecnologías, el establecimiento de normas éticas y la respuesta conjunta a las amenazas son esenciales para garantizar el éxito y la seguridad a largo plazo.

A medida que se avanza en la era de la IA en el ámbito militar, es esencial abordar, de manera proactiva, las cuestiones éticas, legales y estratégicas. La transparencia en las operaciones, la responsabilidad en las decisiones autónomas y la colaboración internacional deben ser prioritarias en el desarrollo y aplicación continua de la IA en las fuerzas armadas.

La IA está transformando, de manera irreversible, las operaciones militares en los dominios aéreo, espacial y ciberespacial. Este cambio representa una

oportunidad para mejorar la eficacia y la seguridad; sin embargo, también plantea desafíos éticos y legales que deben abordarse de manera integral.

A medida que la tecnología evoluciona, es imperativo que la comunidad internacional colabore en la construcción de un marco ético y legal sólido que guíe el desarrollo y la implementación de la IA en el ámbito militar. La aplicación de la IA en ambientes multidominio plantea una serie de desafíos complejos y multifacéticos que exigen un abordaje integral. Desde aspectos técnicos hasta consideraciones éticas, legales y de seguridad, es fundamental comprender y mitigar estos desafíos para garantizar una implementación efectiva y responsable en las operaciones militares y de seguridad nacional.

La integración de la IA en las operaciones militares de los ambientes multidominio es esencial para hacer frente a los desafíos contemporáneos de seguridad y defensa. La IA no solo optimiza la eficiencia y efectividad de las operaciones llevadas a cabo en cada dominio, sino que también facilita una coordinación y sincronización sin precedentes.

La implementación de la IA en las operaciones militares multidominio ha transformado la manera en que se libran las guerras modernas. En cuanto al dominio aéreo, la IA no solo ha optimizado la gestión del espacio y la detección de amenazas, sino que también ha fortalecido el apoyo logístico. En el ciberespacio, ha revolucionado la respuesta a incidentes y la resiliencia cibernética. En el espacio ultraterrestre, ha posibilitado mejoras significativas en la vigilancia, la gestión del tráfico espacial y la protección de activos estratégicos. La continua evolución de la IA augura una ampliación de su papel en las operaciones multidominio, al dotar a las fuerzas armadas de capacidades avanzadas y de una mayor eficiencia operativa.

Referencias

- Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*
- Allen, G. C., Cho, A., Frederick, K., Horowitz, M. C., Kania, E., & Scharre, P. (2018). *Artificial Intelligence and International Security*
- Annett, &, Elise & Giordano, J. (2026). *Artificial Intelligence and a Reconfiguration of Military Power*. Institute for National Strategic Studies National Defense University. <https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/4382869/artificial-intelligence-and-a-reconfiguration-of-military-power/#:~:text=Increasingly%2C%20AI%20is%20regarded%20as,and%20an%20external%20signaling%20mechanism>.
- Barragan, R. (2019). Integración de datos para obtener la Common Operational Picture a nivel operacional y estratégico. *Instituto Español De Estudios Estratégicos, 04* https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx._VV.AA.pdf
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., . . . Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*
- Cozad, M., Engstrom, J., Harold, S. W., Heath, T. R., Lilly, S., Burke, E. J., Brackup, J., & Grossman, D. (2023). *Gaining Victory in Systems Warfare China's Perspective on the U.S.-China Military Balance*
- Enayati, A. (2025). Deciphering China's Military Space Program and Its Global Strategic Components. <https://n9.cl/wcbri>
- Gomez de Agreda, A. (2019). Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R). *Instituto Español De Estudios Estratégicos, 04* https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx._VV.AA.pdf
- Horowitz, M. C., & Scharre, P. (2021). *AI and International Stability Risks and Confidence-Building Measures*
- Huskaj, G. (2026). *AI-Enabled Cyberspace Operations*. THE DEFENGE HORIZONI JOURNAL. <https://tdhj.org/blog/post/ai-cyberspace-operations/>
- Huynh, C. (2025). *AI on the Edge of Space Securing Space Superiority and Avoiding Surprise in Orbit*10.51593/20240060
- Kania, E. (2017). *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*
- Layton, P. (2018). *Algorithmic Warfare: Applying Artificial Intelligence to Warfighting*
- Maris Tech Ltd. (2024). *Space Situational Awareness: Navigating the Next Frontier*. <https://www.maris-tech.com/blog/space-situational-awareness-navigating-the-next-frontier/>
- Montes, B. (2023). *Inteligencia Artificial en el Espacio Ultraterrestre: ¿Un nuevo desafío para la OTAN?*. Editorial Universidad de Sevilla. 10.12795/araucaria.2023.i53.12

- Pouw, E., & Pijpers, P. (2025). *CYCON 2025 Series – AI-Enabled Offensive Cyber Operations: Challenges in the Shadows of Automation*. <https://lieber.westpoint.edu/ai-enabled-offensive-cyber-operations-legal-challenges-shadows-automation/>
- Quiñones Sigala, M. (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.10.26797/rpye.vi14i1.1044
- Raska, M. (2025). *Will AI-Driven “Super-OODA Loops” Revolutionise Military Strategy and Operations?*
- Romero, G. (2020). *Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados*. Escuela Superior de Guerra Naval. 10.35628/resup.v16i1.67
- Secretary of War. (2026). Artificial Intelligence Strategy for the Department of War: Accelerating America’s Military AI Dominance. <https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF>
- Starburst. (2026). *One sky, two systems: What ATM and UTM must learn from each other*. Starburst. <https://starburst.aero/news/one-sky-two-systems-what-atm-and-utm-must-learn-from-each-other/>
- United States Air Force. (2016). *Air Superiority 2030 Flight Plan Enterprise Capability Collaboration Team*
- Vásquez Ruiz, M. (2024). Inteligencia artificial para el desarrollo del sector aeronáutico-militar en entorno de seguridad cibernética., 151–174. <https://esdegrevistas.edu.co/index.php/rcit/article/view/4941/5344>
- Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). *Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research*. Institute of Electrical and Electronics Engineers (IEEE). 10.1109/access.2022.3204051